Аналитический обзор

КАК ЭВОЛЮЦИОНИРУЮТ ВИРУСЫ-ШИФРОВАЛЬЩИКИ И СПОСОБЫ ИХ РАСПРОСТРАНЕНИЯ

group-ib.ru

GROUP IB

ОГЛАВЛЕНИЕ

Введение 3

Что такое вирусы-шифровальщики 4

Способы распространения вирусов-шифровальщиков 5

Компрометация серверов через RDP 5

Фишинговые почтовые рассылки 8

Наборы эксплойтов и другое вредоносное ПО 9

Кейс от Group-IB: заражение «GlobeImposter» 10

Рекомендации по предотвращению атак с использованием программ-вымогателей 11

TDS Polygon от Group-IB 12

Реагирование на вирусы-шифровальщики 13

О компании 14

Введение

Несмотря на то, что наиболее крупномасштабные атаки с использованием вирусов-шифровальщиков, таких как **«WannaCry», «NotPetya»** и **«Bad Rabbit»**, отгремели в 2017 году, этот вид вредоносного программного обеспечения остается одной из самых распространенных киберугроз и в 2018 году, пусть и растеряв, в некотором смысле, свой масштаб. Как и многие другие угрозы, такие программы со временем эволюционируют. Современные вирусы-шифровальщики полностью исключают возможность расшифровки данных без соответствующего криптографического ключа, а целью их распространителей становится не только запуск экземпляра вредоносной программы, но и изучение ИТ-инфраструктуры с целью дальнейшей компрометации, все чаще для шпионажа или кражи данных.

Как показывает опыт Лаборатории компьютерной криминалистики и исследования вредоносного кода Group-IB, наиболее популярным методом распространения программ-вымогателей является компрометация целевой системы путем подбора пароля к учетной записи с административными привилегиями и последующим доступом посредством RDP.

Однако, более традиционные способы распространения, такие как фишинговые почтовые рассылки, также имеют место. В частности, особую популярность получили вложения, доступ к содержимому которых защищен паролем. Наборы эксплойтов также используются злоумышленниками достаточно регулярно, в частности «RIG» и «GrandSoft».

Кроме того, нам известны случаи распространения такого программного обеспечения вредоносным ПО, для которого вымогательство не является основной целью, например, банковскими троянами.

Данный аналитический отчет раскроет некоторые технические подробности расследованных нами атак с использованием вирусов-шифровальщиков, а также представит базовые рекомендации, направленные на предотвращение таких инцидентов.

300 000+

количество зараженных WannaCry компьютеров

200+

стран пострадало от массовой атаки WannaCry

80+

компаний стали жертвами вируса-шифровальщика NotPetya

Что такое вирусы-шифровальщики?

Вирусы-шифровальщики – это тип вредоносного ПО, целью которого является модификация пользовательских файлов при помощи алгоритмов шифрования таким образом, чтобы доступ к ним не был возможен без программы-декриптора.

Такую программу, которая впоследствии может быть использована жертвой для расшифровки данных, злоумышленники предлагают в обмен на криптовалюту. Сумма определяется в файлах с инструкцией, которые создаются в результате работы ПО.

При этом в ходе коммуникаций со злоумышленниками данная сумма может быть значительно снижена.

Необходимо отметить, что целью злоумышленников далеко не всегда является получение выкупа. В нашей практике были случаи, когда распространение вирусов-шифровальщиков по скомпрометированной инфраструктуре осуществлялось для заметания следов целевой атаки.

Способы распространения вирусов-шифровальщиков

Компрометация серверов через RDP

Несмотря на свою примитивность, атаки подобного типа, по нашему опыту, стали наиболее популярными среди распространителей вирусов-шифровальщиков в 2018 году.

Многие системные администраторы оставляют RDP-порт (3389) на некоторых серверах открытым, чтобы облегчить себе работу и иметь доступ к указанным машинам в любое время и из любого места. При этом стандартная учетная запись администратора, которая, возможно, и не используется сотрудниками, не заблокирована, что значительно облегчает злоумышленникам проведение атак по перебору пароля – логин им уже известен.

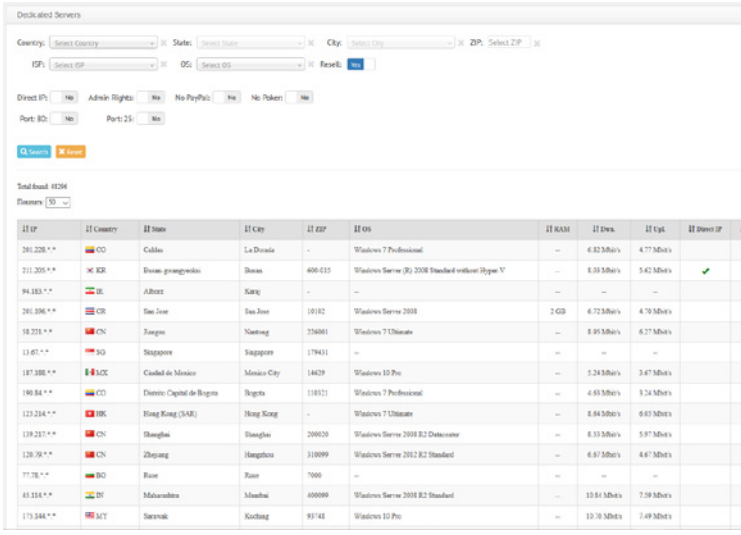
Найти такой сервер довольно просто – достаточно воспользоваться одним из специализированных поисковых сервисов, например, «Shodan».

3 500 000+ систем с доступным портом 3389

Результаты поискового запроса в Shodan

Часто распространителям программ-вымогателей не приходится даже проводить атаку по перебору паролей, чтобы получить доступ к такому серверу – все уже сделано за них. Так, например, через подпольные торговые площадки, такие как «xDedic» и «UAS RDP Shop», всего за несколько долларов можно получить доступ к одному из тысяч скомпрометированных серверов.

Как только злоумышленники получают доступ к серверу, перед ними стоит выбор: запустить программу-вымогатель сразу или попробовать распространиться по ИТ-инфраструктуре, изучить ее и запустить программу массово, а также варьировать сумму выкупа в зависимости от ценности рабочей станции или сервера. Кроме того, злоумышленники могут создать дополнительные каналы доступа, чтобы обеспечить повторную компрометацию инфраструктуры.



Доступ к серверам, выставленный на продажу на «UAS RDP Shop»

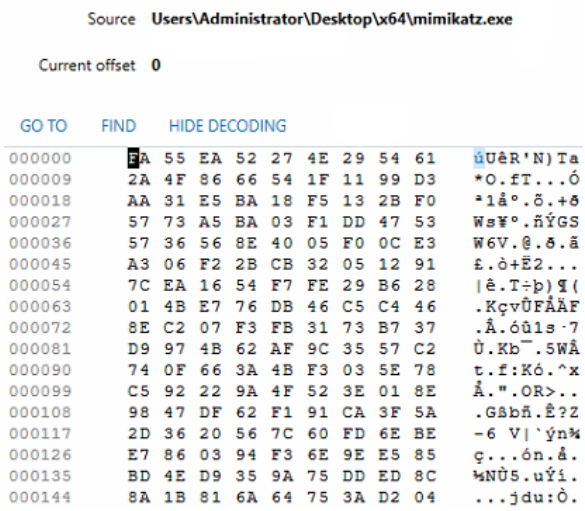
Для массового распространения и запуска вируса-шифровальщика на всех доступных системах злоумышленниками чаще всего используется **утилита «PsExec»** из пакета «Windows Sysinternals».

m.c.	4026768-128-4	C:/Windows/Prefetch/PSEXESVC.EXE-7F956DAF.pf
m.c.	185891-128-4	C:/Windows/Prefetch/DLLHOST.EXE-766398D2.pf
macb	4026871-128-4	C:/Windows/Prefetch/1007.EXE-85F7EB3C.pf
macb	4026871-48-2	C:/Windows/Prefetch/1007.EXE-85F7EB3C.pf ($FILE_NAME)

Prefetch-файлы, иллюстрирующие запуск «PsExec», за которым следует запуск «1007.exe»

Зачастую злоумышленники используют **утилиту «mimikatz»,** чтобы извлечь пароли и хеши авторизованных пользователей, хранящиеся в памяти скомпрометированного сервера, а после используют все тот же RDP, чтобы получить доступ к другим системам в сети.

Необходимо отметить, что в большинстве случаев установить факт использования данной утилиты можно лишь по имени файла, так как восстановить его оригинальное содержимое не представляется возможным ввиду шифрования.



Файл «mimikatz.exe», инфицированный вирусом-шифровальщиком

По нашим данным, посредством атак на RDP в 2018 году наиболее часто распространяли **вирус-шифровальщик «GlobeImposter»**, о котором впервые стало известно в декабре 2017 года.

Для шифрования «GlobeImposter» использует алгоритм RSA с 2048-битным ключом, часть данных которого записывается в «%AllUserProfile%\Public\» в файл с шестнадцатеричным именем. Имя генерируется на основе информации об аппаратном обеспечении целевого компьютера.

Перед началом процесса шифрования «GlobeImposter» осуществляет поиск процессов **с ключевыми словами** и потом **завершает их**.

Это позволяет шифровальщику получить доступ к базам данных «SQL», «Outlook», «PostgreSQL», «1C», а также документам «Word» и таблицам «Excel», которые были открыты в момент его запуска.

Ключевые слова

SQL Outlook SSMS 1C Postgre Excel Word

```
dd offset aSql      ; DATA XREF: sub_409F1B+2D9↓o
                    ; "sql"
dd offset aOutlook  ; "outlook"
dd offset aSsms     ; "sms"
dd offset aPostgre  ; "postgre"
dd offset a1c       ; "1c"
dd offset aExcel    ; "excel"
dd offset aWord     ; "word"
align 10h
dd 6425h            ; DATA XREF: sub_402354+EE↓o
dd 'taskkill /F /T /PID ',0
```

Поиск по ключевым словам

Чтобы исключить возможность восстановления данных и замести следы, вредоносная программа создает и запускает сценарий, который удаляет теневые копии, сведения об RDP-подключениях из реестра и каталога пользователя, а также информацию из журналов событий Windows.

Указанный сценарий будет запущен повторно по завершении процесса шифрования.

```
db '@echo off', 0Dh, 0Ah ; DATA XREF: sub_4096CB+63↓o
db 'vssadmin.exe Delete Shadows /All /Quiet', 0Dh, 0Ah
db 'reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server '
db 'Client\Default" /va /f' , 0Dh, 0Ah
db 'reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server '
db 'Client\Servers" /f'. 0Dh, 0Ah
db 'reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server '
db 'Client\Servers" '. 0Dh, 0Ah
db 'cd %userprofile%\documents\ ', 0Dh, 0Ah
db 'attrib Default.rdp -s -h', 0Dh, 0Ah
db 'for /F "tokens=*" %1 in (',27h,'wevtutil.exe el', 27h,') DO wevtut
db 'il.exe cl "%1"',0
```

Чтобы обеспечить себе повторный запуск после перезагрузки атакуемого компьютера, «GlobeImposter» создает параметр в разделе реестра «HKCU \Software\Microsoft\Windows\CurrentVersion\ RunOnce», в значение которого записывается путь к копии его исполняемого файла.

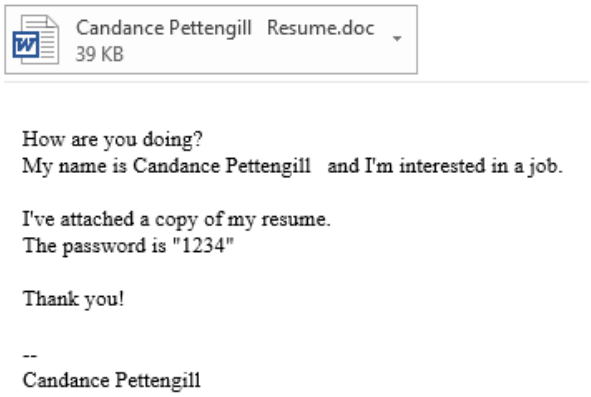
В каждый каталог с зашифрованными файлами помещается файл «how_to_back_files.html», который содержит инструкции по внесению оплаты за расшифровку файлов.

```
aSoftwareMicros:    ;DATA XREF:sub_409D43+1A↓o
                text "UTF-16LE", 'Software\Microsoft\Windows\CurrentVersion\RunOnce',0
aBrowserupdatec:    ;DATA XREF:sub_409D43+46↓o
                text "UTF-16LE", 'BrowserUpdateCheck',0
```

Фишинговые почтовые рассылки

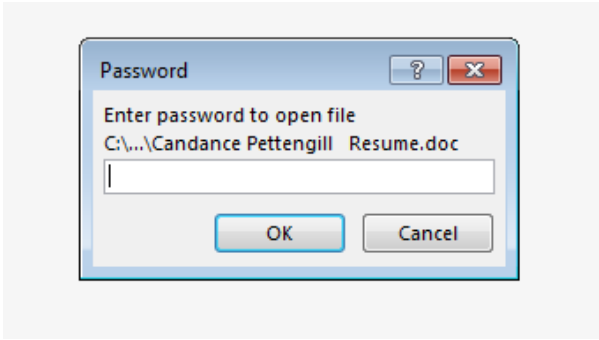
Распространение через фишинговые почтовые рассылки характерно для самых разных видов вредоносных программ, и вирусы-шифровальщики не являются исключением. В 2018 году наиболее часто таким способом распространяли «GandCrab», «GlobeImposter», «Hermes» и «Sigma». Особенную популярность среди распространителей вирусов-шифровальщиков получили документы «Microsoft Word», защищенные паролем.

Чтобы произошла загрузка и запуск вируса-шифровальщика, пользователю необходимо совершить несколько действий:

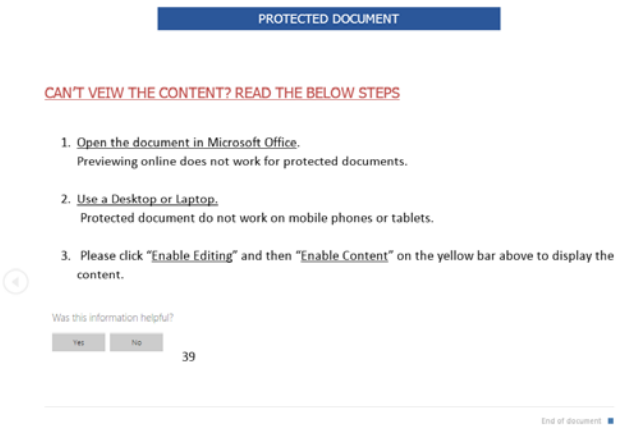


Письмо с вредоносным вложением, которое рассылалось 24 октября 2018 года.

1 **Открыть файл и ввести пароль, представленный в тексте письма**



2 **Разрешить заблокированное содержимое, что и позволит отработать макросу**



В результате его работы вирус-шифровальщик будет загружен с IP-адреса атакующих, сохранен в каталог «Temp» и запущен.

Наборы эксплойтов и другое вредоносное ПО

Для распространения некоторых семейств вирусов-шифровальщиков, например, «GandCrab», злоумышленники использовали наборы эксплойтов, причем как довольно старые, например, «GrandSoft», так и сравнительно актуальные, например, «RIG». Наборы эксплойтов позволяли распространять вирусы-шифровальщики через скомпрометированные сайты, собирая информацию о компьютере жертвы и подбирая эксплойт в соответствии с обнаруженными уязвимостями. В итоге это приводило к загрузке и запуску вредоносной программы.

Кроме того, в 2018 году некоторые известные банковские трояны, в частности «Emotet» и «Trickbot», были замечены в распространении программ-вымогателей «Ryuk» и «BitPaymer».

Данные трояны имеют модульную архитектуру, что позволяет им существенно расширять свои возможности, в том числе осуществлять распространение по сети, эксплуатируя известные уязвимости, и красть пользовательские пароли. Таким образом, атакуемая ИТ-инфраструктура может быть подвержена не только потере доступа к данным, но и стать подконтрольной злоумышленникам. Это позволит последним осуществить повторное заражение или любые другие противоправные действия, например, кражу данных.

Кейс от Group-IB: Заражение «GlobeImposter»

Профиль клиента

Крупная компания-застройщик, в ИТ-инфраструктуру которой входит более 400 рабочих станций и серверов.

Ситуация:

Получив доступ к одному из серверов компании посредством RDP и аутентификационные данные учетной записи с административными привилегиями, злоумышленники распространили вирус-шифровальщик «GlobeImposter». При этом, на некоторых серверах, на которых указанное вредоносное ПО запущено не было, злоумышленники установили «TeamViewer» - ПО для удаленного управления.

Действия:

В ходе реагирования на инцидент специалисты Лаборатории компьютерной криминалистики Group-IB установили скомпрометированный сервер, являвшийся начальной точкой распространения вредоносного ПО, все инфицированные рабочие станции и сервера. Также, благодаря криминалистическому экспресс-анализу, были обнаружены сервера, на которых злоумышленники установили ПО для удаленного управления.

Результат:

- Заказчик получил исчерпывающую информацию об инциденте, которая позволила ему обеспечить защиту от подобных угроз.
- Правильное реагирование на инцидент позволило полностью отрезать злоумышленников от инфраструктуры и не допустить утечки конфиденциальной информации и повторного заражения.
- Заказчик получил подробные рекомендации по улучшению информационной безопасности своей ИТ-инфраструктуры.

Рекомендации по предотвращению атак с использованием программ-вымогателей

1. Осуществлять доступ к серверам по RDP только с использованием VPN.
2. Если обеспечить доступ через VPN не представляется возможным, внедрить мультифакторную аутентификацию.
3. Осуществлять блокировку учетной записи после определенного количества неудачных попыток входа за короткий промежуток времени.
4. Обеспечить сложность пароля учетной записи, использующейся для доступа по RDP, регулярно осуществлять его смену.
5. Использовать NLA (аутентификацию на сетевом уровне) для RDP-соединений.
6. Включить поддержку TLS (протокол защиты транспортного уровня) для RDP-соединений.
7. Изменить порт по умолчанию (3389).
8. Ограничить список IP-адресов, с использованием которых может быть осуществлены RDP-подключения.
9. Внедрить антиспам и антифишинг фильтры.
10. Регулярно обновлять средства антивирусной защиты, а также проводить аудит журналов их работы.
11. Внедрить решение класса «sandbox» для обнаружения вредоносных программ, не детектируемых антивирусным ПО.
12. Осуществлять своевременное обновление операционных систем и прикладного программного обеспечения.

THF Polygon от Group-IB

Предотвращение заражения вирусом-шифровальщиком

THF Polygon – технология поведенческого анализа файлов в изолированной среде. Эффективное обнаружение ранее неизвестного вредоносного кода, не определяемого антивирусами и сигнатурным подходом.

В режиме inline автоматически блокирует вредоносные объекты в почтовых рассылках и при скачивании по ссылкам, предотвращая заражение и потерю данных.

Будьте на шаг впереди злоумышленников

Благодаря 15-летней практике расследований и реагирования мы знаем, как меняются инструменты атакующих, и адаптируем технологии для эффективной защиты

Синергия с собственной системой Threat Intelligence позволяет получать уникальные данные о новых угрозах и оперативно обновлять правила детектирования

Group-IB Threat Intelligence & Attribution входит в отчеты ведущих аналитических агентств

IDC | GARTNER
FORRESTER

Как работает THF Polygon

Извлечение объектов

- Почтовые вложения
- Файлы из трафика
- Ссылки

Запуск в изолированной среде

- Реалистичная эмуляция пользовательской среды
- Противодействие техникам обхода песочниц

Поведенческий анализ

Детальный анализ и автоматическое определение вредоносной активности на основании поведенческих маркеров

Подробный отчет

Сетевая активность объекта, дерево процессов, видео и т.д

Новые индикаторы

Дополнительные индикаторы для поиска других признаков компрометации и эффективного реагирования

Мгновенная блокировка
вредоносного объекта в режиме inline

Подробное уведомление
с рекомендациями по реагированию в режиме monitoring

Узнать больше о Threat Hunting Framework

group-ib.ru/thf

Реагирование на инциденты, связанные с распространением вирусов-шифровальщиков

В большинстве случаев восстановить доступ к данным после заражения вирусом-шифровальщиком без программы-декриптора невозможно. При этом, торопиться платить выкуп злоумышленникам не рекомендуется.

Специалисты Group-IB считают, что правильное реагирование на атаки с использованием таких вредоносных программ имеет критическое значение.

Профессиональное реагирование на атаки с использованием вирусов-шифровальщиков позволяет:

- **Минимизировать ущерб;**
- **Установить начальную точку компрометации, выявить цепочку заражения, чтобы локализовать инцидент и не допустить его повторения;**
- **Собрать информацию, необходимую для составления списка индикаторов компрометации;**
- **Собрать доказательную базу, а также требуемые для проведения расследования сведения;**
- **Получить рекомендации по улучшению безопасности инфраструктуры и персонала.**

Этапы реагирования на инцидент от Group-IB

1 Анализ сетевой активности

Внедрение HUNTBOX, что позволяет команде реагирования:

- **Осуществлять мониторинг сетевого трафика;**
- **Выявлять подозрительные коммуникации, обнаружение которых недоступно системам обеспечения информационной безопасности, основанным на сигнатурном анализе;**
- **Производить анализ и блокировку данных на конечных устройствах.**

2 Криминалистический анализ

Проводится криминалистический экспресс-анализ рабочих станций и серверов, задействованных злоумышленниками в ходе компрометации ИТ-инфраструктуры, чтобы установить:

- **С чего началась компрометация;**
- **Как атакующие осуществляли перемещение по сети;**
- **Какие инструменты были ими использованы;**
- **Какие уязвимости были проэксплуатированы.**

3 Анализ вредоносного кода

Специалисты Лаборатории компьютерной криминалистики Group-IB проводят базовый и продвинутый статический и динамический анализ обнаруженных в ходе реагирования образцов вредоносного кода, что позволяет:

- **Быстро и эффективно обнаружить его следы;**
- **Не допустить его закрепления в системах, а также повторного заражения инфраструктуры;**
- **Обезвредить уже распространившиеся и закрепившиеся угрозы.**

По итогам работ эксперты Group-IB подробно описывают инцидент в отчете и готовят свод рекомендаций по улучшению безопасности инфраструктуры, что позволит свести к минимуму возможность возникновения подобных инцидентов в будущем.

О компании Group-IB

Group-IB – один из ведущих мировых разработчиков решений для детектирования и предотвращения кибератак, выявления фрода и защиты интеллектуальной собственности в сети.

17 лет практического опыта	**1200+** расследований по всему миру	**$300 млн** было возвращено клиентам благодаря нашей работе	**300+** специалистов и разработчиков

Многолетний опыт Group-IB воплощен в системе раннего обнаружения киберугроз – линейке высокотехнологичных продуктов для мониторинга, выявления и предупреждения киберугроз, основанной на самых актуальных данных кибербразведки и глубоком анализе реальных хакерских атак.

Наши продукты

- **Threat Intelligence & Attribution**
- **Threat Hunting Framework**
- **Digital Risk Protection**
- **Fraud Hunting Platform**

INTERPOL | EUROPOL

Официальный партнёр EUROPOL и INTERPOL

IDC | GARTNER | FORRESTER

Threat Intelligence от Group-IB – в числе лучших мировых систем согласно рейтингам IDC, Gartner, Forrester

OSCE

Рекомендована Организацией по Безопасности и Сотрудничеству в Европе

Аудит и Оценка рисков

- Тестирование на проникновение
- Исследование уязвимостей
- Выявление фактов компрометации
- Имитация целевых атак (Red Teaming)
- Проверка готовности к реагированию на инциденты (Pre-IR)
- Оценка соответствия

Threat Hunting и Реагирование

- Проактивное выявление угроз
- 24/7 мониторинг и реагирование
- Реагирование “по подписке” *(целевые атаки, утечки и др.)*

Криминалистика

- Криминалистическое исследование
- Анализ вредоносного кода

Расследования

- Целевые атаки
- Инциденты информационной безопасности
- Финансовые и корпоративные преступления

Свяжитесь с нами, чтобы узнать больше

+7 (495) 984 33 64 info@group-ib.ru www.group-ib.ru

GROUP-IB