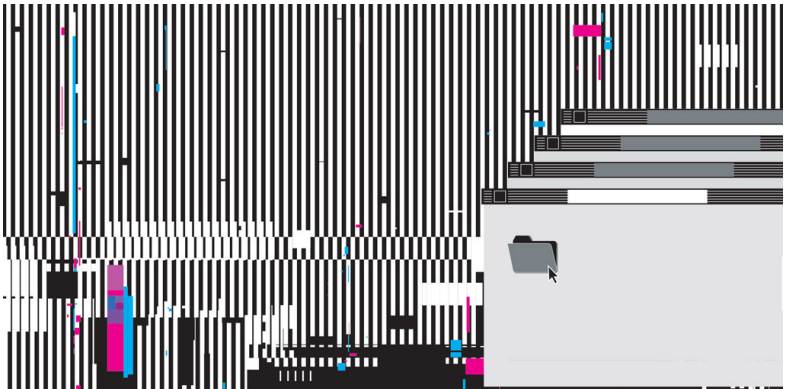

Олег Скулкин

ШИФРОВАЛЬЩИКИ

Как реагировать на атаки с использованием программ-вымогателей

GROUP-IB

альпина PRO

Олег Скулкин

Шифровальщики. Как реагировать на атаки с использованием программ-вымогателей

Текст предоставлен правообладателем
http://www.litres.ru/pages/biblio_book/?art=68872686
Шифровальщики: Как реагировать на атаки с использованием программ-вымогателей: Альпина ПРО; Москва; 2023
ISBN 9785206001709

Аннотация

«Шифровальщики» – это программы, которые находят уязвимости в сетях предприятий, чтобы потом с помощью этих уязвимостей внедриться в сеть, завладеть ценной для предприятия информацией и далее вымогать деньги из руководства компании. Разумеется, программы эти создаются людьми, которые могут как объединяться в преступные группы, так и действовать поодиночке.

«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 году количество атак программ-вымогателей на российские компании увеличилось более чем на 200 %».

В последние годы происходит рост кибератак именно с помощью программ-шифровальщиков. К сожалению, этот тренд не обошел и Россию – здесь количество таких атак только за 2021 год выросло более чем в три (!) раза.

Именно поэтому так кстати в русском переводе выходит книга Олега Скулкина, выдающегося эксперта не только в российской, но и в международной цифровой криминалистике. Автор рассказывает обо всем, что касается шифровальщиков, – от истории атак до цифровых улик. Посреди его повествования вполне естественно выглядят фрагменты программного кода, а кое-где – цветные скриншоты.

«Тщательная разведка уязвимостей ИТ-инфраструктур и их подготовка к развертыванию программ- вымогателей могут принести киберпреступникам миллионы долларов в криптовалюте».

По мнению автора (а это мнение основано на более чем десятилетнем опыте работы в сфере информационной безопасности), сети и деньги предприятия можно уберечь, если понимать жизненный цикл атак программ-вымогателей – об этом цикле подробно рассказывается во второй главе книги, а также в последней главе, где автор помогает читателям научиться реконструировать универсальный жизненный цикл атаки, которому подчиняются все шифровальщики, какими бы индивидуальными особенностями они ни отличались.

«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».

Особенности

• История атак программ-вымогателей;

• Как действуют киберпреступники: их тактика, методы и процедуры;

• Как реагировать на инциденты с программами-вымогателями.

Для кого

Для студентов, изучающих системное администрирование, системных и сетевых администраторов, а также для специалистов по реагированию и аналитиков киберугроз.

Содержание

Предисловие 10
Введение 12
01. Знакомство с современными атаками с использованием программ-вымогателей 20
Глава 1 24
Глава 2 42
Конец ознакомительного фрагмента. 48

Олег Скулкин
Шифровальщики: Как реагировать на атаки с использованием программ-вымогателей

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*

* * *

Олег
Скулкин

ШИФРОВАЛЬЩИКИ

Как реагировать на атаки с использованием программ-вымогателей

Я хотел бы поблагодарить команду Group-IB, а также других коллег из различных компаний, занимающихся кибербезопасностью, чьи выдающиеся исследования всегда вдохновляют меня. Также я благодарен команде Packt за предоставленную возможность и оказанную помощь. Я крайне признателен своему техническому рецензенту Рикоху Даниельсону за его ценнейшие отзывы.

Предисловие

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

Вот уже четвертый год подряд атаки программ-вымогателей становятся одной из самых серьезных и разрушительных киберугроз. Даже киберугрозой № 1. Жертвой шифровальщиков может оказаться как гигантская международная корпорация типа концерна Toshiba или трубопровода Colonial Pipeline, так и небольшой частный бизнес. Одна-единственная успешная атака способна полностью парализовать производство и оставить компанию без денег (суммы выкупа достигают сотен миллионов долларов!) и чувствительных данных, которые злоумышленники могут предварительно выгрузить и выставить на продажу, чтобы жертва была сговорчивее. И хотя основные цели вымогателей по-прежнему располагаются в Северной и Латинской Америке, Европе, Азиатско-Тихоокеанском регионе, последние пару лет и Россия перестала считаться тихой гаванью. По данным Group-

IB, только в 2021 г. количество атак программ-вымогателей на российские компании увеличилось более чем на 200 %. В первом полугодии 2022 года в мире это количество выросло в четыре раза по сравнению с I кварталом 2021 г. Когда случаются (нечасто) аресты, вымогатели уходят на дно (ненадолго) и заметают следы, проводя ребрендинг. Но говорить о закате шифровальщиков пока очень и очень рано. Команда Лаборатории компьютерной криминалистики Group-IB начала следить за шифровальщиками, когда еще мало кто видел в них серьезную угрозу. Автор книги Олег Скулкин – знаковая фигура не только в российской, но и в международной цифровой криминалистике. Он более десяти лет работает в сфере информационной безопасности, написал и выступил соавтором пяти книг по форензике и расследованию инцидентов. Олег – постоянный автор исследований, вебинаров и технических блогов о развитии империи шифровальщиков и наиболее активных преступных групп: Conti, OldGremline, LockBit, Hive, REvil. Читатель в подробностях узнает об истории программ-вымогателей, тактиках и техниках, используемых операторами шифровальщиков, и о том, как расследовать такие атаки. Издание будет незаменимым для специалистов по цифровой криминалистике, реагированию на инциденты, проактивному поиску угроз, киберразведке, а также для профессионалов из смежных областей.

Group-IB

Введение

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

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

Для кого предназначена эта книга?

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

О чем эта книга?

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

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

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

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

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

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

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

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

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

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

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

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

Загрузите цветные изображения

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

Используемые обозначения

В этой книге используется ряд текстовых обозначений.

Код в тексте указывает на участки кода в тексте, имена таблиц базы данных, имена папок, имена файлов, расширения файлов, пути, URL-адреса, пользовательский ввод и псевдонимы Twitter, например: «Создан новый объект с GUID {E97EFF8F-1C38–433C-9715–4F53424B4887}. Кроме того, подозрительный файл 586A97.exe находится в папке C: \Windows\SYSVOL\domain\scripts».

Блок кода выглядит так.

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

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

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

Любой ввод или вывод командной строки записывается следующим образом.

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

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

Свяжитесь с нами

Мы всегда рады читательским отзывам.

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

Исправления. Мы приложили все усилия, чтобы обеспечить точность текста и данных, но ошибки случаются. Если вы нашли в книге ошибку, мы будем признательны, если вы сообщите нам об этом. Пожалуйста, заполните форму по ссылке https://www.packtpub.com/support/errata.

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

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

Отказ от ответственности

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

Поделитесь вашим мнением

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

Ваш отзыв важен для нас и для технического сообщества,

он поможет делать наш контент лучше.

01. Знакомство с современными атаками с использованием программ-вымогателей

1

РАЗДЕЛ

ЗНАКОМСТВО С СОВРЕМЕННЫМИ АТАКАМИ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

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

Этот раздел состоит из следующих глав:

Глава 1. История современных атак с использованием программ-вымогателей

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

Глава 3. Процесс реагирования на инциденты

Глава 1
История современных атак с использованием программ-вымогателей

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

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

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

Мы рассмотрим следующие примеры:

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

2016 г. – программа-вымогатель SamSam

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

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

Как правило, злоумышленники эксплуатировали уязви-

мости 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).

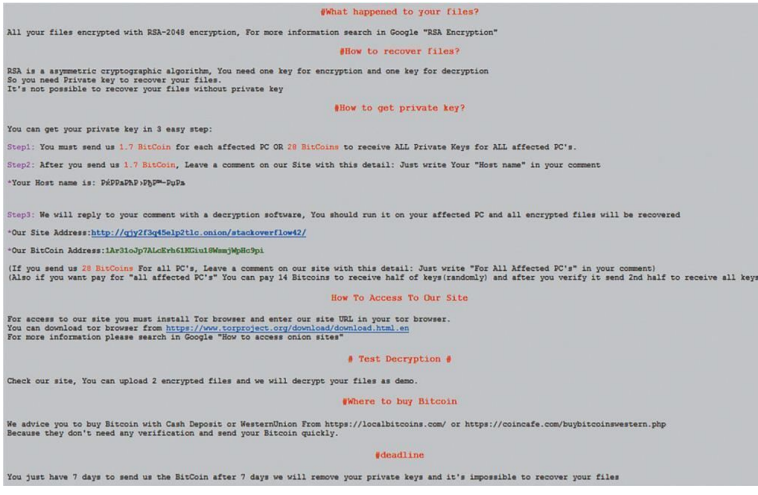

Рис. 1.1. Пример сообщения SamSam с требованием выкупа[1]

[1] #Что случилось с вашими файлами?Все ваши файлы зашифрованы с помощью алгоритма RSA-2048 – см. «RSA-шифрование» в поиске Google.#Как восстановить файлы?RSA – это асимметричный криптографический алгоритм. Вам нужен один ключ для зашифровки и другой ключ для расшифровки.Это значит, что для восстановления файлов вам нужен закрытый ключ.Без закрытого ключа восстановить файлы невозможно.#Как получить закрытый ключ?Чтобы получить закрытый ключ, выполните три простых шага.Шаг 1: отправьте нам 1,7 биткойна за каждый пораженный компьютер или 28 биткойнов за все пораженные компьютеры.Шаг 2: после того как вы отправите нам 1,7 биткойна, оставьте на нашем сайте комментарий с вашим именем хоста.* Ваш хост …Шаг 3: в ответ мы вышлем вам программу дешифрования. Вам нужно будет запустить ее на пораженном компьютере, и все зашифрованные файлы будут восстановлены.Наш сайт: …Наш биткойн-кошелек: …(Если вы отправите нам 28 биткойнов за все пораженные компьютеры, оставьте на сайте комментарий «За все пораженные компьютеры».)(Также вы можете отправить нам 14 биткойнов, получить 14 клю-

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.

чей (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 дешифрованиеВы можете скачать с нашего сайта два зашифрованных файла, и мы расшифруем их для вас.#Где купить биткойнМы советуем покупать биткойны за наличные или через Western Union у …, потому что они не требуют проверки и высылают биткойны быстро.#Крайний срокЕсли в течение семи дней вы не отправите нам биткойны, мы удалим ваши закрытые ключи и файлы будет невозможно восстановить.

Рис. 1.2. Фрагмент плаката ФБР о розыске

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

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

2017 г. – программа-вымогатель BitPaymer

Программа-вымогатель BitPaymer связана с Evil Corp –

киберпреступной группировкой, которая, как считается, имеет российское происхождение. С этим штаммом программы-вымогателя появилась еще одна тенденция атак, управляемых человеком, – **охота на крупную дичь**.

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

Чтобы получить начальный доступ к целевой сети, группа использовала свой давний инструмент – троян **Dridex**. Троян позволял злоумышленникам загружать PowerShell Empire – популярный фреймворк постэксплуатации, – чтобы перемещаться по сети и получать расширенные права доступа, в том числе с использованием Mimikatz, как делали операторы SamSam.

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

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

Рис. 1.3. Пример сообщения BitPaymer с требованием выкупа[2]

[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

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.

файла бесплатно.

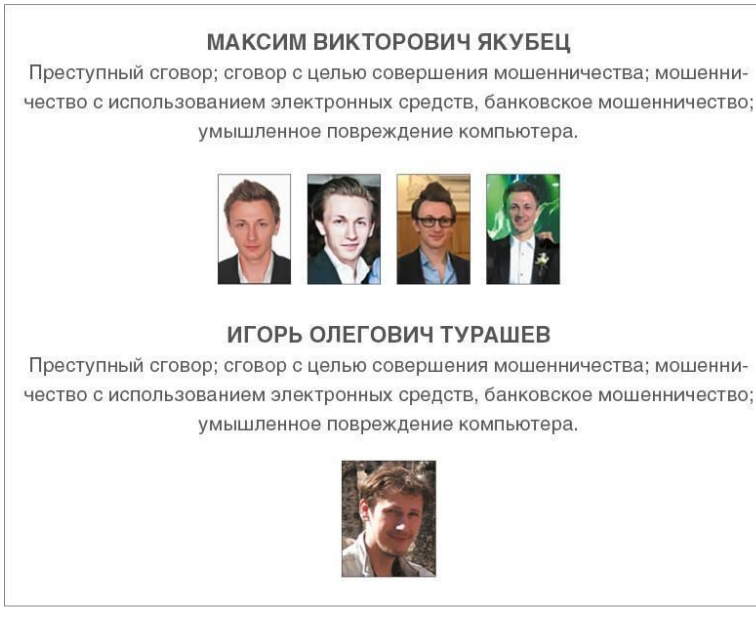

Рис. 1.4. Фрагмент плаката ФБР о розыске

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 под-

писке и номер телефона, по которому можно позвонить, чтобы отменить ее. Если жертва звонит по номеру, оператор подсказывает ей загрузить вредоносный файл Microsoft Office, открыть его и включить макросы, которые заражают компьютер трояном Bazar. Как и в случае с Trickbot, троян используется для загрузки и запуска фреймворка постэксплуатации – чаще всего Cobalt Strike.

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

Рис. 1.5. Инструкции, указанные в сообщении о выкупе[3]

Операторы программы-вымогателя Ryuk по-прежне-

[3] ИНСТРУКЦИЯ1. 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.

му 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.

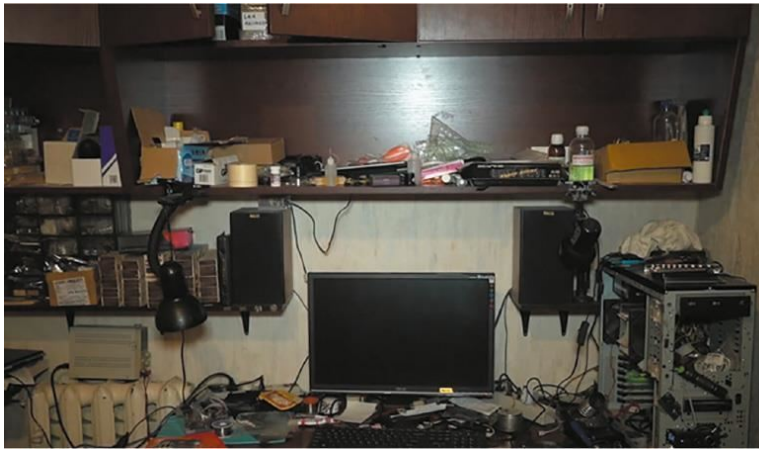

Рис. 1.6. Рабочее место операторов Emotet

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 зло-

умышленникам в обмен на процент от полученного выкупа.

REvil, **LockBit**, **Ragnar Locker**, **Nefilim –** лишь некоторые из семейств программ-вымогателей, распространяемых по модели «программа-вымогатель как услуга». И даже если несколько злоумышленников используют один и тот же тип программы-вымогателя, их тактики, техники и процедуры могут быть очень разными.

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

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

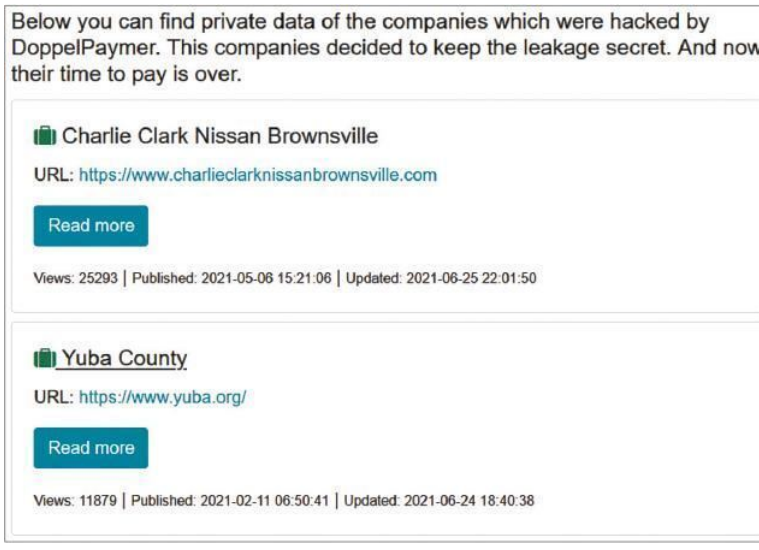

Рис. 1.7. DLS DoppelPaymer[4]

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.

[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 БраунсвиллURL-адрес:Читать далееПросмотров: 25293 / Опубликовано: 2021–05–06 15:21:06 / Обновлено: 2021–06–25 22:01:50Графство ЮбаURL-адрес:Читать далееПросмотров: 11879 / Опубликовано: 2021–02–11 06:50:41 / Обновлено: 2021–06–24 18:40:38

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 програм-

мой-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 рас-

пространенных 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 внима-

ние брокеров первоначального доступа. Вот, например, сообщение, предоставленное платформой *Threat Intelligence and Attribution*

Конец ознакомительного фрагмента.