АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Злоумышленники продолжают использовать Linux/Moose для компрометации устройств

5 ноября 2016 года

В прошлом году наши специалисты опубликовали подробный анализ вредоносной программы **Linux/Moose**, а также деятельности злоумышленников, которые использовали ее для компрометации embedded-устройств. Moose использовался для компрометации сетевых роутеров, подавляющее большинство которых работает под управлением Linux.

Скомпрометированные устройства использовались операторами для кражи незашифрованного сетевого трафика, а также предоставления услуг proxy другим злоумышленникам. На практике, операторы использовали перехват трафика для кражи HTTP cookie от популярных сетевых сервисов, которые затем использовались для выполнения на этих сервисах нелегитимных действий, включая такие как накрутка количества просмотров публикации, установка отметок нравится и добавление новых фолловеров аккаунтов.

В истекшем году, специалисты ESET и security-фирмы GoSecure объединили свои усилия с целью дальнейшего исследования этой вредоносной программы. GoSecure занималась исследованием аспекта социального мошенничества злоумышленников, а также исследованием преступного рынка кибер-услуг ботнета под названием «The Ego Market». Этот рынок был раскрыт в опубликованном исследовании GoSecure. Наш пост посвящен анализу новых функций Linux/Moose, которые появились после публикации нашего предыдущего исследования.

Первое изменение, которое было замечено в новых образцах Moose заключалось в том, что внутри самого исполняемого файла отсутствовал IP-адрес управляющего C&C-сервера. Складывается впечатление, что авторы внимательно прочитали наше предыдущее исследование вредоносной программы и решили сделать ее анализ сложнее. В новой версии, авторы задают IP-адрес управляющего C&C-сервера в виде зашифрованного аргумента командной строки. Ниже указан пример такого метода.

```
[...]
#echo -n -e "\x00\x00\xe6\x13\x02\x00...[REDACTED]" >> /tmp/crondd
#chmod +x /tmp/crondd
#/tmp/crondd 763473758
Loading modules...
Modules are loaded
```

Эта новая функция подразумевает то, что мы теперь не можем просто запустить на исполнение вредоносный файл для исследования его функций. Вместо этого, наши тестовые устройства должны были быть заражены другим уже скомпрометированным злоумышленниками устройством. Видно, что IP-адрес указан в 32-битном целочисленном виде.

Авторы используют шифрование IP-адреса с той целью, чтобы сделать невозможным обнаружение адреса C&C-сервера без знания переданного аргумента даже в том случае, когда у исследователей в распоряжении есть сам образец исполняемого файла. Кроме этого, само по себе знание этого значения, является бесполезным без исполняемого файла, который содержит ключ для расшифровки аргумента. Аргумент расшифровывается операцией XOR с ключом, указанным внутри файла.

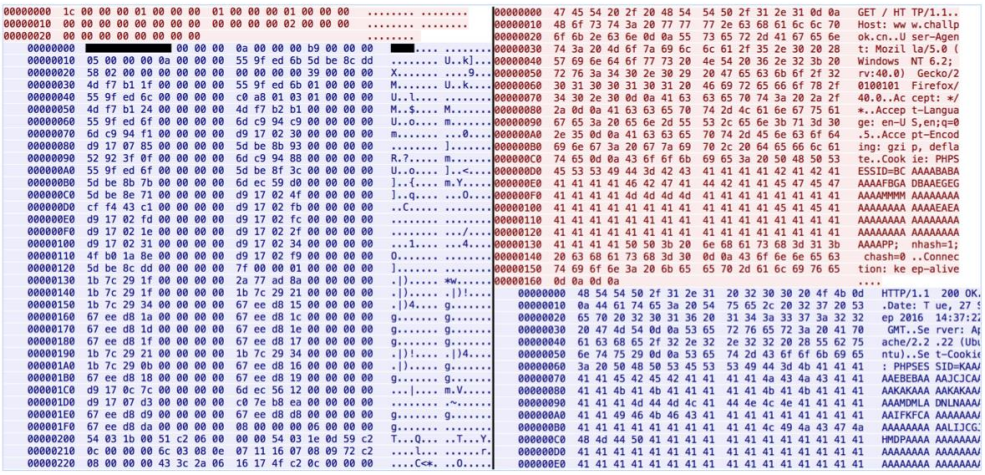
```
[...]
  if ( !cnc_ip )
    return 0;
  cnc_ip ^= 0xF789AC9E;
[...]
```

DECOMPILER OUTPUT

Насколько нам известно, это жестко зашитое значение осталось неизменным на протяжении последних нескольких месяцев. Следующий фрагмент кода на Python предназначен для расшифровки 32-битного целочисленного значения IP-адреса.

```
import socket
import struct
argument = 763473758
static_value = 0xF789AC9E
decrypted_argument = argument ^ static_value
print(socket.inet_ntoa(struct.pack("<I", decrypted_argument)))
```

Сетевой протокол также подвергся изменению, но при этом была сохранена его основа и были добавлены новые функции. Ниже представлен пример сравнения сетевых пакетов двух различных образцов Moose. Видно, что основному изменению подвергся формат протокола, который из двоичного превратился в ASCII. Ниже на рисунке показан старый сетевой протокол (слева) и новый (справа).



В прошлой модификации Moose, информация о конфигурации отправлялась боту управляющим C&C-сервером и содержала различные поля, включая, битовые для определения того, какая функция бота должна быть включена. Для этого использовались такие поля конфигурации, как поле IP-адреса, поле белого списка адресов, поле со списком паролей. Эти поля все еще присутствуют в новой версии вредоносной программы, но теперь они разделены на три разных ключа (см. таблицу ниже). Для отправки этих конфигурационных данных, оператор использует параметры Cookie: и Set-Cookie: заголовка HTTP-протокола. Эта информация шифруется в цикле простым алгоритмом XOR, который также использовался и в первой версии. Однако, информация также кодируется в читабельный ASCII-вид в заголовке HTTP.

```
char *__fastcall to_printable(char *result, char *a2, int len)
{
  unsigned __int8 v3; // ST13_1@2
  int i; // [sp+14h] [bp-8h]@1

  for ( i = 0; i < len; ++i )
  {
    v3 = a2[i];
    result[2 * i] = (v3 & 0xF) + 'A';
    result[2 * i + 1] = (v3 >> 4) + 'A';
  }
  return result;
}
```

Ключ	Значение
PHPSESSID	Основные данные конфигурации (сканирование локальных/внешних адресов, данные сниффера, параметры убийства процессов).
LP	Список паролей.
WL	Белый список адресов

Ключ конфигурации PHPSESSID фиксирует зашифрованное содержимое битового поля, которое позволяет включить или отключить различные функции Moose. Параметр LP фиксирует список паролей, которые вредоносная программа будет использовать в попытках заражения других устройств при доступе к ним по telnet. Авторы значительно уменьшили этот список, если в 2015 г в нем было около 300 логинов и паролей, то сейчас (2016) их осталось около 10.

```
support support
admin admin
root root
guest
admin smcadmin
root
admin
adm
1234 1234
root 12345
admin 1234
```

Ключ WL указывает на белый список IP-адресов устройств, которые не должны подвергнуться заражению. В новой версии список сокращен с 50 адресов до 10. Список этих IP-адресов указан ниже. Linux/Moose по-прежнему имеет возможность предоставлять злоумышленникам услуги прокси, при этом входящие подключения прослушиваются по TCP-порту 20012. Предыдущие модификации использовали для этих целей порт с номером 10073. Функция прокси позволяет IP-адресам из белого списка взаимодействовать с вредоносной программой.

Заключение

Авторы Linux/Moose проделали большую работу по модификации вредоносной программы, добавив в нее функцию сокрытия месторасположения управляющих C&C-серверов, а также изменив сетевой протокол. Эти новые функции позволяют авторам вредоносной программы сделать бесполезными индикаторы компрометации активности предыдущих версий Moose в случае с новыми версиями. Уменьшение размера белого списка адресов, а также паролей, показывает их более деликатный подход к использованию бота. В файлах Moose нами были обнаружены и специальные фальшивые индикаторы для введение в заблуждение исследователей, например, домен www.challpok.cn, который был найден в открытом виде в списке строк. Кроме этого, там же были обнаружены строки, которые пытаются маскировать Moose под майнер биткоинов или DDoS-бот. Бот не использует каких-либо средств обеспечения своего выживания в системе, поэтому простая перезагрузка устройства завершит его вредоносную деятельность.

Индикаторы компроментации (IoC)

```
Хэши

Версия 0x1F (31)
c6edfa2bf916d374e60f1b5444be6dbbee099692
c9ca4820bb7be18f36b7bad8e3044b2d768a5db8
5b444f1ac312b4c24b6bde304f00a5772a6a19a4
f7574b3eb708bd018932511a8a3600d26f5e3be9

Версия 0x20 (32)
34802456d10efdf211a7d486f7108319e052cd17
0685cb1d72107de63fa1da52930322df04a72dbc
2876cad26d6dabdc0a9679bb8575f88d40ebd960
f94b6cc5aea170cee55a238eaa9339279fba962f
274ef5884cb256fd4edd7000392b0e326ddd2398
c3f0044ffa9d0bc950e9fd0f442c955b71a706b6
f3daea1d06b1313ec061d93c9af12d0fe746839a

Версия 0x21 (33)
7767c8317fb0bbf91924bddffe6a5e45069b0182
1caac933ae6ca326372f7e5dd9fff82652e22e34
5dea6c0c4300e432896038661db2f046c523ce35
e8dc272954d5889044e92793f0f637fe4d53bb91
0843239b3d0f62ae6c5784ba4589ef85329350fa
1d1d46c312045e17f8f4386adc740c1e7423a24a
d8b45a1114c5e0dbfa13be176723b2288ab12907

Версия 0x22 (34)
c35d6812913ef31c20404d9bbe96db813a764886

IP-адреса

Основные C&C-сервера
192.3.8.218
192.3.8.219

Белый список
155.133.18.64
178.19.111.181
151.80.8.2
151.80.8.19
151.80.8.30
62.210.6.34
```

Список индикаторов компрометации также доступен на нашем репозитории.