АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Новая атака шифратора Shade нацелена на российских бизнес-пользователей

29 января 2019 года

В январе 2019 года мы зафиксировали резкий рост числа обнаружений вредоносных почтовых вложений JavaScript (в 2018 году данный вектор атаки использовался минимально). В «новогоднем выпуске» можно выделить рассылку на русском языке, предназначенную для распространения шифратора Shade (он же Troldesh), который детектируется продуктами ESET как Win32/Filecoder.Shade.

Похоже, что эта атака продолжает спам-кампанию по распространению шифратора Shade, обнаруженную в октябре 2018 года.

Новая кампания Shade

По данным нашей телеметрии, октябрьская кампания шла в постоянном темпе до второй половины декабря 2018 года. Далее последовал перерыв на Рождество, а затем в середине января 2019 года активность кампании удвоилась (см. график ниже). Падения на графике, соответствующие выходным дням, говорят о том, что атакующие предпочитают корпоративные адреса электронной почты.

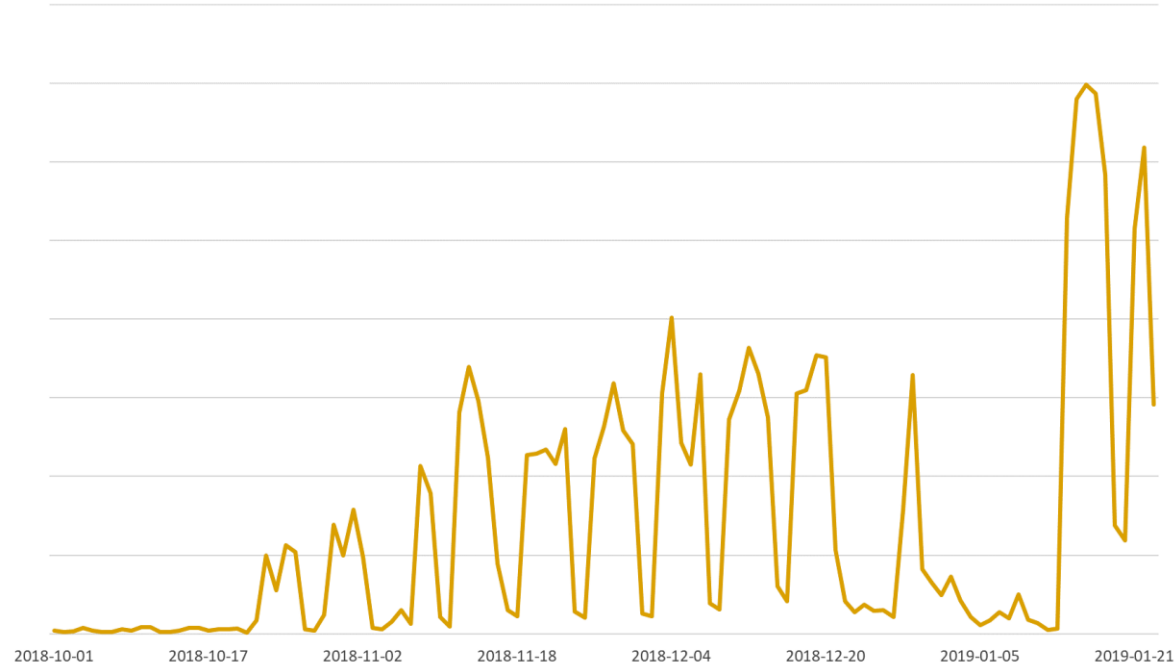

Рисунок 1. Детектирование вредоносных вложений JavaScript, распространяющих Win32/Filecoder.Shade с октября 2018 года

Как упоминалось ранее, кампания иллюстрирует тренд, который мы наблюдаем с начала 2019 года, – возвращение вредоносных JavaScript-вложений в качестве вектора атаки. Динамика отображена на графике ниже.

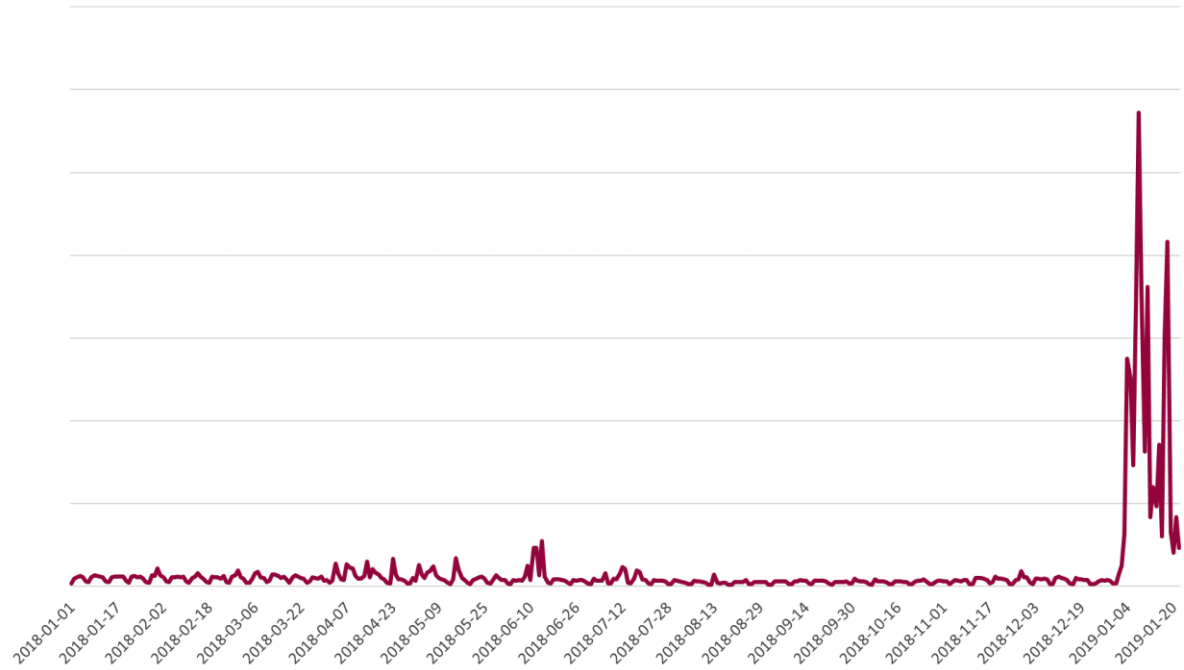

Рисунок 2. Обнаружение вредоносных JavaScript, распространяемых во вложениях электронной почты с 2018 года. Вложения детектируются ESET как JS/Danger.ScriptAttachment

Стоит отметить, что кампания по распространению шифратора Shade наиболее активна в России, на которую приходится 52% от общего числа обнаружений вредоносных вложений JavaScript. В числе прочих пострадавших – Украина, Франция, Германия и Япония, как показано ниже.

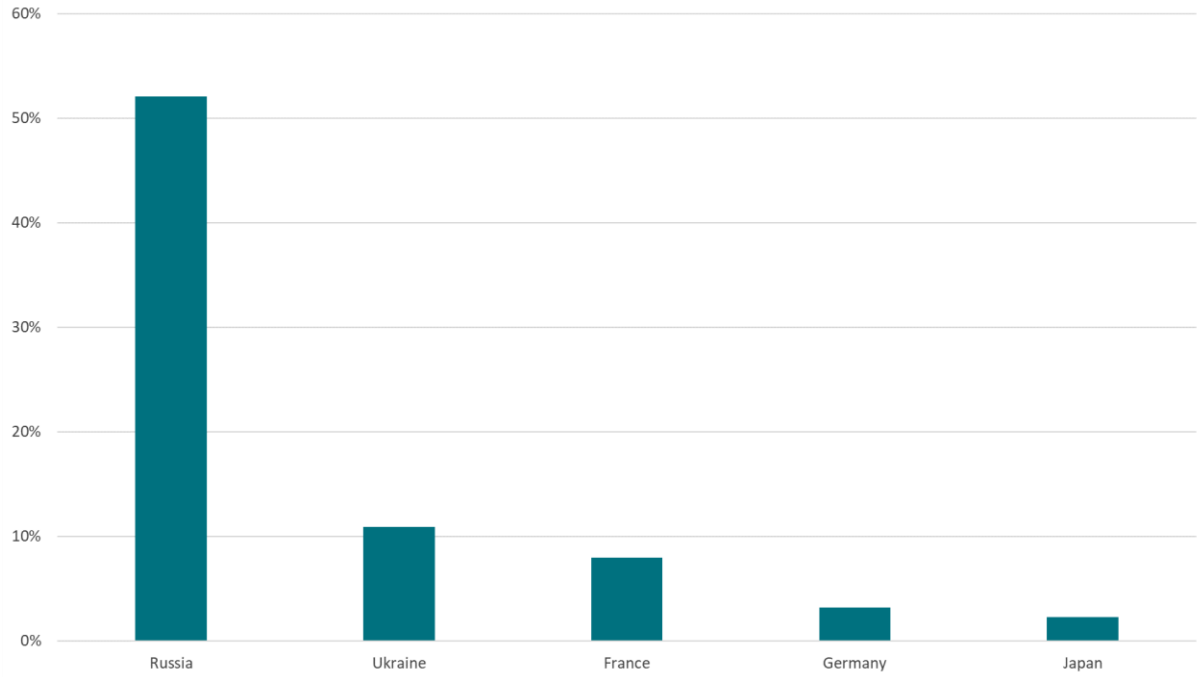

Рисунок 3. Число обнаружений вредоносных JavaScript-вложений, распространяющих Win32/Filecoder.Shade. Данные с 1 по 24 января 2019 года

Согласно нашему анализу, типичная атака январской кампании начинается с получения жертвой письма на русском языке с ZIP-архивом info.zip или inf.zip во вложении.

Письма маскируются под официальные запросы легитимных российских компаний. Мы видели рассылку от лица «Бинбанк» (с 2019 года объединен с банком «Открытие») и розничной сети «Магнит». Текст на рисунке ниже.

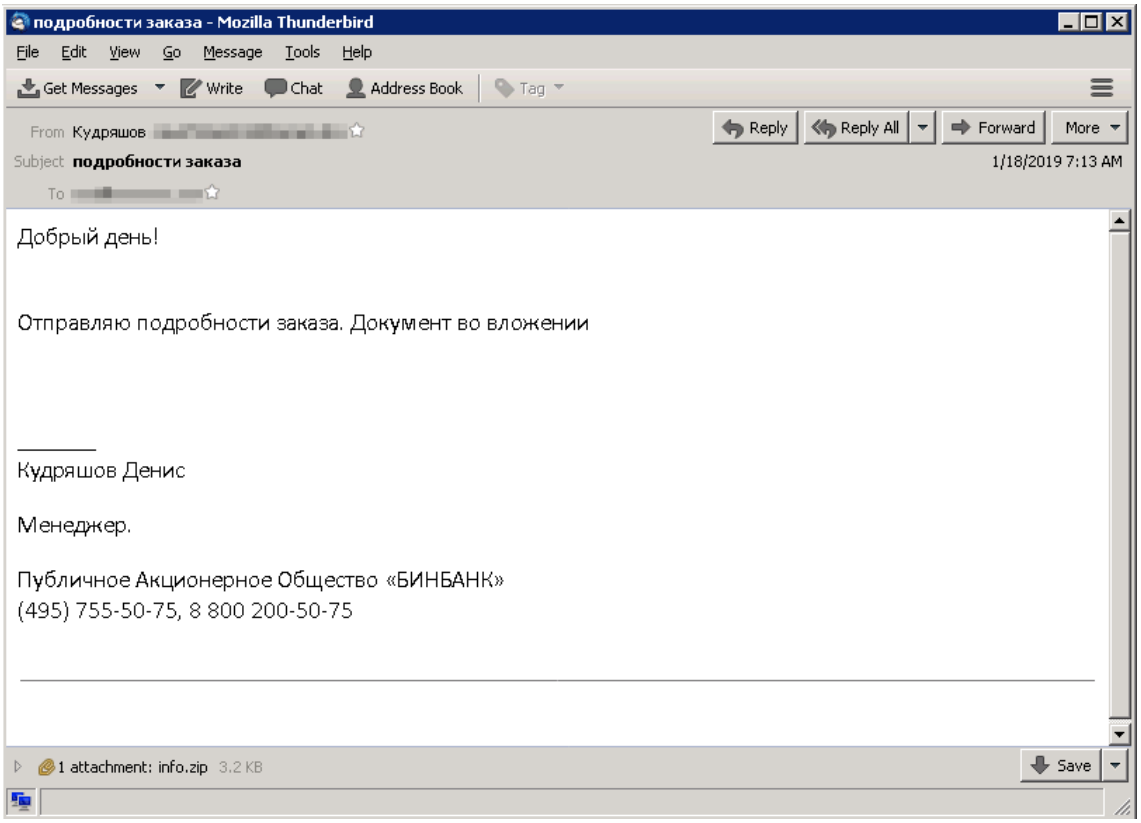

Рисунок 4. Образец спам-рассылки, используемой в январской кампании

В ZIP-архиве находится JavaScript-файл под названием «Информация.js». После извлечения и запуска файл скачивает вредоносный загрузчик, детектируемый продуктами ESET как Win32/Injector. Загрузчик расшифровывает и запускает финальную полезную нагрузку – шифратор Shade.

Вредоносный загрузчик скачивается с URL-адреса скомпрометированных легитимных сайтов WordPress, где маскируется под изображение. Для компрометации страниц WordPress атакующие используют массовую автоматизированную брутфорс-атаку с использованием ботов. Наша телеметрия фиксирует сотни URL, по которым хостится вредоносный загрузчик, все адреса заканчиваются строкой ssj.jpg.

Загрузчик подписан недействительной цифровой подписью, которая, как утверждается, выдана Comodo. Значение поля Signer information и временная метка уникальны для каждого образца.

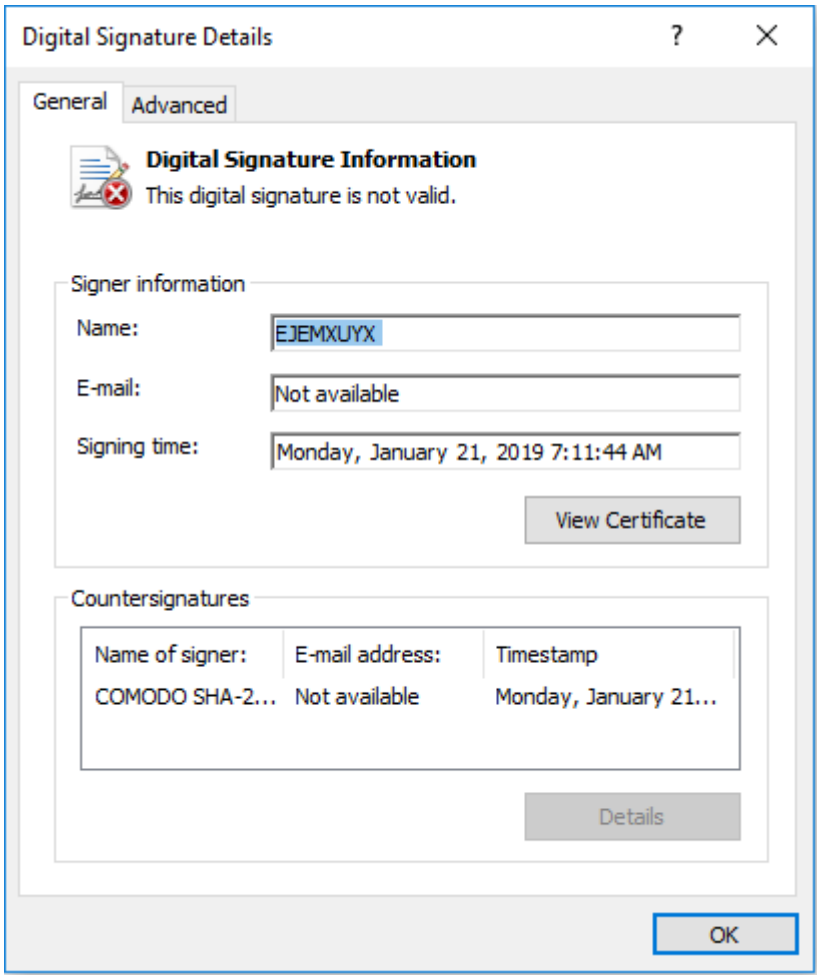

Рисунок 5. Поддельная цифровая подпись, используемая вредоносным загрузчиком

Кроме того, загрузчик пытается маскироваться, выдавая себя за легитимный системный процесс Client Server Runtime Process (csrss.exe). Он копирует себя в C:\ProgramData\Windows\csrss.exe, где Windows – скрытая папка, созданная загрузчиком; обычно в ProgramData этой папки нет.

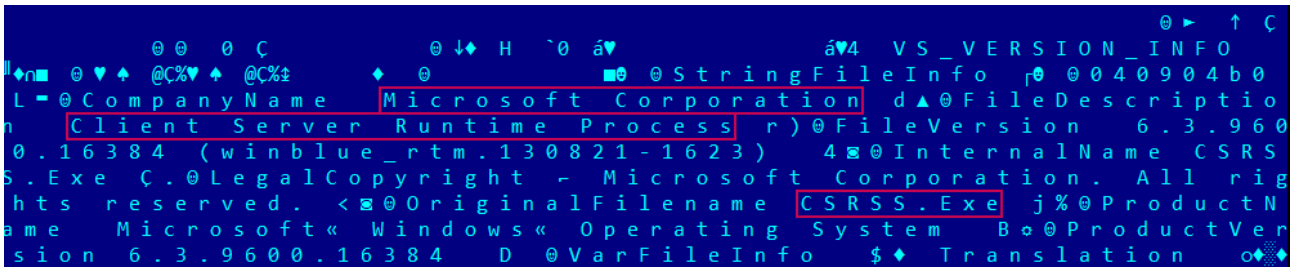

Рисунок 6. Вредоносное ПО, представляющее собой системный процесс и использующий сведения о версии, скопированные из легитимного бинарного файла Windows Server 2012 R2

Шифратор Shade

Финальная полезная нагрузка – шифратор Shade (Troldesh). Впервые он был обнаружен in the wild в конце 2014 года, с тех пор неоднократно обновлялся. Shade шифрует широкий спектр файлов на локальных дисков. В новой кампании он добавляет к зашифрованным файлам расширение .crypted000007.

Жертва получает инструкции по оплате на русском и английском языках в TXT-файле, сохраняемом на зараженном компьютере. Текст такой же, как в прошлой кампании в октябре 2018 года.

```
Ваши файлы были зашифрованы.
Чтобы расшифровать их, Вам необходимо отправить код:
1C75444CDBB110436B9C|0
на электронный адрес pilotpilot088@gmail.com .
Далее вы получите все необходимые инструкции.
Попытки расшифровать самостоятельно не приведут ни к чему, кроме безвозвратной потери информации.
Если вы всё же хотите попытаться, то предварительно сделайте резервные копии файлов, иначе в случае
их изменения расшифровка станет невозможной ни при каких условиях.
Если вы не получили ответа по вышеуказанному адресу в течение 48 часов (и только в этом случае!),
воспользуйтесь формой обратной связи. Это можно сделать двумя способами:
1) Скачайте и установите Tor Browser по ссылке: https://www.torproject.org/download/download-easy.html.en
В адресной строке Tor Browser-а введите адрес:
http://cryptsen7fo43rr6.onion/
и нажмите Enter. Загрузится страница с формой обратной связи.
2) В любом браузере перейдите по одному из адресов:
http://cryptsen7fo43rr6.onion.to/
http://cryptsen7fo43rr6.onion.cab/


All the important files on your computer were encrypted.
To decrypt the files you should send the following code:
1C75444CDBB110436B9C|0
to e-mail address pilotpilot088@gmail.com .
Then you will receive all necessary instructions.
All the attempts of decryption by yourself will result only in irrevocable loss of your data.
If you still want to try to decrypt them by yourself please make a backup at first because
the decryption will become impossible in case of any changes inside the files.
If you did not receive the answer from the aforecited email for more than 48 hours (and only in this case!),
use the feedback form. You can do it by two ways:
1) Download Tor Browser from here:
https://www.torproject.org/download/download-easy.html.en
Install it and type the following address into the address bar:
http://cryptsen7fo43rr6.onion/
Press Enter and then the page with feedback form will be loaded.
2) Go to the one of the following addresses in any browser:
http://cryptsen7fo43rr6.onion.to/
http://cryptsen7fo43rr6.onion.cab/
```

Рисунок 7. Требования выкупа Shade, январь 2019

АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Индикаторы компрометации

Примеры хешей вредоносных ZIP-вложений

```
0A76B1761EFB5AE9B70AF7850EFB77C740C26F82
D072C6C25FEDB2DDF5582FA705255834D9BC9955
80FDB89B5293C4426AD4D6C32CDC7E5AE32E969A
5DD83A36DDA8C12AE77F8F65A1BEA804A1DF8E8B
6EA6A1F6CA1B0573C139239C41B8820AED24F6AC
43FD3999FB78C1C3ED9DE4BD41BCF206B74D2C76
```

Детектирование ESET: JS/Danger.ScriptAttachment

Примеры хешей загрузчиков JavaScript

```
37A70B19934A71DC3E44201A451C89E8FF485009
08C8649E0B7ED2F393A3A9E3ECED89581E0F9C9E
E6A7DAF3B1348AB376A6840FF12F36A137D74202
1F1D2EEC68BBEC77AFAE4631419E900C30E09C2F
CC4BD14B5C6085CFF623A6244E0CAEE2F0EBAF8C
```

Детектирование ESET: Win32/Injector

Примеры хешей шифратора Shade

```
FEB458152108F81B3525B9AED2F6EB0F22AF0866
7AB40CD49B54427C607327FFF7AD879F926F685F
441CFA1600E771AA8A78482963EBF278C297F81A
9023B108989B61223C9DC23A8FB1EF7CD82EA66B
D8418DF846E93DA657312ACD64A671887E8D0FA7
```

Детектирование ESET: Win32/Filecoder.Shade

Характерная строка в URL-адресах, на которых хостится шифратор Shade

```
hxxp://[redacted]/ssj.jpg
```