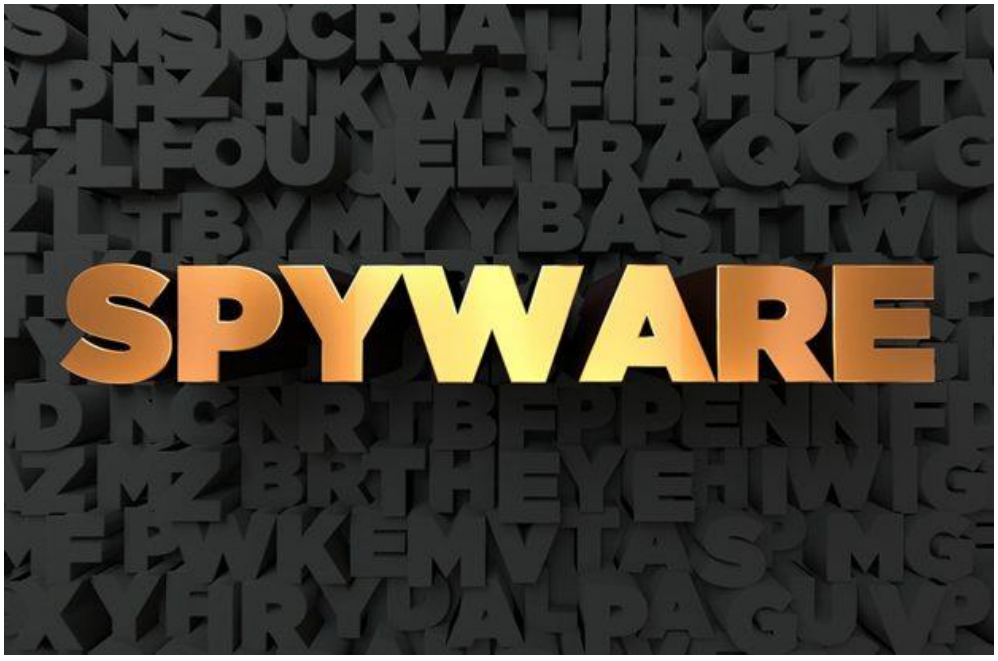
АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Новая операция кибершпионажа FinFisher: атаки MitM на уровне провайдера?

21 сентября 2017 года

ESET выявила новые операции с применением шпионской программы FinFisher, также известной как FinSpy, некогда продаваемой правительственным структурам по всему миру. Помимо технических доработок FinFisher, зафиксирован новый, ранее неизвестный вектор заражения, указывающий на возможное участие в схеме крупного интернет-провайдера (ISP).

У FinFisher широкий набор возможностей для слежки через веб-камеру и микрофон, а также функции кейлоггинга и кражи файлов. Что отличает FinFisher от других инструментов слежки, так это противоречивая информация о его внедрении. FinFisher позиционируют как инструмент правоохранительных органов, считается, что он используется диктатурами. Мы обнаружили последние версии FinFisher в семи странах. Назвать их, к сожалению, не сможем, чтобы никого не подвергать опасности.



Заражение целей

В кампаниях FinFisher используют различные механизмы заражения, включая целевой фишинг, установку вручную при наличии физического доступа к устройствам, уязвимости нулевого дня и watering hole атаки – заражение сайтов, которые предположительно посещают потенциальные жертвы (схема использовалась для распространения мобильной версии FinFisher).

Новое и наиболее тревожное в последних кампаниях FinFisher – появление схемы man-in-the-middle, где указанный «man» с большой долей вероятности находится на уровне интернет-

провайдера. Мы видели использование этого вектора в двух странах, где обнаружена последняя версия FinFisher (в остальных пяти странах используются традиционные векторы заражения).

Когда пользователь (объект слежки) собирается скачать одно из популярных легитимных приложений, его перенаправляют на версию программы, зараженную FinFisher. Мы видели троянизированные версии WhatsApp, Skype, Avast, WinRAR, VLC Player и некоторых других программ. Важно отметить, что теоретически таким образом можно использовать любое легитимное приложение.

Атака начинается, когда пользователь ищет на легитимных сайтах одно из упомянутых приложений. Когда он нажимает на ссылку для скачивания, его браузер получает модифицированную ссылку, которая перенаправляет его на троянизированный установщик, размещенный на сервере атакующих. После скачивания и исполнения на устройстве пользователя появится не только легитимное приложение, но и шпионское ПО FinFisher.

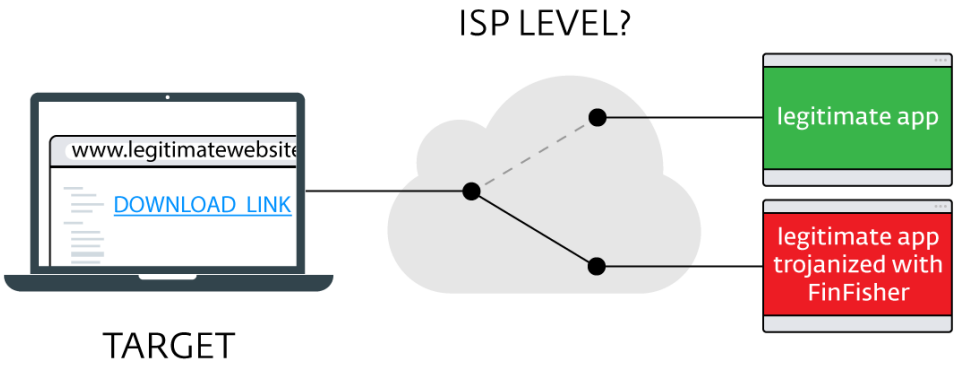


Рисунок 1. Механизм заражения последними версиями FinFisher

Переадресация осуществляется путем подмены легитимной ссылки вредоносной.

Модифицированная вредоносная ссылка доставляется в браузер пользователя с помощью кода ответа на статус перенаправления HTTP 307 Temporary Redirect (запрошенное содержимое временно перемещено по новому адресу). Процесс переадресации невидим для пользователя.

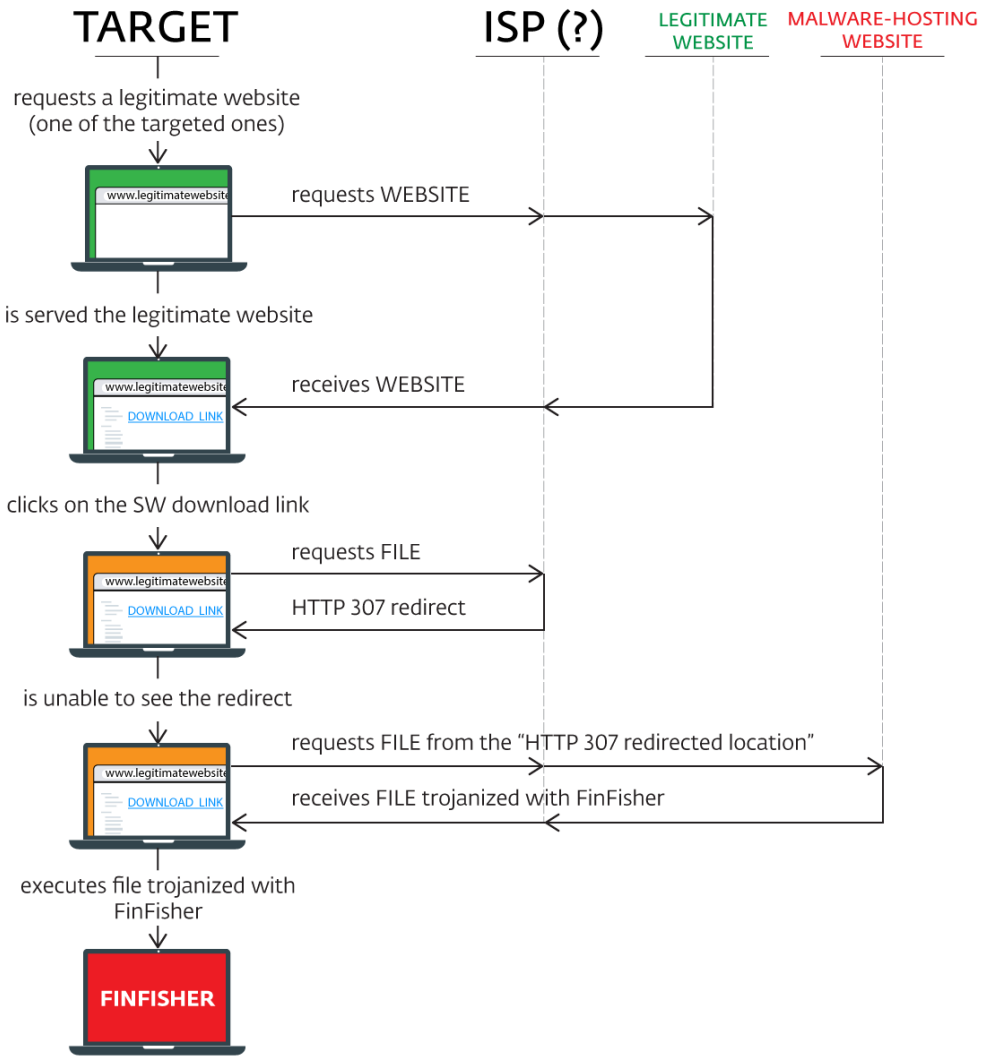


Рисунок 2. Детальное описание механизма заражения

FinFisher: работа вне зоны видимости

Последняя версия FinFisher была технически улучшена, авторы сфокусировались на обеспечении скрытности. Шпионское ПО использует кастомную виртуализацию кода для защиты большинства компонентов, включая драйвер, работающий в режиме ядра. Кроме того, в коде предусмотрены приемы анти-дизассемблирования. Мы обнаружили в FinFisher анти-отладочные, анти-эмуляционные и анти-виртуализационные приемы.

После преодоления первого уровня защиты (анти-дизассемблирование), следующий уровень — виртуализация кода. В диспетчере виртуальной машины 34 обработчика; почти все исполнение шпионского ПО производится в интерпретаторе, что добавляет еще один уровень защиты, с которым придется иметь дело в ходе анализа.

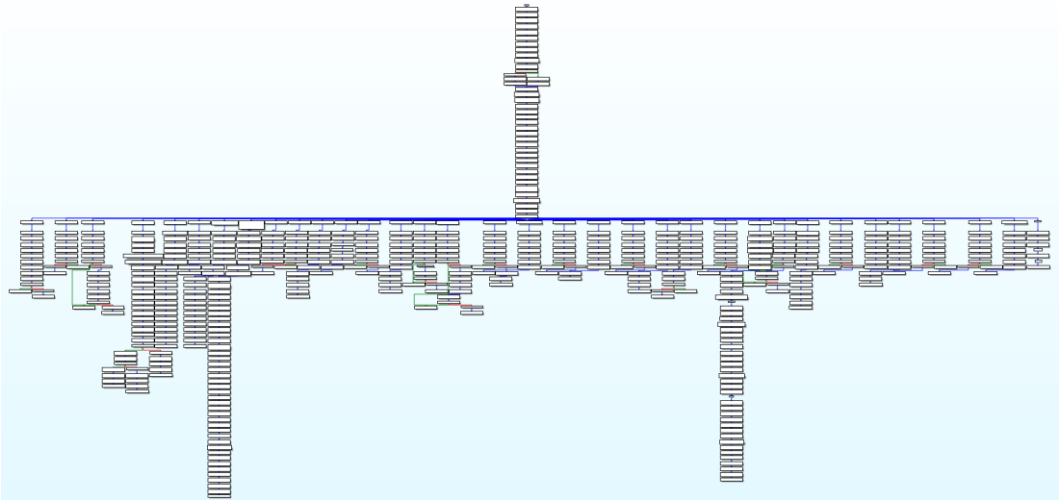


Рисунок 3. Визуализация многочисленных обработчиков, затрудняющих анализ кода

В следующем отчете мы представим более детальный технический анализ последней версии FinFisher.

Особый подход к пользователям, заинтересованным в конфиденциальности

В ходе анализа недавних кампаний мы обнаружили интересный образец – FinFisher, замаскированный под исполняемый файл под названием Threema. Он может быть использован для атак на пользователей, обеспокоенных вопросами приватности, – легитимное приложение Threema обеспечивает безопасный обмен мгновенными сообщениями со сквозным шифрованием. Есть некая ирония в том, что пользователь, стремящийся к конфиденциальности, своими руками загружает файл и запускает процесс слежки.

Акцент на пользователей, интересующихся шифрованием, не ограничивается мессенджерами. В ходе исследования мы обнаружили установочный файл, зараженный FinFisher, в некогда очень популярном ПО для шифрования диска TrueCrypt.

Кто он – man-in-the-middle?

Технически можно предположить, что man-in-the-middle участвует в атаке на одном из этапов пути от целевого компьютера до легитимного сервера (как вариант, это может быть скомпрометированная точка Wi-Fi). Однако географическое распределение последних версий FinFisher, обнаруженных ESET, позволяет предположить, что атаки MitM производятся на более высоком уровне, и наиболее вероятный вариант – участие интернет-провайдера (ISP).

Это предположение подтверждает ряд фактов. Во-первых, согласно утекшим в сеть материалам, опубликованным WikiLeaks, разработчик FinFisher предлагал решение под названием «FinFly ISP» для развертывания в сетях ISP с функциями, напоминающими те, что нужны для атак MitM. Во-вторых, способ заражения (переадресация HTTP 307) применяется идентичным образом в обеих странах, где происходило заражение. Маловероятно, что данные схемы разработаны и/или предоставлены разными источниками. В-третьих, все пораженные цели в пределах страны используют услуги одного интернет-провайдера. Наконец, тот же метод и

формат переадресации используется провайдерами для фильтрации интернет-контента как минимум в одной из этих стран.

Использование техники MitM на уровне провайдера, о котором говорится в утекшем в сеть документе, до сих пор нигде не обнаруживалось – до сегодняшнего дня. Если эта информация подтвердится, новые атаки с FinFisher – начало новых, беспрецедентных по техникам, методам и охвату операций кибершпионажа.

Мой компьютер заражен?

Все продукты ESET обнаруживают и блокируют эту угрозу как Win32/FinSpy.AA и Win32/FinSpy.AB. При помощи ESET Online Scanner вы можете проверить компьютер на наличие угрозы и удалить ее при обнаружении. Пользователи ESET защищены автоматически.

Индикаторы компрометации

Имена обнаружения ESET:
Win32/FinSpy.AA
Win32/FinSpy.AB

Переадресация:
HTTP/1.1 307 Temporary Redirect\r\nLocation:\r\nConnection: close\r\n\r\n

Список адресов URL, обнаруженных в процессе исследования:
hxxp://108.61.165.27/setup/TrueCrypt-7.2.rar
hxxp://download.downloading.shop/pcdownload.php?a=dad2f8ed616d2bfe2e9320a821f0ee39
hxxp://download.downloading.shop/pcdownload.php?a=84619b1b3dc8266bc8878d2478168baa
hxxp://download.downloading.shop/pcdownload.php?a=ddba855c17da36d61bcab45b042884be
hxxp://download.downloading.shop/pcdownload.php?a=d16ef6194a95d4c8324c2e6673be7352
hxxp://download.downloading.shop/pcdownload.php?a=95207e8f706510116847d39c32415d98
hxxp://download.downloading.shop/pcdownload.php?a=43f02726664a3b30e20e39eb866fb1f8
hxxp://download.downloading.shop/pcdownload.php?a=cb858365d08ebfb029083d9e4dcf57c2
hxxp://download.downloading.shop/pcdownload.php?a=8f8383592ba080b81e45a8913a360b27
hxxp://download.downloading.shop/pcdownload.php?a=e916ba5c43e3dd6adb0d835947576123
hxxp://download.downloading.shop/pcdownload.php?a=96362220acc8190dcd5323437d513215
hxxp://download.downloading.shop/pcdownload.php?a=84162502fa8a838943bd82dc936f1459
hxxp://download.downloading.shop/pcdownload.php?a=974b73ee3c206283b6ee4e170551d1f7
hxxp://download.downloading.shop/pcdownload.php?a=cd32a3477c67defde88ce8929014573d
hxxp://download.downloading.shop/pcdownload.php?a=36a5c94ffd487ccd60c9b0db4ae822cf
hxxp://download.downloading.shop/pcdownload.php?a=0ebb764617253fab56d2dd49b0830914
hxxp://download.downloading.shop/pcdownload.php?a=f35e058c83bc0ae6e6c4dffa82f5f7e7
hxxp://download.downloading.shop/pcdownload.php?a=64f09230fd56149307b35e9665c6fe4c
hxxp://download.downloading.shop/pcdownload.php?a=b3cc01341cb00d91bcc7d2b38cedc064
hxxp://download.downloading.shop/pcdownload.php?a=5fc0440e395125bd9d4c318935a6b2b0
hxxp://download.downloading.shop/pcdownload.php?a=5ca93ad295c9bce5e083faab2e2ac97a
hxxp://download.downloading.shop/pcdownload.php?a=f761984bb5803640aff60b9bc2e53db7
hxxp://download.downloading.shop/pcdownload.php?a=5ca93ad295c9bce5e083faab2e2ac97a
hxxp://download.downloading.shop/pcdownload.php?a=514893fa5f3f4e899d2e89e1c59096f3
hxxp://download.downloading.shop/pcdownload.php?a=a700af6b8a49f0e1a91c48508894a47c
hxxp://download.downloading.shop/pcdownload.php?a=36a5c94ffd487ccd60c9b0db4ae822cf

hxxp://download.downloading.shop/pcdownload.php?a=a700af6b8a49f0e1a91c48508894a47c
hxxp://download.downloading.shop/pcdownload.php?a=395ce676d1ebc1048004daad855fb3c4
hxxp://download.downloading.shop/pcdownload.php?a=cd32a3477c67defde88ce8929014573d
hxxp://download.downloading.shop/pcdownload.php?a=49d6d828308e99fede1f79f82df797e9
hxxp://download.downloading.shop/pcdownload.php?a=d16ef6194a95d4c8324c2e6673be7352

Образцы (SHA-1)
ca08793c08b1344ca67dc339a0fb45e06bdf3e2f
417072b246af74647897978902f7d903562e0f6f
c4d1fb784fcd252d13058dbb947645a902fc8935
e3f183e67c818f4e693b69748962eecda53f7f88
d9294b86b3976ddf89b66b8051ccf98cfae2e312
a6d14b104744188f80c6c6b368b589e0bd361607
417072b246af74647897978902f7d903562e0f6f
f82d18656341793c0a6b9204a68605232f0c39e7
df76eda3c1f9005fb392a637381db39cceb2e6a8
5f51084a4b81b40a8fcf485b0808f97ba3b0f6af
4b41f36da7e5bc1353d4077c3b7ef945ddd09130
1098ba4f3da4795f25715ce74c556e3f9dac61fc
d3c65377d39e97ab019f7f00458036ee0c7509a7
c0ad9c242c533effd50b51e94874514a5b9f2219
a16ef7d96a72a24e2a645d5e3758c7d8e6469a55
c33fe4c286845a175ee0d83db6d234fe24dd2864
cfa8fb7c9c3737a8a525562853659b1e0b4d1ba8
9fc71853d3e6ac843bd36ce9297e398507e5b2bd
66eccea3e8901f6d5151b49bca53c126f086e437
400e4f843ff93df95145554b2d574a9abf24653f
fb4a4143d4f32b0af4c2f6f59c8d91504d670b41
f326479a4aacc2aaf86b364b78ed5b1b0def1fbe
275e76fc462b865fe1af32f5f15b41a37496dd97
df4b8c4b485d916c3cadd963f91f7fa9f509723f