АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Hacking Team снова в деле: ESET обнаружила новые образцы шпионского ПО компании

27 марта 2018 года

С момента основания в 2003 году итальянский разработчик программного обеспечения для кибершпионажа Hacking Team приобрел известность, продавая свои продукты правительствам и спецслужбам во всем мире. Возможности флагмана компании – Remote Control System (RCS) – включают извлечение файлов с целевого устройства, перехват писем и сообщений, а также удаленное управление веб-камерой и микрофоном.

ESET обнаружила в 14 странах мира ранее неизвестные образцы RCS. Анализ новых образцов позволяет сделать вывод о том, что разработку этих программных инструментов продолжает сама Hacking Team.

От Hacking Team к Hacked Team

Hacking Team неоднократно подвергалась критике за продажу шпионского ПО авторитарным режимам, но всегда отрицала эти обвинения. Ситуация изменилась в июле 2015 года, когда компания стала жертвой взлома и факты использования RCS диктатурами получили подтверждение. После утечки 400 Гб данных, включая список клиентов, переписку сотрудников и исходный код шпионского ПО, Hacking Team была вынуждена просить клиентов приостановить использование RCS и оказалась в состоянии неопределенности.

После взлома ИБ-сообщество внимательно следило за попытками компании встать на ноги. Первые сообщения о новых операциях Hacking Team появились шесть месяцев спустя – новый

образецшпионской программы для Mac, по всей видимости, использовался на практике. Через год после утечки в Hacking Team инвестировала компания Tablem Limited, получившая 20% акций разработчика. Tablem Limited официально зарегистрирована на Кипре, но есть указания на ее связь с Саудовской Аравией.

Завершив исследование еще одного шпионского ПО, FinFisher, мы отметили два интересных события, связанных с Hacking Team: отчет о финансовом оздоровлении группы и открытие новой версии RCS с действительным цифровым сертификатом.

RCS: жизнь продолжается

На ранних этапах исследования наши коллеги из Citizen Lab, которые давно наблюдают за деятельностью Hacking Team, предоставили нам ценный материал, позволивший открыть новую версию шпионского ПО. Малварь в настоящее время используется на практике и имеет новый цифровой сертификат.

Дальнейшее исследование выявило еще несколько образцов программ Hacking Team, созданных после взлома 2015 года, причем все они слегка модифицированы в сравнении с инструментами, выпущенными до утечки исходного кода.

Образцы были скомпилированы в период с сентября 2015 по октябрь 2017 гг. Мы считаем даты компиляции достоверными, поскольку телеметрия ESET зафиксировала практическое применение образцов через несколько недель после компиляции.

Дальнейший анализ позволил сделать вывод, что происхождение всех образцов сводится к одной кибергруппе; это не изолированные версии разных разработчиков, использующих слитый в интернет исходный код Hacking Team.

Одним из аргументов в пользу этой точки зрения является последовательность цифровых сертификатов, которыми подписаны образцы. Мы обнаружили шесть разных сертификатов, выпущенных один за другим. Четыре из них выданы центром сертификации Thawte четырем различным компаниям, два – персональные сертификаты на имя Валериано Бедеши (соучредителя Hacking Team) и некоего Рафаэля Карнасина, как показано ниже:

Certificate issued to	Validity period
Valeriano Bedeschi	8/13/2015 – 8/16/2016
Raffaele Carnacina	9/11/2015 – 9/15/2016
Megabit, OOO	6/8/2016 - 6/9/2017
ADD Audit	6/20/2016 - 6/21/2017
Media Lid	8/29/2016 - 8/30/2017
Ziber Ltd	7/9/2017 - 7/10/2018

Также образцы содержат поддельные метаданные манифеста, чтобы маскироваться под легитимное ПО Advanced SystemCare 9 (9.3.0.1121), Toolwiz Care 3.1.0.0 и SlimDrivers (2.3.1.10).

Наш анализ показывает, что автор(ы) образцов использовали VMProtect, по-видимому, пытаясь сделать образцы менее предрасположенными к обнаружению. Метод использовался в программах Hacking Team и до утечки.

Сама по себе связь между этими образцами может указывать практически на любую кибергруппу, видоизменившую слитый исходный код Hacking Team или установщик – как это было с группой Callisto в начале 2016 года. Однако мы собрали другие доказательства, которые позволяют связать новые образцы с самими разработчиками Hacking Team.

Версионность в новых образцах, доступ к которой мы получили после преодоления защиты VMProtect, начинается до утечки, продолжается после нее и следует тем же шаблонам. Для разработчиков компании характерно компилировать функциональную часть малвари (под названиями Scout и Soldier) последовательно и зачастую в один день – это можно наблюдать и в новых образцах.

В таблице ниже представлены даты компиляции, версии и сертификаты образцов шпионского ПО Hacking Team для Windows, выпущенных с 2014 по 2017 гг. Повторное использование слитого исходного кода группой Callisto выделено красным:

Compilation date	Scout version	Soldier version	Certificate issued to
2014-11-27		1007	Open Source Developer, Muhammad Lee's
2014-12-05	11		Open Source Developer, Muhammad Lee's
2014-12-12	12	1008	Open Source Developer, meicun ge
2015-03-19		1009	Open Source Developer, meicun ge
2015-03-27	13		Open Source Developer, meicun ge
JULY 2015 LEAK			
2015-09-04	15		Valeriano Bedeschi
2015-10-19	16	1011	Raffaele Carnacina
2016-01-05	17		SPC
2016-01-18	17		Raffaele Carnacina
2016-03-24	18	1012	Raffaele Carnacina
2016-06-17		1014	Megabit, OOO
2016-08-02	21	1016	Megabit, OOO

2016-09-01	22	1017	ADD Audit
2016-12-19	23	1018	ADD Audit
2017-01-31	24	1019	ADD Audit
2017-04-28	25	1020	ADD Audit, Media Lid
2017-06-28	27	1022	Media Lid, Ziber Ltd
2017-10-09	28		Ziber Ltd
2017-10-18		1025	Ziber Ltd

Кроме того, наши исследования подтвердили, что изменения, внесенные после утечки, выполнены в соответствии с собственным стилем программирования Hacking Team и часто встречаются в местах, указывающих на глубокое понимание кода. Маловероятно, что игрок не из числа разработчиков Hacking Team, создающий новые версии на базе слитого исходного кода, мог внести изменения именно в эти фрагменты.

Одно из различий между образцами до и после утечки – размер файла автозапуска. До утечки использовался скопированный файл размером около 4 Мб. После утечки размер составлял 6 Мб – возможно, в качестве примитивного метода защиты от обнаружения.

PRE-LEAK

```
sub_420D30(&v16, &v18);
if ( v18 )
  lpFirst = (LPCWSTR)sub_420DF0(1);
else
  lpFirst = (LPCWSTR)sub_420DF0(0);
if ( StrStrIW(lpFirst, &Srch) )
{
  hFile = CreateFileW(lpFileName, 0x80000000, 1u, 0, 3u, 0x80u, 0);
  if ( hFile != (HANDLE)-1 )
  {
    Scout to be increased to this size = 4194314
    var_2C = GetFileSize(hFile, 0);
    for ( i = 4194314 - var_2C; i % 8; ++i )
      ;
    if ( i )
    {
      if ( sub_425D00() )
      {
        v6 = (void *)sub_421830(i);
        v7 = sub_421970(hFile, v6, i, (int)&var_2C);
        unknown_libname_11(v6);
        if ( v7 )
        {
          CloseHandle(hFile);
          v4 = (LPCWSTR)sub_425A70();
          hFatScout = CreateFileW(v4, 0xC0000000, 3u, 0, 4u, 0x80u, 0);
          if ( hFatScout != (HANDLE)-1 )
          {
            v3 = 0;
            v2 = WriteFile(hFatScout, v7, var_2C, &v3, 0);
            CloseHandle(hFatScout);
            sub_4260B0(v4, lpFileName, &v1);
            sub_426DB0(v1);
            ExitProcess(0);
          }
        }
      }
    }
```

```
sub_421CD0(&v24, &Src);
v23 = sub_421C30((int)&v51, v24, Src);
if ( !v23 )
{
  hFile = CreateFileW(lpFileName, 0x80000000, 1u, 0, 3u, 0x80u, 0);
  if ( hFile != (HANDLE)-1 )
  {
    Scout to be increased to this size = 6291466
    nNumberOfBytesToWrite = GetFileSize(hFile, 0);
    for ( i = 6291466 - nNumberOfBytesToWrite; i % 8; ++i )
      ;
    if ( i )
    {
      if ( sub_425D70() )
      {
        v6 = (void *)sub_420CE0(i);
        v7 = (LPCVOID)sub_421A60(hFile, v6, i, (int)&nNumberOfBytesToWrite);
        unknown_libname_11(v6);
        if ( v7 )
        {
          CloseHandle(hFile);
          v4 = (LPCWSTR)sub_425AE0();
          hObject = CreateFileW(v4, 0xC0000000, 3u, 0, 4u, 0x80u, 0);
          if ( hObject != (HANDLE)-1 )
          {
            v3 = 0;
            v2 = WriteFile(hObject, v7, nNumberOfBytesToWrite, &v3, 0);
            CloseHandle(hObject);
            sub_426620(v4, lpFileName, &v1);
            sub_426E70(v1);
            ExitProcess(0);
          }
        }
      }
    }
```

Мы обнаружили некоторые другие различия, которые полностью убедили нас в участии Hacking Team. Однако раскрытие этих данных может помешать дальнейшему наблюдению за активностью группы, поэтому мы не можем опубликовать их. Готовы поделиться информацией с другими исследователями, запрос можно отправить на threatintel@eset.com.

Функциональность шпионского ПО в значительной степени соответствует тому, что было в слитом исходном коде. Наш анализ до сих пор не подтвердил выпуск какого-либо значительного обновления, которое обещала Hacking Team после взлома.

Как минимум, два изученных образца распространялись с помощью фишинговых рассылок. Вредоносный исполняемый файл маскировался под документ PDF с использованием двойного расширения файла. Названия документов-приманок, вероятно, ориентированы на потенциальных жертв из числа сотрудников дипломатических представительств.

2003
Hacking Team founded

October 2012
The Citizen Lab publishes its first research on Hacking Team

February 2014
The Citizen Lab accuses Hacking Team of selling to oppressive governments

19 March 2015
Soldier version 1009
Signed by: Open Source Developer, meicun ge

27 March 2015
Scout version 13
Signed by: Open Source Developer, meicun ge

July 2015
Hacking Team hacked

4 September 2015
Scout version 15
Signed by: Valeriano Bedeschi

19 October 2015
Scout version 16, Soldier version 1011
Signed by: Raffaele Carnacina

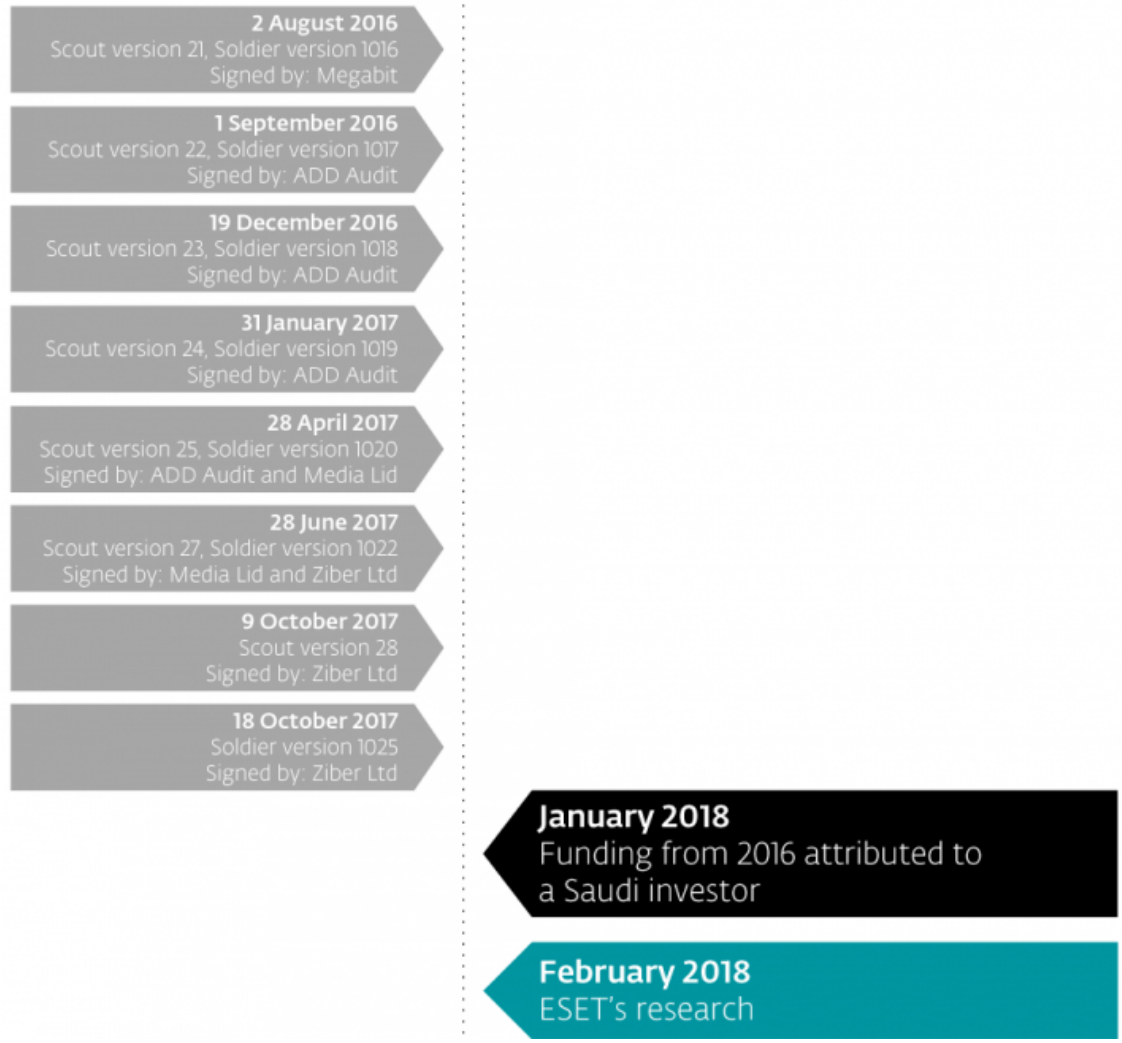
5 January 2016
Scout version 13,
Signed by: SPC

January 2016
Callisto Group sample built from leaked source code (reported by F-Secure)

18 January 2016
Scout version 17
Signed by: Raffaele Carnacina

February 2016
New Mac sample spotted in the wild

24 March 2016
Scout version 18, Soldier version 1012
Signed by: Raffaele Carnacina



Выводы

Наши исследования позволяют утверждать, что образцы шпионского ПО RCS, помимо одного исключения, являются результатом работы Hacking Team, а не повторного использования кода как в кейсе с группой Callisto в 2016 году.

На момент написания этой статьи наши системы телеметрии детектируют новые образцы шпионского ПО Hacking Team в 14 странах мира. Предпочитаем не называть страны, чтобы предотвратить неверную атрибуцию, поскольку геолокация обнаружений не всегда может дать информацию об источнике атаки.

Индикаторы компрометации

Детектирование продуктами ESET

Trojan.Win32/CrisisHT.F
Trojan.Win32/CrisisHT.H
Trojan.Win32/CrisisHT.E
Trojan.Win32/CrisisHT.L
Trojan.Win32/CrisisHT.J
Trojan.Win32/Agent.ZMW
Trojan.Win32/Agent.ZMX

Trojan.Win32/Agent.ZMY
Trojan.Win32/Agent.ZMZ

Образцы, подписанные Ziber Ltd

Thumbprint: 14 56 d8 a0 0d 8b e9 63 e2 22 4d 84 5b 12 e5 08 4e a0 b7 07
Serial Number: 5e 15 20 5f 18 04 42 cc 6c 3c 0f 03 e1 a3 3d 9f

SHA-1

2eebf9d864bef5e08e2e8abd93561322de2ab33b
51506ed3392b9e59243312b0f798c898804913db
61eda4847845f49689ae582391cd1e6a216a8fa3
68ffd64b7534843ac2c66ed68f8b82a6ec81b3e8
6fd86649c6ca3d2a0653fd0da724bada9b6a6540
92439f659f14dac5b353b1684a4a4b848ecc70ef
a10ca5d8832bc2085592782bd140eb03cb31173a
a1c41f3dad59c9a1a126324a4612628fa174c45a
b7229303d71b500157fa668cece7411628d196e2
eede2e3fa512a0b1ac8230156256fc7d4386eb24

C&Cs

149.154.153.223
192.243.101.125
180.235.133.23
192.243.101.124
95.110.167.74
149.154.153.223

Образцы, подписанные ADD Audit

Thumbprint: 3e 19 ad 16 4d c1 03 37 53 26 36 c3 7c a4 c5 97 64 6f bc c8
Serial Number: 4c 8e 3b 16 13 f7 35 42 f7 10 6f 27 20 94 eb 23

SHA-1

341dbcb6d17a3bc7fa813367414b023309eb69c4
86fad7c362a45097823220b77dcc30fb5671d6d4
9dfc7e78892a9f18d2d15adbfa52cda379ddd963
e8f6b7d10b90ad64f976c3bfb4c822cb1a3c34b2

C&Cs

188.166.244.225
45.33.108.172
178.79.186.40
95.110.167.74
173.236.149.166

Образцы, подписанные Media Lid

Thumbprint: 17 f3 b5 e1 aa 0b 95 21 a8 94 9b 1c 69 a2 25 32 f2 b2 e1 f5
Serial Number: 2c e2 bd 0a d3 cf de 9e a7 3e ec 7c a3 04 00 da

SHA-1

27f4287e1a5348714a308e9175fb9486d95815a2
71a68c6140d066ca016efa9087d71f141e9e2806
dc817f86c1282382a1c21f64700b79fcd064ae5c

SHA-1
27f4287e1a5348714a308e9175fb9486d95815a2
71a68c6140d066ca016efa9087d71f141e9e2806
dc817f86c1282382a1c21f64700b79fcd064ae5c

C&Cs
188.226.170.222
173.236.149.166

Образцы, подписанные Megabit, OOO
Thumbprint: 6d e3 a1 9d 00 1f 02 24 c1 c3 8b de fa 74 6f f2 3a aa 43 75
Serial Number: 0f bc 30 db 12 7a 53 6c 34 d7 a0 fa 81 b4 81 93

SHA-1
508f935344d95ffe9e7aedff726264a9b500b854
7cc213a26f8df47ddd252365fadbb9cca611be20
98a98bbb488b6a6737b12344b7db1acf0b92932a
cd29b37272f8222e19089205975ac7798aac7487
d21fe0171f662268ca87d4e142aedfbe6026680b
5BF1742D540F08A187B571C3BF2AEB64F141C4AB
854600B2E42BD45ACEA9A9114747864BE002BF0B

C&Cs
95.110.167.74
188.226.170.222
173.236.149.166
46.165.236.62

Образцы, подписанные Рафаэлем Карнасина
Thumbprint: 8a 85 4f 99 2a 5f 20 53 07 f8 2d 45 93 89 af da 86 de 6c 41
Serial Number: 08 44 8b d6 ee 91 05 ae 31 22 8e a5 fe 49 6f 63

SHA-1
4ac42c9a479b34302e1199762459b5e775eec037
2059e2a90744611c7764c3b1c7dcf673bb36f7ab
b5fb3147b43b5fe66da4c50463037c638e99fb41
9cd2ff4157e4028c58cef9372d3bb99b8f2077ec
b23046f40fbc931b364888a7bc426b56b186d60e
cc209f9456f0a2c5a17e2823bdb1654789fcadc8
99c978219fe49e55441e11db0d1df4bda932e021
e85c2eab4c9eea8d0c99e58199f313ca4e1d1735
141d126d41f1a779dca69dd09640aa125afed15a

C&Cs
199.175.54.209
199.175.54.228
95.110.167.74

Образцы, подписанные Валериано Бедеши
Thumbprint: 44 a0 f7 f5 39 fc 0c 8b f6 7b cd b7 db 44 e4 f1 4c 68 80 d0
Serial Number: 02 f1 75 66 ef 56 8d c0 6c 9a 37 9e a2 f4 fa ea

SHA-1

baa53ddba627f2c38b26298d348ca2e1a31be52e
5690a51384661602cd796e53229872ff87ab8aa4
aa2a408fcaa5c86d2972150fc8dd3ad3422f807a
83503513a76f82c8718fad763f63fcd349b8b7fc

C&Cs

172.16.1.206 – это внутренний адрес, найденный в образцах