СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Группа хакеров атакует правительственные сервера, шифрует и выкачивает терабайт важных данных у трех десятков министерств, экономика в ступоре, силовики бессильны, народ выходит на улицы с требованием отставки правительства, в стране вводится чрезвычайное положение… Это не сценарий сериала для Netflix, а реальные события, которые произошли весной 2022 г., когда группировка вымогателей Conti атаковала целое государство — Коста-Рику.

Вот уже четвертый год подряд атаки программ-вымогателей становятся одной из самых серьезных и разрушительных киберугроз. Даже киберугрозой № 1. Жертвой шифровальщиков может оказаться как гигантская международная корпорация типа концерна Toshiba или трубопровода Colonial Pipeline, так и небольшой частный бизнес. Одна-единственная успешная атака способна полностью парализовать производство и оставить компанию без денег (суммы выкупа достигают сотен миллионов долларов!) и чувствительных данных, которые злоумышленники могут предварительно выгрузить и выставить на продажу, чтобы жертва была сговорчивее. И хотя основные цели вымогателей по-прежнему располагаются в Северной и Латинской Америке, Европе, Азиатско-Тихоокеанском регионе, последние пару лет и Россия перестала считаться тихой гаванью. По данным Group-IB, только в 2021 г. количество атак программ-вымогателей на российские компании увеличилось более чем на 200%. В первом полугодии 2022 года в мире это количество выросло в четыре раза по сравнению с I кварталом 2021 г. Когда случаются (нечасто) аресты, вымогатели уходят на дно (ненадолго) и заметают следы, проводя ребрендинг. Но говорить о закате шифровальщиков пока очень и очень рано. Команда Лаборатории компьютерной криминалистики Group-IB начала следить за шифровальщиками, когда еще мало кто видел в них серьезную угрозу. Автор книги Олег Скулкин — знаковая фигура не только в российской, но и в международной цифровой криминалистике. Он более десяти лет работает в сфере информационной безопасности, написал и выступил соавтором пяти книг по форензике и расследованию инцидентов. Олег — постоянный автор исследований, вебинаров и технических блогов о развитии империи шифровальщиков и наиболее активных преступных групп: Conti, OldGremline, LockBit, Hive, REvil. Читатель в подробностях узнает

об истории программ-вымогателей, тактиках и техниках, используемых операторами шифровальщиков, и о том, как расследовать такие атаки. Издание будет незаменимым для специалистов по цифровой криминалистике, реагированию на инциденты, проактивному поиску угроз, киберразведке, а также для профессионалов из смежных областей.

Group-IB

ВВЕДЕНИЕ

Атаки программ-вымогателей под управлением человека кардинально изменили всю современную картину угроз и стали главной опасностью для многих организаций — вот почему организации всех размеров повышают бдительность и готовятся реагировать на подобные инциденты.

Эта книга познакомит вас с миром современных атак программ-вымогателей. Особое внимание в ней уделено упреждающему, основанному на анализе данных об угрозах подходу к защите от инцидентов, связанных с такими атаками, и реагированию на них.

Для кого предназначена эта книга?

Эта книга заинтересует широкий круг технических специалистов — от студентов, изучающих кибербезопасность, до системных и сетевых администраторов малых и средних предприятий и даже специалистов по реагированию на инциденты и аналитиков киберугроз, которые хотели бы больше узнать об атаках программ-вымогателей, управляемых человеком.

О чем эта книга?

Глава 1 «История современных атак с использованием программ-вымогателей» рассказывает о мире управляемых человеком атак программ-шантажистов и их истории.

Глава 2 «Жизненный цикл современной атаки с использованием программы-вымогателя» представляет собой краткое описание того, как современные злоумышленники действуют в ходе атаки с использованием программы-вымогателя.

Глава 3 «Процесс реагирования на инциденты» описывает процесс реагирования на инциденты, связанные с атаками с использованием программ-вымогателей.

В *главе 4 «Кибербразведка и программы-вымогатели»* представлены общие сведения о кибербразведке с акцентом на атаки с использованием программ-вымогателей.

Глава 5 «Тактики, техники и процедуры групп, занимающихся распространением программ-вымогателей» подробно описывает приемы, процедуры, методы и инструменты, часто используемые теми или иными атакующими, которые занимаются программами-вымогателями.

Глава 6 «Сбор данных о киберугрозах, связанных с программами-вымогателями» содержит обзор различных источников и методов сбора сведений о киберугрозах, связанных с атаками современных программ-вымогателей.

В *главе 7 «Цифровые криминалистические артефакты и их основные источники»* представлен обзор различных источников криминалистических артефактов, на которые можно опираться при реагировании на инциденты для реконструкции жизненного цикла атаки.

В *главе 8 «Методы первоначального доступа»* предлагается практическое исследование методов первоначального доступа, используемых злоумышленниками.

В *главе 9 «Методы постэксплуатации»* рассматриваются различные методы постэксплуатации, применяемые злоумышленниками.

В *главе 10 «Методы кражи данных»* исследуются используемые методы кражи данных.

В *главе 11 «Методы развертывания программ-вымогателей»* изучаются различные методы развертывания программ-вымогателей.

В *главе 12 «Унифицированный жизненный цикл атак с использованием программ-вымогателей»* описана концепция уникального жизненного цикла, реализуемого в рамках атак, и использование программ-вымогателей.

Загрузите цветные изображения

PDF-файл с цветными изображениями снимков экрана и диаграмм, используемых в этой книге, можно получить по ссылке `https://static.packt-cdn.com/downloads/9781803240442_ColorImages.pdf`.

Используемые обозначения

В этой книге используется ряд текстовых обозначений.

`Код в тексте` указывает на участки кода в тексте, имена таблиц базы данных, имена папок, имена файлов, расширения файлов, пути, URL-адреса,

пользовательский ввод и псевдонимы Twitter, например: «Создан новый объект с `GUID {E97EFF8F-1C38-433C-9715-4F53424B4887}`. Кроме того, подозрительный файл `586A97.exe` находится в папке `C:\Windows\SYSVOL\domain\scripts`».

Блок кода выглядит так.

```
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQLPBENGINE" image="4" changed="2022-01-16 14:15:49"
uid="{94D8973D-A08E-4F28-B7D7-3745321C40A4}" disabled="0">
```

Чтобы привлечь внимание читателя к определенной части блока кода, соответствующие строки или элементы выделяются **полужирным шрифтом**.

```
<Properties startupType="DISABLED" serviceName="SQLPBENGINE"
serviceAction="STOP" timeout="30"/></NTService>
```

Любой ввод или вывод командной строки записывается следующим образом.

```
vssadmin delete shadows /all /quiet & wmic shadowcopy delete
& bcdedit /set {default} bootstatuspolicy ignoreallfailures
& bcdedit /set {default} recoveryenabled no & wbadmin delete
catalog -quiet
```

Полужирным шрифтом выделены новые термины, важные слова или слова, которые появляются на экране, — в частности, команды меню или диалоговых окон, например: «Как правило, вам нужно искать события с идентификаторами `21` (**Успешный вход в сеанс**) и `25` (**Успешное возобновление сеанса**)».

Свяжитесь с нами

Мы всегда рады читательским отзывам.

Общие вопросы. Если у вас есть любые вопросы об этой книге, напишите нам по адресу `customercare@packtpub.com`, указав в теме сообщения название книги.

Исправления. Мы приложили все усилия, чтобы обеспечить точность текста и данных, но ошибки случаются. Если вы нашли в книге ошибку, мы будем

признательны, если вы сообщите нам об этом. Пожалуйста, заполните форму по ссылке `https://www.packtpub.com/support/errata`.

Пиратство. Если вы столкнетесь с любыми незаконными копиями наших работ в интернете, мы просим вас сообщить нам адрес или название веб-сайта по адресу `copyright@packt.com`.

Будущим авторам. Если вы разбираетесь в той или иной теме и хотите посвятить ей книгу, пожалуйста, посетите страницу `authors.packtpub.com`.

Отказ от ответственности

Информацией, приводимой в этой книге, можно пользоваться, только соблюдая этические нормы. Не используйте никакую информацию из книги, если у вас нет письменного разрешения от владельца оборудования. Если вы совершите незаконные действия, вас арестуют и привлекут к ответственности по всей строгости закона. Издательство не несет никакой ответственности за неправильное использование информации, содержащейся в книге. Информация, представленная в этой книге, предназначена только для демонстрации, в зависимости от конкретного случая использования она может требовать изменений. Приведенной здесь информацией можно пользоваться только в целях тестирования с надлежащим письменным разрешением от соответствующих ответственных лиц.

Поделитесь вашим мнением

Мы будем рады узнать ваше мнение о книге. Посетите страницу `https://www.amazon.com/Incident-Response-Techniques-Ransomware-Attacks/dp/180324044X` и поделитесь своим мнением.

Ваш отзыв важен для нас и для технического сообщества, он поможет делать наш контент лучше.

РАЗДЕЛ 1

ЗНАКОМСТВО С СОВРЕМЕННЫМИ АТАКАМИ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Первый раздел этой книги поможет вам получить ясное представление о современной картине угроз, связанной с программами-вымогателями, и о том, как правильно планировать реагирование на такие инциденты.

Этот раздел состоит из следующих глав:

Глава 1. История современных атак с использованием программ-вымогателей

Глава 2. Жизненный цикл современной атаки с использованием программы-вымогателя

Глава 3. Процесс реагирования на инциденты

Глава 1

ИСТОРИЯ СОВРЕМЕННЫХ АТАК С ИСПОЛЬЗОВАНИЕМ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Атаки с использованием программ-вымогателей стали второй после COVID-19 пандемией 2020 г. — и она, к сожалению, продолжает развиваться. Некоторые злоумышленники прекратили свою деятельность, но их место быстро занимает следующее поколение киберпреступников.

Сейчас эти атаки у всех на слуху, но начались они еще до известных вспышек распространения программ-вымогателей, таких как **WannaCry** и **NotPetya**. В отличие от неконтролируемых программ-вымогателей, ими управляют различные операторы и их сообщники. Тщательная разведка уязвимостей ИТ-инфраструктур и их подготовка к развертыванию программ-вымогателей могут принести киберпреступникам миллионы долларов в криптовалюте.

Существует много ярких примеров штаммов программ-вымогателей, используемых в атаках. В этой главе мы сосредоточимся на самых важных с исторической точки зрения примерах, включая угрозу, наиболее характерную для современного ИТ-ландшафта, — программы-вымогатели как услуга.

Мы рассмотрим следующие примеры:

- 2016 г.: программа-вымогатель SamSam.
- 2017 г.: программа-вымогатель BitPaymer.
- 2018 г.: программа-вымогатель Ryuk.
- 2019 г. — настоящее время: программы-вымогатели как услуга.

2016 г. — программа-вымогатель SamSam

Операторы SamSam появились в начале 2016 г. и коренным образом изменили картину угроз, связанную с программами-вымогателями. Их целью были не обычные пользователи и отдельные устройства — используя ручное управление, они атаковали различные компании, осуществляя продвижение по сети и шифруя как можно больше устройств, в том числе тех, которые содержали наиболее важные данные.

Атакам подверглись самые разные цели, включая предприятия сферы здравоохранения и образования — и даже целые города. Ярким примером стал город Атланта (штат Джорджия), который пострадал в марте 2018 г. Восстановление инфраструктуры, пострадавшей в результате атаки, обошлось городу примерно в $2,7 млн.

Как правило, злоумышленники эксплуатировали уязвимости в общедоступных приложениях, например системах JBOSS, или просто подбирали пароли к RDP-серверам, чтобы установить первоначальный доступ к целевой сети. Чтобы получить расширенные права доступа, они использовали ряд распространенных хакерских инструментов и эксплойтов, в том числе пресловутый Mimikatz, позволяющий завладеть учетными данными администратора домена. После этого операторы SamSam просто сканировали сеть, чтобы добыть информацию о доступных хостах, на каждый из которых они копировали программу-вымогатель и запускали ее с помощью другого широко распространенного инструмента двойного назначения — **PsExec**.

Злоумышленники пользовались платежным сайтом в даркнете. Жертва получала сообщение с требованием выкупа и информацией о расшифровке файлов, сгенерированное программой-вымогателем (рис. 1.1).

По данным Sophos, в 2016–2018 гг. злоумышленники заработали около $6 млн (источник: `https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf`).

#What happened to your files?

All your files encrypted with RSA-2048 encryption. For more information search in Google "RSA Encryption"

#How to recover files?

RSA is a asymmetric cryptographic algorithm. You need one key for encryption and one key for decryption
So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can get your private key in 3 easy step:

Step1: You must send us 1.7 BitCoin for each affected PC OR 28 BitCoins to receive ALL Private Keys for ALL affected PC's.

Step2: After you send us 1.7 BitCoin, Leave a comment on our Site with this detail: Just write Your "Host name" in your comment

"Your Host name is: P4PDwPkP-PtjP"-PuPa

Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

"Our Site Address:http://qjy2f3q4bwlq2fic.onion/stackoverflow42/

"Our BitCoin Address:1Ar81cuQy7kLnKvbtiMCLsiiMeajMgMcMpi

(If you send us 28 BitCoins for all PC's, Leave a comment on our site with this detail: Just write "For All Affected PC's" in your comment)
(Also if you want pay for "all affected PC's" You can pay 14 Bitcoins to recieve half of keys(randomly) and after you verify it send 2nd half to receive all keys)

How To Access To Our Site

For access to our site you must install Tor browser and enter our site URL in your tor browser.
You can download tor browser from https://www.torproject.org/download/download.html.en
For more information please search in Google "How to access onion sites"

Test Decryption

Check our site, You can upload 2 encrypted files and we will decrypt your files as demo.

#Where to buy Bitcoin

We advise you to buy Bitcoin with Cash Deposit or WesternUnion from https://localbitcoins.com/ or https://coincafe.com/buybitcoinsnewyork.php
Because they don't need any verification and send your Bitcoin quickly.

#deadline

You just have 7 days to send us the BitCoin after 7 days we will remove your private keys and it's impossible to recover your files

Рис. 1.1. Пример сообщения SamSam с требованием выкупа[1]

---

[1] #Что случилось с вашими файлами?
Все ваши файлы зашифрованы с помощью алгоритма RSA-2048 — см. «RSA-шифрование» в поиске Google.
#Как восстановить файлы?
RSA — это асимметричный криптографический алгоритм. Вам нужен один ключ для зашифровки и другой ключ для расшифровки.
Это значит, что для восстановления файлов вам нужен закрытый ключ.
Без закрытого ключа восстановить файлы невозможно.
#Как получить закрытый ключ?
Чтобы получить закрытый ключ, выполните три простых шага.
Шаг 1: отправьте нам 1,7 биткойна за каждый пораженный компьютер или 28 биткойнов за все пораженные компьютеры.
Шаг 2: после того как вы отправите нам 1,7 биткойна, оставьте на нашем сайте комментарий с вашим именем хоста.
* Ваш хост …
Шаг 3: в ответ мы вышлем вам программу дешифрования. Вам нужно будет запустить ее на пораженном компьютере, и все зашифрованные файлы будут восстановлены.
Наш сайт: …
Наш биткойн-кошелек: …
(Если вы отправите нам 28 биткойнов за все пораженные компьютеры, оставьте на сайте комментарий «За все пораженные компьютеры».)
(Также вы можете отправить нам 14 биткойнов, получить 14 ключей (случайным образом), а после проверки доплатить, чтобы получить оставшиеся ключи.)
Как попасть на наш сайт?
Чтобы зайти на наш сайт, вы должны установить браузер TOR и ввести в нем адрес нашего сайта.
Загрузить браузер TOR можно по ссылке …
См. также в Google «Как открывать onion-сайты».
#Тестовое дешифрование
Вы можете скачать с нашего сайта два зашифрованных файла, и мы расшифруем их для вас.
#Где купить биткойн
Мы советуем покупать биткойны за наличные или через Western Union у …, потому что они не требуют проверки и высылают биткойны быстро.
#Крайний срок
Если в течение семи дней вы не отправите нам биткойны, мы удалим ваши закрытые ключи и файлы будет невозможно восстановить.

Кто стоит за программой-вымогателем SamSam?

28 ноября 2018 г. ФБР обнародовало акт, обвиняющий в международном распространении программы-вымогателя SamSam Фарамарза Шахи Саванди и Мохаммада Мехди Шаха Мансури.

СОЗДАТЕЛИ SAMSAM

Сговор с целью совершения мошенничества и связанной с ним деятельности, имеющей отношение к компьютерам; сговор с целью совершения мошенничества с использованием электронных средств связи; умышленное повреждение защищенного компьютера; передача требования, связанного с повреждением защищенного компьютера.

Мохаммад Мехди Шах Мансури

Фарамарз Шахи Саванди

Рис. 1.2. Фрагмент плаката ФБР о розыске

Оба подозреваемых из Ирана. После публикации обвинительного акта злоумышленникам удалось завершить свою криминальную деятельность — по крайней мере под именем SamSam.

Поскольку пример этих преступников показал, что атаки программ-вымогателей на корпорации могут быть очень прибыльными, стали появляться новые подобные группы. Одним из примеров стала программа-вымогатель BitPaymer.

2017 г. — программа-вымогатель BitPaymer

Программа-вымогатель BitPaymer связана с Evil Corp — киберпреступной группировкой, которая, как считается, имеет российское происхождение. С этим штаммом программы-вымогателя появилась еще одна тенденция атак, управляемых человеком, — **охота на крупную дичь**.

Все началось в августе 2017 г., когда операторы BitPaymer успешно атаковали несколько больниц управления NHS Lanarkshire и потребовали астрономическую сумму выкупа в размере $230 000, или 53 биткойнов.

Чтобы получить начальный доступ к целевой сети, группа использовала свой давний инструмент — троян **Dridex**. Троян позволял злоумышленникам

загружать PowerShell Empire — популярный фреймворк постэксплуатации, — чтобы перемещаться по сети и получать расширенные права доступа, в том числе с использованием Mimikatz, как делали операторы SamSam.

Преступники развертывали программу-вымогатель в масштабах предприятия, используя модификацию групповой политики, которая позволяла им отправлять на каждый хост скрипт для запуска экземпляра программы-вымогателя.

Злоумышленники общались с жертвами как по электронной почте, так и в онлайн-чатах.

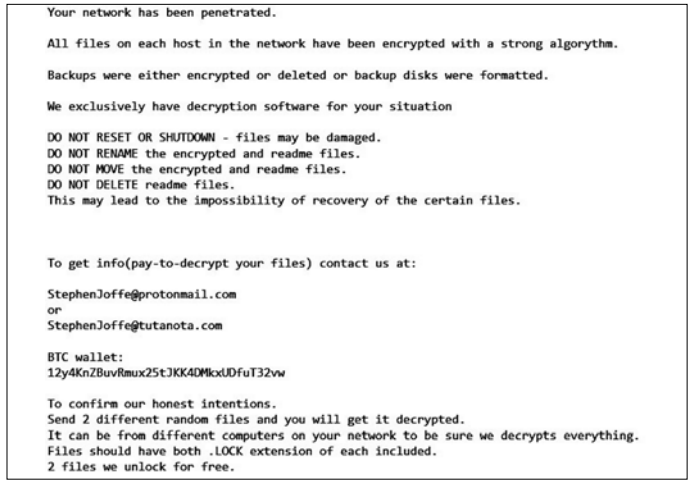


Рис. 1.3. Пример сообщения BitPaymer с требованием выкупа[1]

В июне 2019 г. появилась новая программа-вымогатель DoppelPaymer, основанная на BitPaymer. Считается, что ею управляла дочерняя группа Evil Corp (источник: `https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/`).

---

[1] Ваша сеть взломана.
Все файлы на каждом хосте сети зашифрованы с помощью надежного алгоритма.
Резервные копии либо зашифрованы или удалены, либо отформатированы диски резервных копий.
У нас есть уникальное программное обеспечение для расшифровки ваших файлов.
Не перезагружайте и не выключайте компьютер — это может повредить файлы.
Не переименовывайте зашифрованные файлы или файлы readme.
Не перемещайте зашифрованные файлы или файлы readme.
Не удаляйте файлы readme.
Это может привести к тому, что определенные файлы будет невозможно восстановить.
Чтобы получить информацию об оплате расшифровки ваших файлов, свяжитесь с нами по адресу:
…
Кошелек BTC: …
Чтобы убедиться в наших честных намерениях:
отправьте два разных случайных файла и получите их расшифровку.
Чтобы убедиться в том, что мы все расшифруем, вы можете отправить файлы с разных компьютеров вашей сети.
Оба файла должны иметь расширение .LOCK. Мы разблокируем два файла бесплатно.

Создатели программы-вымогателя BitPaymer

13 ноября 2019 г. ФБР обнародовало заключение, в котором виновными в управлении троянскими программами Dridex были названы Максим Викторович Якубец и Игорь Олегович Турашев.

МАКСИМ ВИКТОРОВИЧ ЯКУБЕЦ

Преступный сговор; сговор с целью совершения мошенничества; мошенничество с использованием электронных средств, банковское мошенничество; умышленное повреждение компьютера.

ИГОРЬ ОЛЕГОВИЧ ТУРАШЕВ

Преступный сговор; сговор с целью совершения мошенничества; мошенничество с использованием электронных средств, банковское мошенничество; умышленное повреждение компьютера.

Рис. 1.4. Фрагмент плаката ФБР о розыске

Максим Викторович Якубец в настоящее время находится в розыске по нескольким пунктам обвинения в киберпреступной деятельности. По различным данным, за его поимку назначена награда в $5 млн.

Разумеется, Dridex не был единственным трояном, использованным в атаках программ-вымогателей, управляемых людьми. Другой яркий пример — Trickbot, тесно связанный с программой-вымогателем Ryuk.

2018 г. — программа-вымогатель Ryuk

Программа-вымогатель Ryuk вывела охоту на крупную дичь на новый уровень. Этот штамм программы-вымогателя, связанный с группой Trickbot, также известной как **Wizard Spider**, активен и сегодня.

По данным AdvIntel, за свою историю группа атаковала различные организации и заработала не менее $150 млн (источник: `https://www.`

advanced-intel.com/post/crime-laundering-primer-inside-ryuk-crime-crypto-ledger-risky-asian-crypto-traders).

Некоторое время Ryuk называли *тройной угрозой*, поскольку заражения обычно начинались с трояна Emotet, который загружал Trickbot, который, в свою очередь, использовался для загрузки инструментов постэксплуатации и окончательного развертывания программы-вымогателя. Обычно Trickbot использовался для загрузки агента PowerShell Empire или **Cobalt Strike Beacon** — элемента еще одного чрезвычайно популярного фреймворка постэксплуатации.

Недавно группа изменила набор инструментов и стала использовать новый троян под названием **Bazar**. Интересно, что они начали применять «вишинг» (голосовой фишинг). Фишинговые письма содержат не вредоносные файлы или ссылки, а лишь ложную информацию о платной подписке и номер телефона, по которому можно позвонить, чтобы отменить ее. Если жертва звонит по номеру, оператор подсказывает ей загрузить вредоносный файл Microsoft Office, открыть его и включить макросы, которые заражают компьютер трояном Bazar. Как и в случае с Trickbot, троян используется для загрузки и запуска фреймворка постэксплуатации — чаще всего Cobalt Strike.

Злоумышленники использовали несколько методов запуска Ryuk, в том числе ранее упомянутый PsExec и модификацию групповой политики. Поначалу они указывали адреса электронной почты, чтобы жертвы могли связаться с ними, но вскоре начали использовать onion-сервисы Tor.

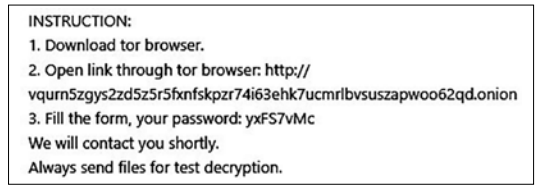


Рис. 1.5. Инструкции, указанные в сообщении о выкупе[1]

Операторы программы-вымогателя Ryuk по-прежнему активны и, по данным AdvIntel и HYAS, уже заработали более $150 млн (источник: https://www.advanced-intel.com/post/crime-laundering-primer-inside-ryuk-crime-crypto-ledger-risky-asian-crypto-traders).

---

[1] ИНСТРУКЦИЯ
1. Скачайте браузер TOR.
2. Откройте ссылку через браузер TOR …
3. Заполните форму, ваш пароль: …
Мы свяжемся с вами в скором времени.
Всегда отправляйте файлы для тестовой расшифровки.

Кто стоит за программой-вымогателем Ryuk?

4 июня 2021 г. ФБР обнародовало документ, обвиняющий Аллу Витте, также известную как Макс, в причастности к транснациональной организации, ответственной за создание и распространение трояна Trickbot.

Некоторые другие лица, связанные с Ryuk, были операторами ботнета Emotet. Их арестовали в январе 2021 г. в результате совместной операции правоохранительных органов Нидерландов, Германии, США, Великобритании, Франции, Литвы, Канады и Украины. В результате власти взяли инфраструктуру ботнета под полный контроль.

Вот как выглядело рабочее место операторов Emotet.

Рис. 1.6. Рабочее место операторов Emotet

Несмотря на аресты злоумышленников, «большая игра» привлекает все больше и больше киберпреступников. В результате появился еще один феномен — программа-вымогатель как услуга.

2019 г. — настоящее время: программы-вымогатели как услуга (RaaS)

2019 г. был годом роста популярности **программ-вымогателей как услуги**, и сегодня они по-прежнему остаются главной тенденцией. Многие разработчики программ-вымогателей начали предлагать свои продукты различным злоумышленникам в обмен на процент от полученного выкупа.

REvil, **LockBit**, **Ragnar Locker**, **Nefilim** — лишь некоторые из семейств программ-вымогателей, распространяемых по модели «программа-вымогатель как услуга». И даже если несколько злоумышленников используют

один и тот же тип программы-вымогателя, их тактики, техники и процедуры могут быть очень разными.

Тем не менее в настоящее время многие злоумышленники используют один и тот же подход: они извлекают данные до фактического развертывания программ-вымогателей. Этот тренд заложили еще в 2019 г. операторы программ-вымогателей Maze. В настоящее время почти все злоумышленники, предпринимающие подобные атаки, имеют свои собственные **сайты утечки данных (Data Leak Site, DLS)**.

Вот пример DLS, используемого в операциях с программой-вымогателем DoppelPaymer.

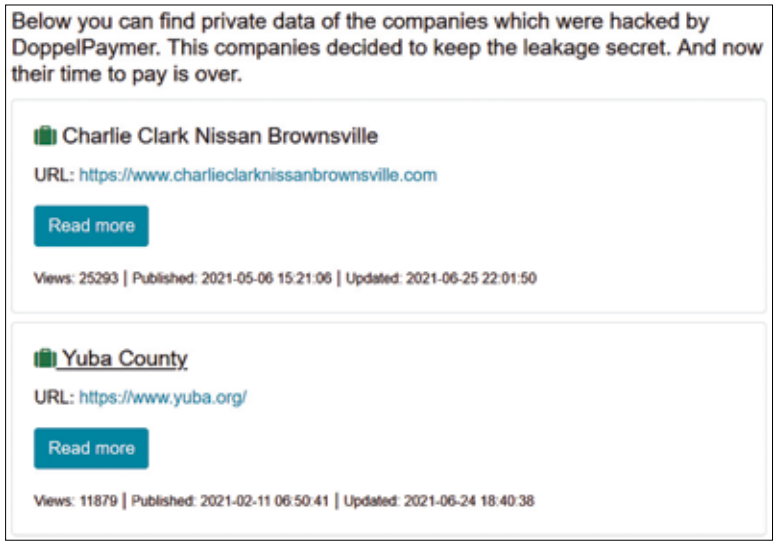


Рис. 1.7. DLS DoppelPaymer[1]

Обычно инициаторы атаки не управляют сами всем ее жизненным циклом, а пользуются услугами других злоумышленников. Например, они могут сотрудничать с брокерами первоначального доступа, которые позволяют им проникнуть в скомпрометированные корпоративные сети. В некоторых случаях они могут платить профессиональным тестировщикам

[1] Ниже вы можете найти личные данные компаний, которые были взломаны DoppelPaymer. Эти компании решили сохранить утечку в тайне. И теперь их время платить истекло.
Чарли Кларк Ниссан Браунсвилл
URL-адрес:
Читать далее
Просмотров: 25293 / Опубликовано: 2021–05–06 15:21:06 / Обновлено: 2021–06–25 22:01:50
Графство Юба
URL-адрес:
Читать далее
Просмотров: 11879 / Опубликовано: 2021–02–11 06:50:41 / Обновлено: 2021–06–24 18:40:38

на проникновение (пентестерам) за расширение прав доступа или обход защиты, чтобы затем беспрепятственно запускать программы-вымогатели в масштабах всего предприятия.

Злоумышленники, участвующие в проекте, могут получать различные доли от выкупа. Обычно разработчики получают около 20%, инициаторы атаки — около 50%, брокеры первоначального доступа — 10%, а остальное достается вспомогательным злоумышленникам, например пентестерам или переговорщикам.

Программы-вымогатели как услуга в настоящее время чрезвычайно распространены. Согласно отчету *Group-IB Ransomware Uncovered 2020/2021* (`https://www.group-ib.com/ resources/threat-research/ransomware-2021.html`), 64% всех атак программ-вымогателей в 2020 г. были совершены лицами, связанными с RaaS.

Кто стоял за программами-вымогателями как услугой?

Одному из лиц, связанных с программой-вымогателем NetWalker, Себастьену Вашон-Дежардену, гражданину Канады, было предъявлено обвинение в январе 2021 г. Утверждается, что он в общей сложности заработал вымогательством более $27,6 млн.

Другой пример — пара лиц, аффилированных с программой-вымогателем Egregor, которые были арестованы с помощью французских властей, отследивших уплаты выкупа в их адрес.

Еще один пример — лица, связанные с программой-вымогателем Clop, которые помогали злоумышленникам в отмывании денег и также были арестованы в июне 2021 г.

Таким образом, программы-вымогатели как услуга позволили присоединиться к «большой игре» многим киберпреступникам — даже тем, кому не хватало навыков и возможностей. Это один из важных факторов превращения атак программ-вымогателей, управляемых людьми, в киберпандемию.

Выводы

В этой главе вы ознакомились с историей современных атак с использованием программ-вымогателей и немного узнали о тактиках, техниках и процедурах злоумышленников, их бизнес-модели — и даже о некоторых людях, которые стояли за описанными атаками.

В следующей главе мы углубимся в современную картину угроз, связанную с программами-вымогателями, и сосредоточимся на жизненном цикле атаки — от получения первоначального доступа до фактического запуска программы-вымогателя.

Глава 2

ЖИЗНЕННЫЙ ЦИКЛ СОВРЕМЕННОЙ АТАКИ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММЫ-ВЫМОГАТЕЛЯ

Атаки с использованием программ-вымогателей могут быть очень сложными, особенно если речь идет об охоте на крупную дичь — корпорации. Поэтому, прежде чем углубляться в технические детали, очень важно разобраться в том, как устроен жизненный цикл типичной атаки. Понимание жизненного цикла атаки помогает специалистам по безопасности правильно реконструировать инциденты и принимать верные решения на различных этапах реагирования.

Как вы уже знаете из *главы 1 «История современных атак с использованием программ-вымогателей»*, программой-вымогателем как услугой может управлять как группа лиц, так и ряд отдельных злоумышленников. Что это значит? Тактики, техники и процедуры могут сильно различаться, но жизненный цикл атаки в большинстве случаев будет примерно одинаковым, поскольку злоумышленники обычно преследуют две основные цели — украсть конфиденциальную информацию из целевой сети и развернуть копию программы-вымогателя в масштабах предприятия.

В этой главе мы кратко обсудим различные этапы атак программ-вымогателей, управляемых человеком, чтобы сформировать ясное представление о жизненном цикле этих атак и подготовиться к погружению в технические детали.

В этой главе мы рассмотрим следующие темы:

- Начальные векторы атаки.
- Постэксплуатация.
- Кража данных.
- Развертывание программ-вымогателей.

Начальные векторы атаки

Любая атака начинается с получения первоначального доступа. Это можно сделать через подключенный к внутренней сети VPN, доставленный с помощью целевого фишинга троян, развернутый с помощью взлома общедоступного приложения веб-интерфейс и даже с помощью атаки на цепочку поставок (другой термин — атака через третью сторону).

Три наиболее распространенных начальных вектора атаки — это получение доступа через протокол удаленного рабочего стола (RDP), целевой фишинг и эксплуатация уязвимостей программного обеспечения.

Ниже приведены статистические данные о наиболее распространенных векторах атак программ-вымогателей до II квартала 2021 г. включительно, собранные Coveware (источник: `https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority`).

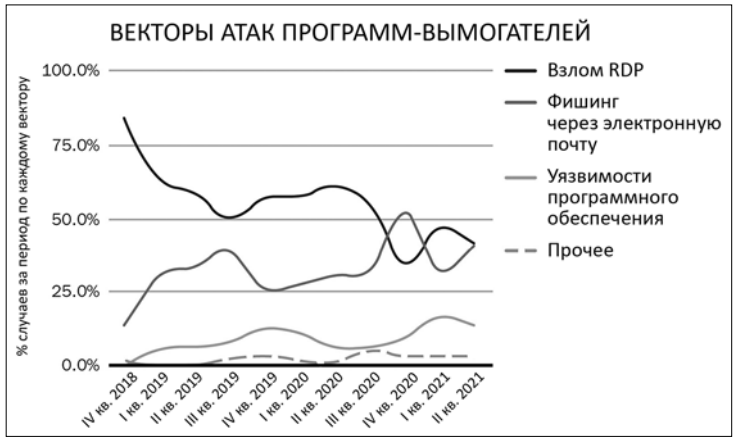


Рис. 2.1. Наиболее распространенные векторы атак программ-вымогателей, согласно Coveware

Рассмотрим каждый из них подробнее и сопроводим примерами.

Получение доступа через протокол удаленного рабочего стола (RDP)

В течение многих лет RDP оставался наиболее распространенным способом доступа злоумышленников к целевой сети. Из *главы 1 «История современных атак с использованием программ-вымогателей»* вы уже знаете, что его использовали пионеры подобных атак — операторы **SamSam**. Конечно, SamSam — не единственный пример. В настоящее время этим вектором пользуется множество злоумышленников — и действующие от случая к случаю, как операторы программы-вымогателя **Dharma**, и целенаправленные организованные группы вроде **REvil**.

Пандемия усугубила ситуацию — многие компании предоставили своим сотрудникам возможность удаленной работы и были вынуждены открыть свои серверы, которые стали мишенями для разного рода злоумышленников, включая операторов программ-вымогателей.

Например, воспользовавшись системой поиска общедоступных серверов Shodan с открытым портом `3389` (порт по умолчанию для RDP), можно увидеть миллионы устройств.

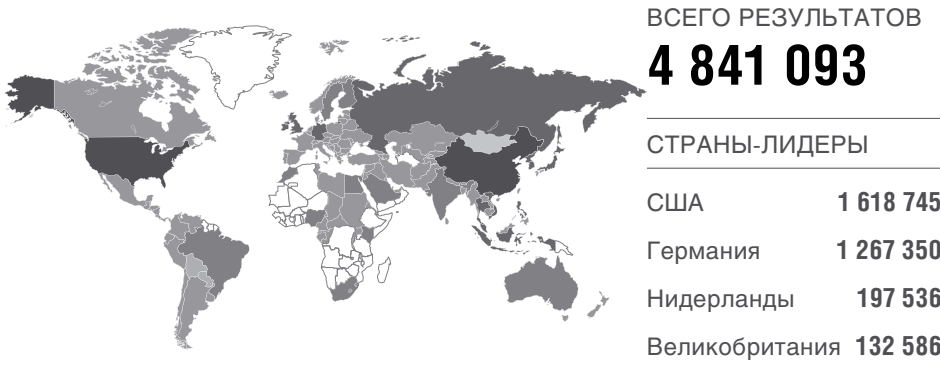


Рис. 2.2. Количество устройств, подключенных к интернету с открытым портом 3389

Простейший поиск выдает миллионы результатов — это одна из причин, по которой данный начальный вектор атаки так популярен среди операторов программ-вымогателей.

На практике злоумышленники не всегда пытаются сами атаковать такие серверы, они могут просто купить доступ к ним. Операторы программ-вымогателей как услуги могут не только арендовать программы-вымогатели, но и покупать доступ к корпоративным сетям у так называемых брокеров первоначального доступа. Такие брокеры обычно не участвуют в этапе

постэксплуатации, чаще они продают первоначальный доступ или отдают его за долю (в среднем до 10%) в возможной сумме выкупа.

Иногда операторы программ-вымогателей даже создают темы на андеграундных форумах, чтобы привлечь внимание брокеров первоначального доступа. Вот, например, сообщение, предоставленное платформой *Threat Intelligence and Attribution* компании *Group-IB*, — оно показывает, что операторы программы-вымогателя **Crylock** заинтересованы в покупке различных типов доступа к корпоративным сетям.

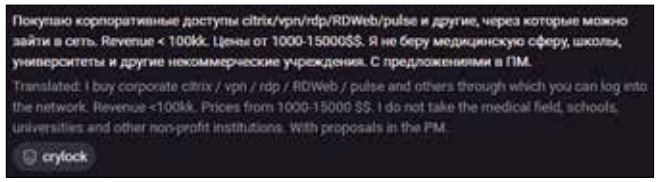


Рис. 2.3. Пост на андеграундном форуме

Далее мы рассмотрим другой чрезвычайно популярный начальный вектор атаки — целевой фишинг.

Целевой фишинг

Целевой фишинг подразумевает использование социальной инженерии. Злоумышленники манипулируют пользователями, чтобы те открывали вредоносные вложения или переходили по опасным ссылкам. Так в их распоряжении оказываются учетные данные, которые потенциально можно использовать для получения VPN-доступа к целевой сети или, как вы уже знаете из *главы 1 «История современных атак с использованием программ-вымогателей»*, для заражения устройств троянскими программами. Поначалу многие злоумышленники использовали такое вредоносное ПО для банковского мошенничества, но оно также применяется для получения первоначального доступа к корпоративным сетям.

Наиболее распространенные примеры подобных троянов:

- BazarLoader
- Hancitor
- IcedID
- Qakbot
- Trickbot

Естественно, список неполный — это лишь наиболее распространенные примеры средств, прокладывающих дорогу операторам программ-вымогателей.

Обычно операторы таких троянов проводят массированные спам-кампании, в основном среди корпоративных пользователей. Чаще всего они

используют перехват цепочки сообщений — со взломанных адресов электронной почты злоумышленники отправляют вредоносные документы в ответ на подлинные электронные письма.

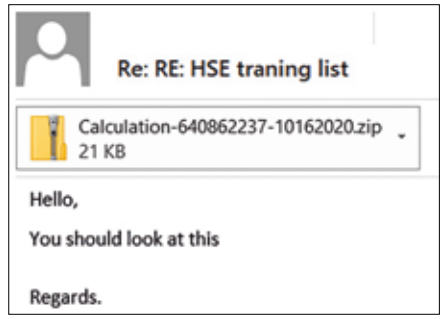
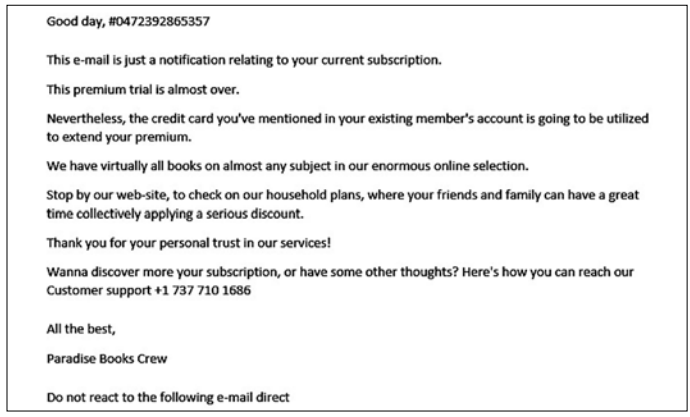


Рис. 2.4. Пример перехвата цепочки сообщений операторами Qakbot[1]

В некоторых случаях злоумышленники используют еще более изощренные методы: из *главы 1 «История современных атак с использованием программ-вымогателей»* вы знаете, что операторы **BazarLoader** также использовали вишинг (голосовой фишинг).

Пример такого электронного письма приведен ниже.


Good day, #0472392865357

This e-mail is just a notification relating to your current subscription.

This premium trial is almost over.

Nevertheless, the credit card you've mentioned in your existing member's account is going to be utilized to extend your premium.

We have virtually all books on almost any subject in our enormous online selection.

Stop by our web-site, to check on our household plans, where your friends and family can have a great time collectively applying a serious discount.

Thank you for your personal trust in our services!

Wanna discover more your subscription, or have some other thoughts? Here's how you can reach our Customer support +1 737 710 1686

All the best,

Paradise Books Crew

Do not react to the following e-mail direct

Рис. 2.5. Пример фишингового письма с целью распространения BazarLoader[2]

---

[1] Привет! Посмотри, пожалуйста. С уважением.

[2] Здравствуйте, #0472392865357
Это письмо касается вашей подписки. Срок пробной премиум-версии почти истек. Для продления премиум-подписки будет использована указанная вами в личном кабинете кредитная карта.
В нашей огромной онлайн-коллекции представлены практически все книги на любые темы. Загляните на наш сайт, чтобы ознакомиться с семейными подписками, благодаря которым ваши близкие смогут насладиться первоклассным контентом с большой групповой скидкой. Благодарим вас за доверие к нашему сервису!
У вас остались вопросы о подписке? Свяжитесь с нашей службой поддержки по телефону +1 737 710 1686.
С наилучшими пожеланиями, команда Paradise Books. Не отвечайте на это письмо.

Как видите, вредоносных вложений в данном случае нет. Вместо этого злоумышленники просят жертву не отвечать на письмо, а позвонить по телефону службы поддержки, чтобы связаться с подставной компанией и отменить подписку.

Если жертва позвонит, злоумышленники из фальшивого кол-центра направят ее на веб-сайт, чтобы она самостоятельно открыла вредоносный документ и включила макросы, чтобы загрузить и запустить BazarLoader.

Мы рассмотрим дополнительные технические подробности запуска и маскировки таких троянских программ в следующих главах, а пока запомните, что злоумышленники могут использовать их для загрузки дополнительных инструментов на скомпрометированный хост, чтобы затем выполнить шаги постэксплуатации и получить в свое распоряжение привилегированные учетные записи для продвижения по сети.

В завершение нашего обзора начальных векторов атак мы сделаем обзор различных уязвимостей программного обеспечения, позволяющих операторам программ-вымогателей получать доступ к целевой сети.

Уязвимости ПО

Уязвимости программного обеспечения позволили многим брокерам начального доступа разбогатеть на сотни тысяч долларов, но при помощи программ-вымогателей как услуги были получены миллионы.

Конечно, не каждая уязвимость дает злоумышленнику возможность получить первоначальный доступ в сеть. Чаще всего используются уязвимости, которые позволяют удаленно запустить код или получить файлы с учетными данными.

Хороший пример уязвимости — приложение **Pulse Secure VPN**. Например, уязвимость CVE-2019–11510 позволяла злоумышленникам получать имена пользователей и незашифрованные пароли от уязвимых устройств, чтобы использовать их для доступа в сеть.

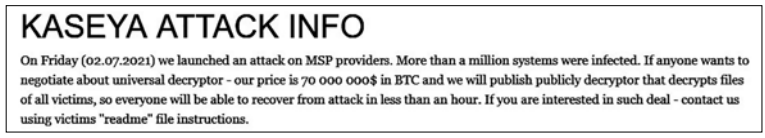
Другая уязвимость, популярная среди операторов программ-вымогателей, — CVE-2018–13379 в серверах **FortiGate VPN**. Она тоже позволяет злоумышленникам читать файлы с незашифрованными учетными данными.

Уязвимость CVE-2019–19781 в решении **Citrix ADC and Gateway** также активно использовалась многими группами вымогателей — она позволяла злоумышленникам удаленно загружать и запускать вредоносный код и выполнять другие действия постэксплуатации.

Еще один пример — многочисленные уязвимости в Accellion Legacy File Transfer Appliance, включая CVE-2021–27101, CVE-2021–27102, CVE-2021–27103 и CVE-2021–27104, используемые бандой вымогателей **Clop**.

Наконец, в некоторых случаях злоумышленникам удается использовать даже уязвимости «нулевого дня» — это такие уязвимости в системах или

устройствах, которые уже стали известны, но еще не были исправлены разработчиками. В июле 2021 г. участники группировки REvil успешно воспользовались несколькими уязвимостями в службе удаленного управления Kaseya VSA и запустили вредоносный пакет обновления, что привело к развертыванию программы-вымогателя. Атака затронула многих клиентов Kaseya, в том числе поставщиков услуг комплексного управления ИТ-инфраструктурой, поэтому злоумышленники запросили действительно крупный выкуп — $70 млн.


KASEYA ATTACK INFO

On Friday (02.07.2021) we launched an attack on MSP providers. More than a million systems were infected. If anyone wants to negotiate about universal decryptor - our price is 70 000 000$ in BTC and we will publish publicly decryptor that decrypts files of all victims, so everyone will be able to recover from attack in less than an hour. If you are interested in such deal - contact us using victims "readme" file instructions.

Рис. 2.6. Информация об атаке на DLS REvil[1]

Конечно, получение начального доступа в сеть — это еще не все. В большинстве случаев злоумышленникам приходится повышать права доступа, получать учетные данные, выполнять разведку сети и другие действия постэксплуатации.

Постэксплуатация

Доступ в сеть — это только полдела. Во многих случаях злоумышленники недостаточно хорошо знакомы с сетью и получают доступ только к учетным записям с ограниченными правами, а значит, не могут отключить элементы управления безопасностью и продвигаться по сети, чтобы получить конфиденциальные данные и развернуть программу-вымогатель.

Действия в рамках постэксплуатации зависят от типа доступа. Например, если злоумышленники имеют доступ к VPN, они могут просканировать сеть на наличие уязвимостей, которые обеспечат им возможность продвижения по ней.

Не удивляйтесь — пресловутый эксплойт **EternalBlue** (CVE-2017–0144) до сих пор чрезвычайно распространен во многих корпоративных сетях, в том числе на действительно крупных предприятиях.

Еще одна очень распространенная уязвимость, используемая различными операторами программ-вымогателей, — **Zerologon** (CVE-2020–1472).

---

[1] Информация об атаке на Kaseya
В пятницу (02.07.2021) мы атаковали провайдеров MSP. Заражено более миллиона систем. Наша цена полного декодирования — $70 млн в биткойнах, на этих условиях мы выложим в открытый доступ декриптор для расшифровки всех пострадавших файлов, то есть все жертвы смогут ликвидировать последствия атаки в течение часа. Если вам интересно наше предложение, свяжитесь с нами, используя инструкции в файлах readme пострадавших устройств.

Она позволяет злоумышленникам получить доступ к контроллеру домена в несколько щелчков мышью.

Злоумышленники, которые применяют различные трояны, обычно начинают с использования встроенных сервисов Windows для диагностики сети и службы каталогов Active Directory, таких как net.exe, nltest и др., а затем пользуются сторонними инструментами, загружаемыми на скомпрометированный хост. Наиболее распространенные инструменты:

- AdFind
- Bloodhound (Sharphound)
- ADRecon

Эти инструменты позволяют собирать информацию о пользователях и группах, компьютерах, подсетях, правах доступа к доменам и даже выявлять доверительные отношения внутри Active Directory.

Если взломщики получили доступ к скомпрометированному узлу по RDP, они обычно используют широкий набор инструментов — от сетевых сканеров до дамперов паролей. Вот некоторые самые распространенные инструменты:

- SoftPerfect Network Scanner
- Advanced IP Scanner
- Mimikatz
- LaZagne
- Process Hacker
- ProcDump
- NLBrute

В некоторых случаях, особенно если злоумышленники уже имеют первоначальный доступ к серверу, они могут почти сразу получить учетные данные с повышенными правами, используя части загруженного набора инструментов, например, для создания снимка памяти процесса Сервиса проверки подлинности локальной системы безопасности (**Local Security Authority Subsystem Service, LSASS**).

Другая типичная характеристика современных атак программ-вымогателей, управляемых человеком, — интенсивное использование различных фреймворков постэксплуатации. Я почти уверен, что вы слышали о Cobalt Strike. Это самый распространенный фреймворк, используемый не только киберпреступниками, но и хакерами, действующими по заказу государств.

Но это только один из примеров. Реагируя на атаки с использованием программ-вымогателей, вы можете также столкнуться с:

- Metasploit
- PowerShell Empire
- CrackMapExec
- Koadic
- PoshC2

Подобные сервисы позволяют операторам программ-вымогателей решать различные задачи: сканировать сеть, повышать права доступа, выгружать учетные данные, загружать и запускать сторонние инструменты и сценарии, горизонтально перемещаться по сети с использованием различных методов и многое другое.

Еще один важный шаг злоумышленников — обеспечение резервного доступа. В частности, они могут распространять трояны, которые уже использовались для получения первоначального доступа, запускать элементы фреймворков постэксплуатации на удаленных хостах и даже устанавливать на отдельные серверы с доступом в интернет легитимное программное обеспечение для удаленного доступа, такое как TeamViewer.

Как только злоумышленники достаточно хорошо изучат сеть, в которую проникли, и получат повышенные права, они могут приступить к достижению основных целей — краже данных и развертыванию программ-вымогателей.

Кража данных

Кражу данных иногда называют утечкой данных, экспортом данных или эксфильтрацией данных, и она чрезвычайно популярна среди операторов программ-вымогателей. Практически у всех злоумышленников, связанных с атаками программ-вымогателей, управляемых человеком, есть собственные **сайты утечки данных (Data Leak Site, DLS)**. Они публикуют на таких веб-сайтах информацию об успешных атаках — и даже сами украденные данные, если компания отказывается платить выкуп.

Объем украденных данных может быть самым разным. В некоторых случаях это всего несколько гигабайт, в других — терабайты. Эксфильтрованные данные могут включать информацию о кредитных картах, номера социального страхования (*англ.* **Social Security numbers**, сокр. **SSN**), персональные данные (**Personal Identifiable Information, PII**), защищенную медицинскую информацию (**Protected Health Information, PHI**) и национальные идентификаторы поставщиков медицинских услуг (**National Provider Identifiers, NPI**) и не ограничены частной и конфиденциальной информацией компании.

На рисунке 2.7 приведен пример DLS программы-вымогателя **Conti**.

Большинство таких веб-сайтов расположены в даркнете, и доступ к ним можно получить, например, через браузер Tor. Если вы хотите отслеживать изменения на таких сайтах с помощью обычного веб-браузера, рекомендуем использовать проект **Ransomwatch** (`https://www.ransomwatch.org/`). Этот веб-сайт автоматически снимает и публикует скриншоты активных DLS, принадлежащих различным операторам программ-вымогателей.

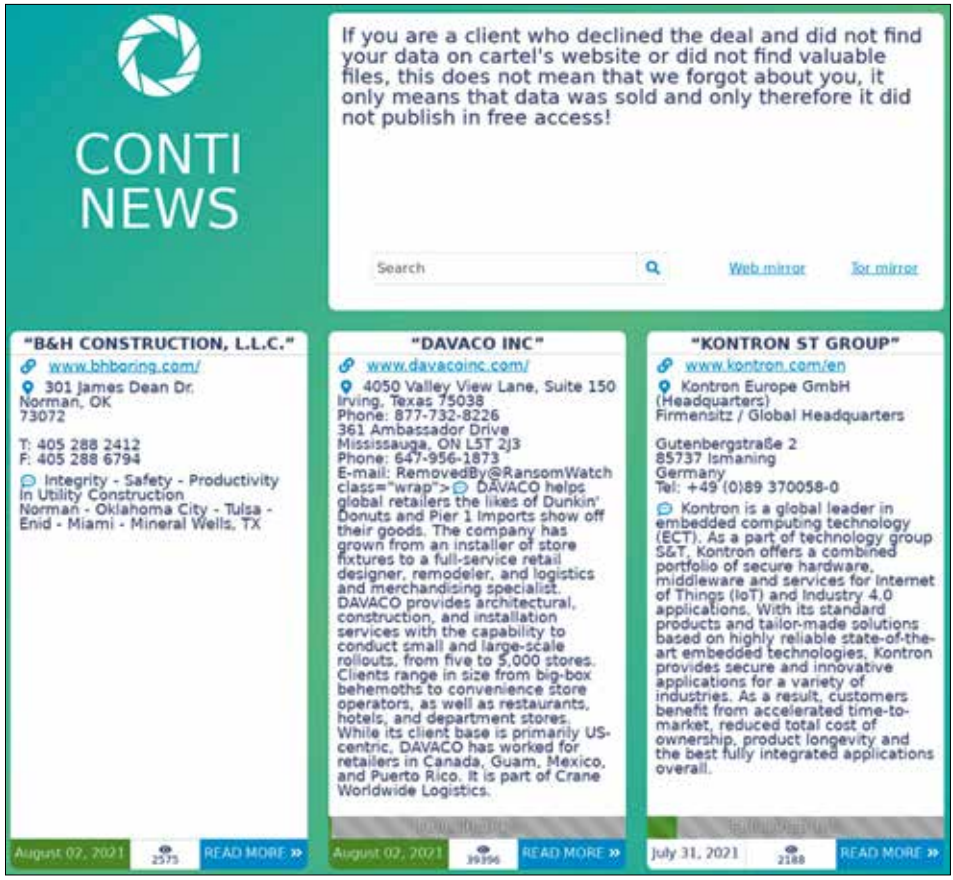


Рис. 2.7. DLS программы-вымогателя Conti[1]

Злоумышленники могут потратить довольно много времени на извлечение данных из взломанной сети — иногда несколько месяцев. За это время они могут найти наиболее конфиденциальные данные и обеспечить дополнительные средства удаленного доступа к скомпрометированной сети на случай, если метод первоначального доступа будет раскрыт и доступ заблокирован.

Как правило, применяется один из двух подходов к эксфильтрации данных. В первом случае преступники могут настроить для этой цели сервер или использовать те же серверы, с которых осуществлялась атака, — например, с помощью фреймворков постэксплуатации.

[1] Если вы клиент, отказавшийся от сделки, и не нашли свои данные или ценные файлы на сайте картеля, это не значит, что мы о вас забыли, — просто ваши данные уже проданы и поэтому не опубликованы в открытом доступе.

В этих случаях злоумышленники обычно крадут данные с помощью легальных инструментов, таких как **WinSCP** или **FileZilla**. Обнаружить такие инструменты может быть чрезвычайно сложно, особенно если в составе службы безопасности организации нет специальной группы мониторинга, которая постоянно вела бы активный поиск угроз.

Как правило, данные сначала нужно собрать, но в некоторых случаях их можно извлечь прямо с файлового сервера — даже без архивации.

Другой подход — использовать общедоступные облачные хранилища, такие как **MEGA**, **DropMeFiles** и др. Эти же хранилища злоумышленники могут использовать для публикации данных на своих DLS.

Так выглядят данные, украденные злоумышленниками, использующими программу-вымогатель Everest, и загруженные в DropMeFiles.

Рис. 2.8. Украденные данные, опубликованные злоумышленниками, использующими программу-вымогатель Everest

Чтобы выгружать данные таким способом, злоумышленники могут использовать обычный веб-браузер или, в некоторых случаях, соответствующие клиентские приложения. Например, операторы программы-вымогателя **Nefilim** просто установили **MEGAsync** на целевой хост и выгружали данные с его помощью.

Другой яркий пример: партнеры **Mount Locker** использовали для кражи собранных данных хранилище Amazon S3. AWS и другие облачные решения могут быть хорошим подспорьем для крупных краж данных, так что использование таких решений без надлежащего управления и надзора — большая помощь злоумышленникам.

Как только все конфиденциальные данные (по крайней мере с точки зрения злоумышленников) извлечены, сеть жертвы готова к развертыванию программы-вымогателя.

Развертывание программ-вымогателей

Как вы думаете, кто злейший враг оператора программы-вымогателя? Верно, резервные копии — если они защищены от взлома и хранятся