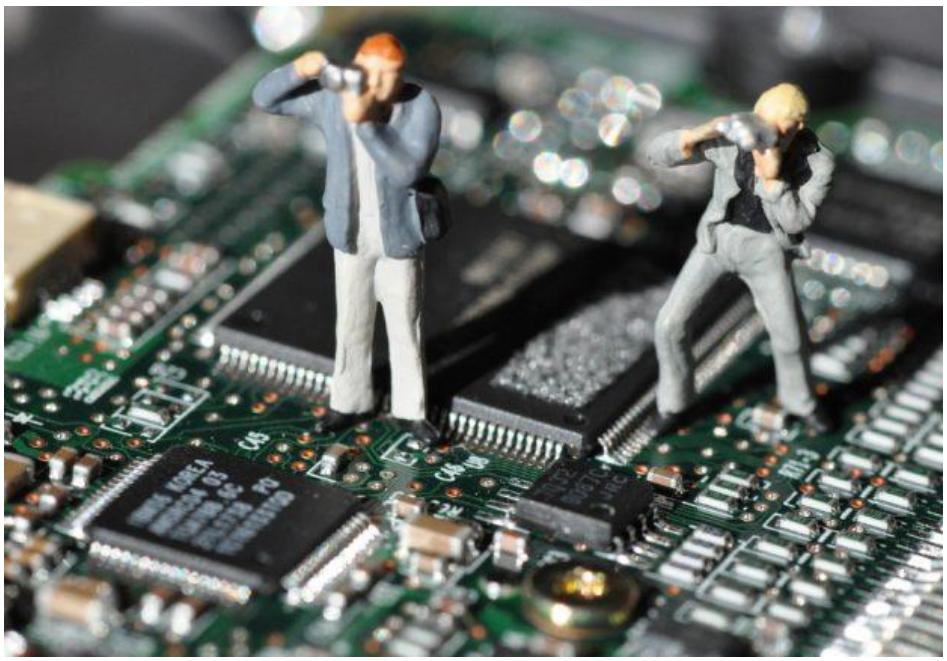
АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Новая спайварь StrongPity2 сменила FinFisher в кампании кибершпионажа с возможным участием интернет-провайдера

12 декабря 2017 года

Продолжая исследование операции кибершпионажа с явными следами участия в схеме крупного интернет-провайдепра, мы обнаружили, что известное шпионское ПО FinFisher (FinSpy) сменила другая программа. Антивирусные продукты ESET детектируют новую спайварь как Win32/StrongPity2, она заметно напоминает программу, авторство которой приписывают кибергруппе StrongPity. Все продукты ESET, включая бесплатный инструмент ESET Online Scanner, детектируют и блокируют угрозу, а также устраняют StrongPity2 из скомпрометированной системы.



Как мы писали в сентябре, в кампаниях, зафиксированных в двух странах мира, для распространения FinFisher использовались атаки man-in-the-middle. В большинстве случаев упомянутый «man» с большой долей вероятности находится на уровне интернет-провайдера. По данным телеметрии ESET, кампании были прекращены 21 сентября 2017 года – в день публикации нашего отчета.

8 октября в одной из двух стран стартовала идентичная кампания, использующая ту же самую (причем довольно необычную) структуру перенаправлений HTTP для переадресации браузеров «на лету», только теперь вместо FinFisher распространялся Win32/StrongPity2. Мы изучили новое шпионское ПО и обнаружили сходство с программой, которую в прошлом предположительно использовала группа StrongPity.

Первое сходство – сценарий атаки. Пользователь, который пытается загрузить легитимное ПО, перенаправляется на поддельный сайт, с которого загружается троянизированная версия нужного софта. Подобные watering hole атаки в исполнении группы StrongPity были зафиксированы летом

2016 года, их целью выступали преимущественно итальянские и бельгийские пользователи программ для шифрования.

В ходе исследования мы обнаружили зараженные Win32/StrongPity2 версии следующих программ:

- CCleaner v 5.34
- Driver Booster
- The Opera Browser
- Skype
- The VLC Media Player v2.2.6 (32bit)
- WinRAR 5.50

С начала кампании наши системы телеметрии зафиксировали больше ста попыток атак с использованием Win32/StrongPity2.

Мы обнаружили и другие сходства между спайварью группы StrongPity и реализацией Win32/StrongPity2:

- идентичные фрагменты кода
- структуры конфигурационных файлов (довольно необычные) имеют заметные сходства, как показано на рисунке 1:

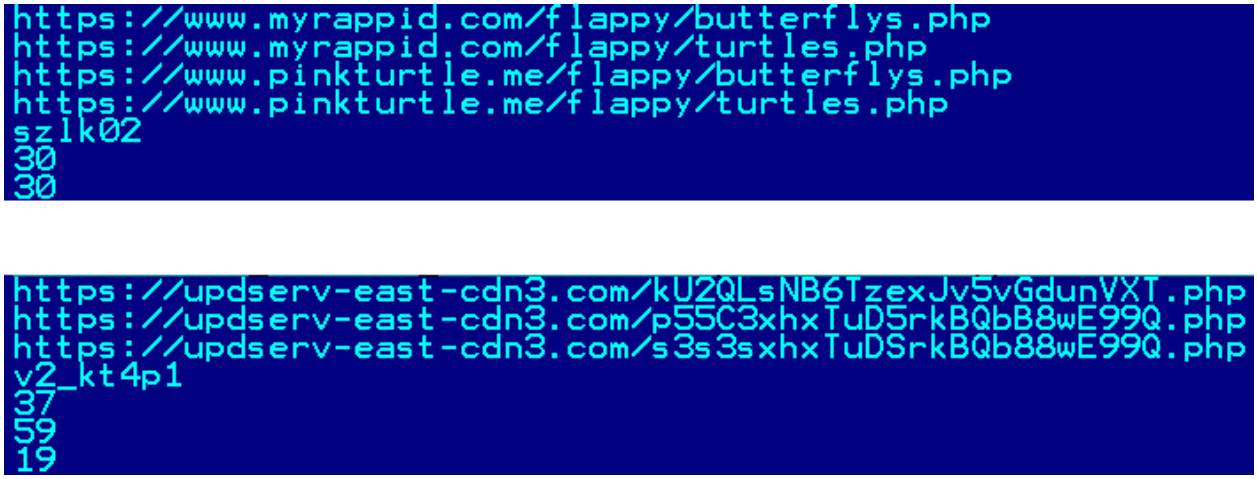


Рисунок 1. Образцы конфигурационных файлов: сверху StrongPity, внизу StrongPity2

- в StrongPity и StrongPity2 используется один и тот же алгоритм шифрования (очень необычный Byte ^= ((Byte & 0xF0) >> 4)
- в обеих программах используется идентичная (старая) версия `libcurl` 7.45
- обе программы используют один и тот же способ эксфильтрации файлов (основная полезная нагрузка производит эксфильтрацию файлов, предварительно собранных и сохраненных специальным модулем)

Если говорить о краже данных, под прицелом Win32/StrongPity2 несколько типов файлов:

- .ppt
- .pptx
- .xls
- .xlsx
- .txt
- .doc
- .docx

- .pdf
- .rtf

В поисках этих файлов программа избегает следующих папок:

- "%Windows%"
- "%Windows.old%"
- "%AppData%"
- "%Program Files%"
- "%Program Files (x86)%"
- "%ProgramData%"

В дополнение к эксфильтрации данных Win32/StrongPity2 может загружать и выполнять другие вредоносные программы по выбору атакующих с привилегиями скомпрометированной учетной записи.

Как проверить систему на предмет компрометации, удалить вредоносную программу и предотвратить заражение

Чтобы проверить систему на предмет заражения Win32/StrongPity2, используйте бесплатный ESET Online Scanner. Обнаружив Win32/StrongPity2, сканер удалит его.

Систему можно проверить вручную. Для этого нужно проверить наличие/отсутствие папки `%temp%\lang_be29c9f3-83we`, которую вредоносная программа создает для хранения своих компонентов, основной из которых – файл `wmpsvn32.exe`.

Еще один индикатор заражения, который легко проверить, – строковой параметр реестра, расположенный в `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, под названием `Help Manager` со строкой `%temp% \lang_be29c9f3-83we\wmpsvn32.exe` в поле данных:

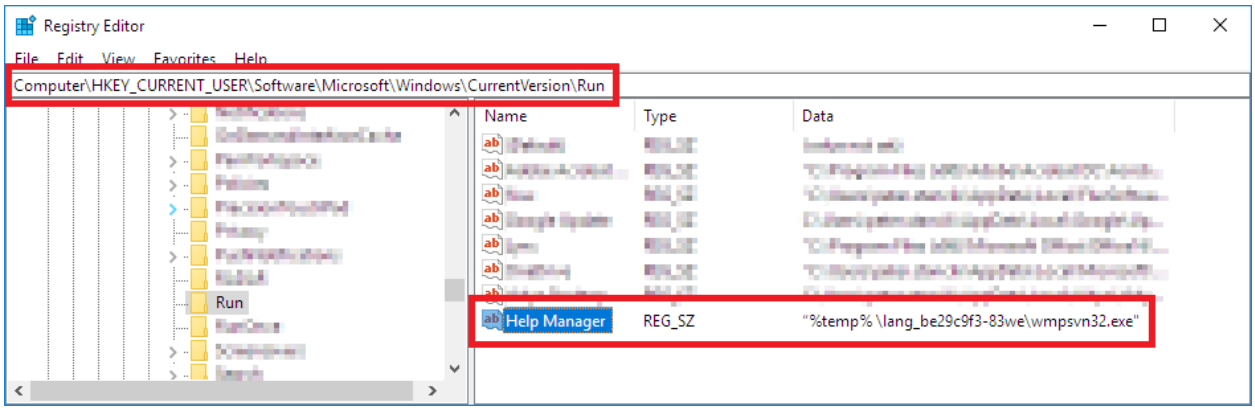


Рисунок 2. Запись реестра, используемая вредоносным ПО

Для очистки зараженной системы вручную нужно выполнить следующие действия:

1. Устранить основной процесс компонента `wmpsvn32.exe`
2. Удалить папку `%temp%\lang_be29c9f3-83we` и все ее содержимое
3. Удалить значение Help Manager в упомянутой записи реестра

Для профилактики заражения рекомендуем использовать комплексные решения для безопасности.

Индикаторы заражения

Хеши изученных образцов:

```
4ad3ecc01d3aa73b97f53e317e3441244cf60cbd
8b33b11991e1e94b7a1b03d6fb20541c012be0e3
49c2bcae30a537454ad0b9344b38a04a0465a0b5
e17b5e71d26b2518871c73e8b1459e85fb922814
76fc68607a608018277afa74ee09d5053623ff36
87a38a8c357f549b695541d603de30073035043d
9f2d9d2131eff6220abaf97e2acd1bbb5c66f4e0
f8009ef802a28c2e21bce76b31094ed4a16e70d6
a0437a2c8c50b8748ca3344c38bc80279779add7
```

Домен, использующийся для загрузки троянизированного Win32/StrongPity2 софта:

```
hxxps://downloading.internetdownloading.co
```

URL, используемые для эксфильтрации украденных данных:

```
hxxps://updserv-east-cdn3.com/s3s3sxhxTuDSrkBQb88wE99Q.php
hxxps://updserv-east-cdn3.com/kU2QLsNB6TzexJv5vGdunVXT.php
hxxps://updserv-east-cdn3.com/p55C3xhxTuD5rkBQbB8wE99Q.php
```

Папка, создаваемая Win32/StrongPity2 для хранения своих компонентов:

```
%temp%\lang_be29c9f3-83we
```