Our website uses cookies. By continuing to browse the site you are agreeing to our use of cookies. For more details about cookies and how to manage them, see our **Cookie Policy**

welivesecurity

News, views, and insight from the ESET security community

Type your keyword... Search

New traces of Hacking Team in the wild

BY FILIP KAFKA POSTED 9 MAR 2018 - 06:01PM

Previously unreported samples of Hacking Team's infamous surveillance tool – the Remote Control System (RCS) – are in the wild, and have been detected by ESET systems in fourteen countries.

Our analysis of the samples reveals evidence suggesting that Hacking Team's developers themselves are actively continuing the development of this spyware.

From Hacking Team to Hacked Team to…?

Since being founded in 2003, the Italian spyware vendor Hacking Team gained notoriety for selling surveillance tools to governments and their agencies across the world.

The capabilities of its flagship product, the Remote Control System (RCS), include extracting files from a targeted device, intercepting emails and instant messaging, as well as remotely activating a device's webcam and microphone. The company has been criticized for selling these capabilities to **authoritarian governments** – an allegation it has consistently denied.

When the tables turned in July 2015, with Hacking Team itself **suffering a damaging hack**, the reported use of RCS by oppressive regimes was **confirmed**. With 400GB of internal data – including the once-secret list of customers, internal communications, and spyware source code – leaked online, Hacking Team was forced to request its customers to **suspend all use of RCS**, and was left facing an uncertain future.

Following the hack, the security community has been keeping a close eye on the company's efforts to get back on its feet. The first reports suggesting Hacking Team's resumed operations came six months later – a **new sample of Hacking Team's Mac spyware** was apparently in the wild. A year after the breach, an investment by a company named Tablem Limited brought changes to Hacking Team's shareholder structure, with Tablem Limited taking 20% of Hacking Team's shareholding. Tablem Limited is officially based in Cyprus; however, recent news suggests it has **ties to Saudi Arabia**.

Having just concluded our research into another commercial spyware product, **FinFisher**, two interesting events involving Hacking Team occurred in close succession – the report about Hacking Team's apparent financial recovery and our discovery of a new RCS variant in the wild with a valid digital certificate.

The spyware lives on

In the early stages of this investigation, our friends from **the Citizen Lab** – who have a long record of keeping track of Hacking Team – provided us with valuable input that led to the discovery of a version of the spyware currently being used in the wild and signed with a previously unseen valid digital certificate.

Our further research uncovered several more samples of Hacking Team's spyware created after the 2015 hack, all being slightly modified compared to variants released before the source code leak.

The samples were compiled between September 2015 and October 2017. We have deemed these compilation dates to be authentic, based on ESET telemetry data indicating the appearance of the samples in the wild within a few days of those dates.

Further analysis led us to conclude that all the samples can be traced back to a single group, rather than being isolated instances of diverse actors building their own versions from the leaked Hacking Team source code.

One indicator supporting this is the sequence of digital certificates used to sign the samples – we found six different certificates issued in succession. Four of the certificates were issued by Thawte to four different companies, and two are personal certificates issued to Valeriano Bedeschi (Hacking Team co-founder) and someone named Raffaele Carnacina, as shown in the following table:

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

The samples also have forged Manifest metadata – used to masquerade as a legitimate application – in common, appearing as “Advanced SystemCare 9 (9.3.0.1121)”, “Toolwiz Care 3.1.0.0” and “SlimDrivers (2.3.1.10)”.

Our analysis further shows that the author(s) of the samples have been using VMProtect, apparently in an effort to make their samples less prone to detection. This was also common among pre-leak Hacking Team spyware.

The connections among these samples alone could have originated with virtually any group re-purposing the leaked Hacking Team source code or installer – as was the case with **Callisto Group** in early 2016. We have, however, collected further evidence that ties these post-leak samples to Hacking Team’s developers themselves.

The versioning (which we accessed after overcoming VMProtect protection) observed in the analyzed samples continues where Hacking Team left off before the breach, and follows the same patterns. Hacking Team’s habit of compiling their payloads – named Scout and Soldier – consecutively, and often on the same day, can also be seen across the newer samples.

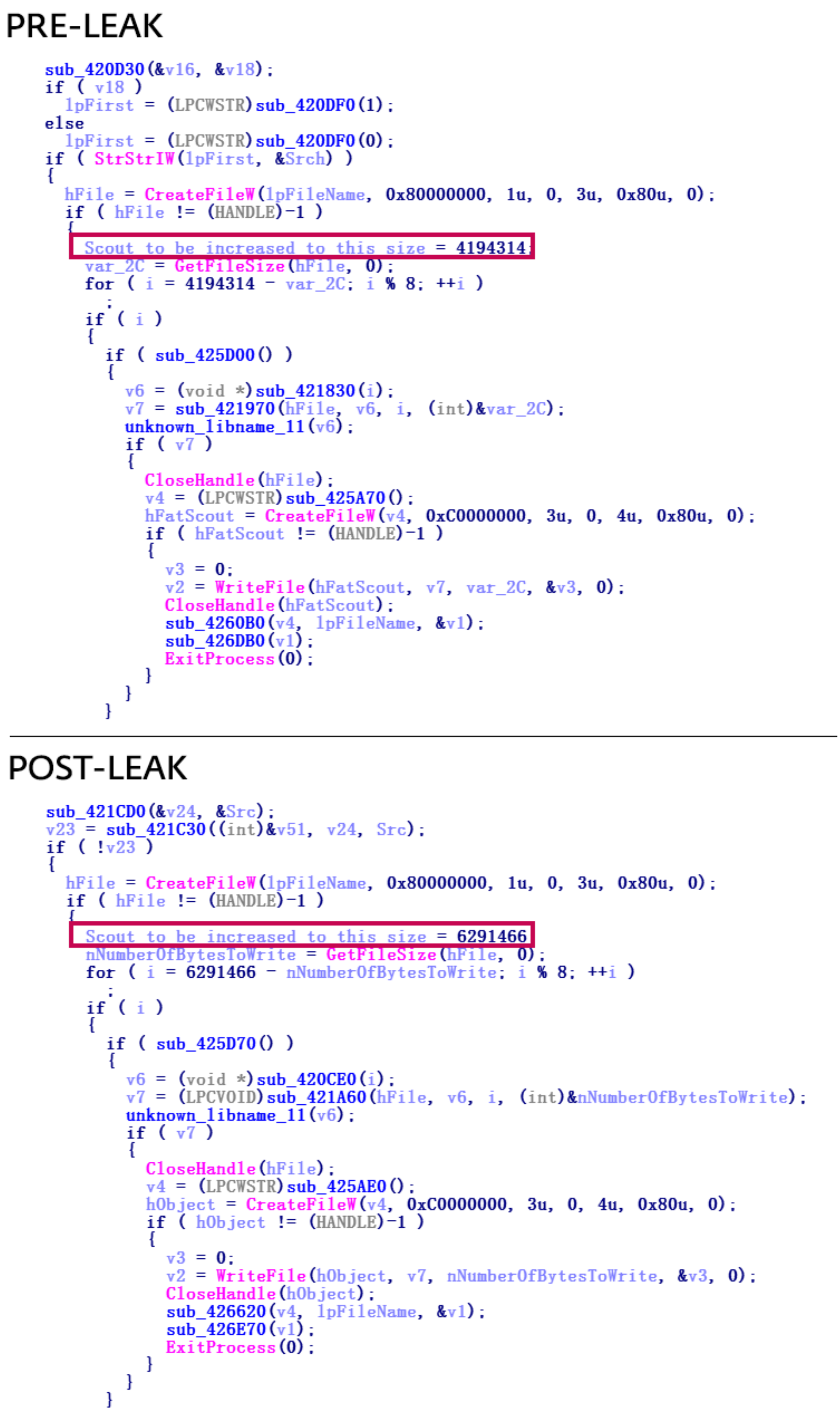
The following table shows the compilation dates, versioning and certificate authorities of Hacking Team Windows spyware samples seen between 2014 and 2017. Reuse of leaked source code by Callisto Group is marked in red.

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	13		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

Compilation date	Scout version	Soldier version	Certificate issued to
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

Furthermore, our research has confirmed that the changes introduced in the post-leak updates were made in line with Hacking Team's own coding style and are often found in places indicating a deep familiarity with the code. It is highly improbable that some other actor – that is, other than the original Hacking Team developer(s) – would make changes in exactly these places when creating new versions from the leaked Hacking Team source code.

One of the subtle differences we spotted between the pre-leak and the post-leak samples is the difference in Startup file size. Before the leak, the copied file was padded to occupy 4MB. In the post-leak samples, this file copy operation is padded to 6MB – most likely as a primitive detection evasion technique.



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);
          }
        }
      }
```

POST-LEAK

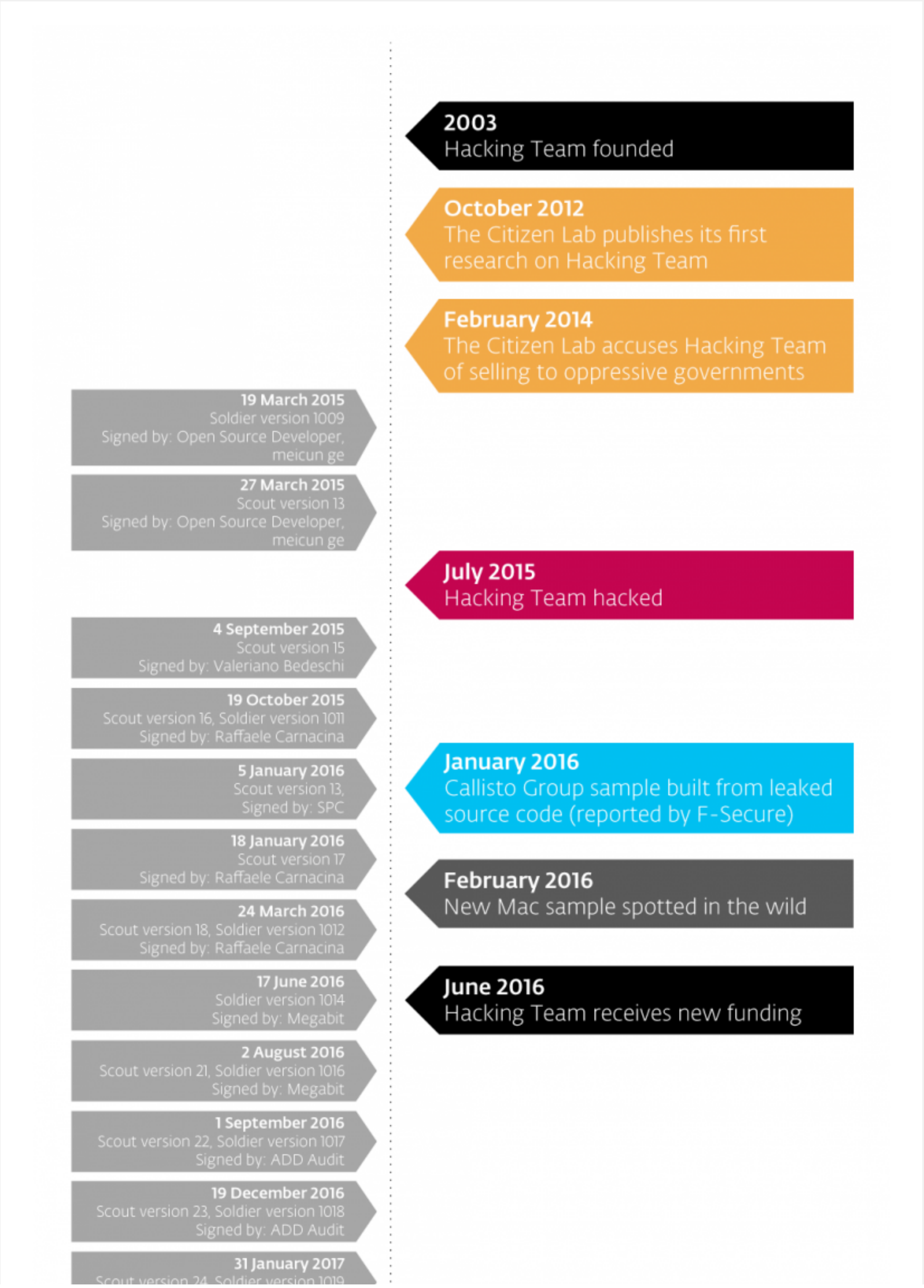
```
sub_421CD0(&v24, &Src);
v23 = sub_421C30((int)&v51, v24, Src);
if ( !v23 )
{
  hFile = CreateFileW(lpFileName, 0x80000000, 1u, 0, 3u, 0x80u, 0);
  if ( hFile != (HANDLE)-1 )
  {
    Scout_to_be_increased_to_this_size = 6291466;
    nNumberOfBytesToWrite = GetFileSize(hFile, 0);
    for ( i = 6291466 - 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);
          }
        }
      }
```

Figure 1 – Startup file size copy changed from 4 MB pre-leak to 6MB post-leak

We found further differences that fully convinced us of Hacking Team's involvement. However, the disclosure of these details could interfere with the future tracking of the group, which is why we choose not to publish them. We are, however, open to share these details with fellow researchers (for any inquiries contact us at threatintel@eset.com).

The functionality of the spyware largely overlaps with that in the leaked source code. Our analysis so far has not confirmed the release of any significant update, as **promised** by Hacking Team following the hack.

As for the distribution vector of the post-leak samples we analyzed, at least in two cases, we detected the spyware in an executable file disguised as a PDF document (using multiple file extensions) attached to a spearphishing email. The names of the attached files contain strings likely aimed to reduce suspicion when received by diplomats.


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
17 June 2016
Soldier version 1014
Signed by: Megabit
June 2016
Hacking Team receives new funding
2 August 2016
Scout version 21, Soldier version 1016
Signed by: Megabit
1 September 2016
Scout version 22, Soldier version 1017
Signed by: ADD Audit
19 December 2016
Scout version 23, Soldier version 1018
Signed by: ADD Audit
31 January 2017
Scout version 24, Soldier version 1019

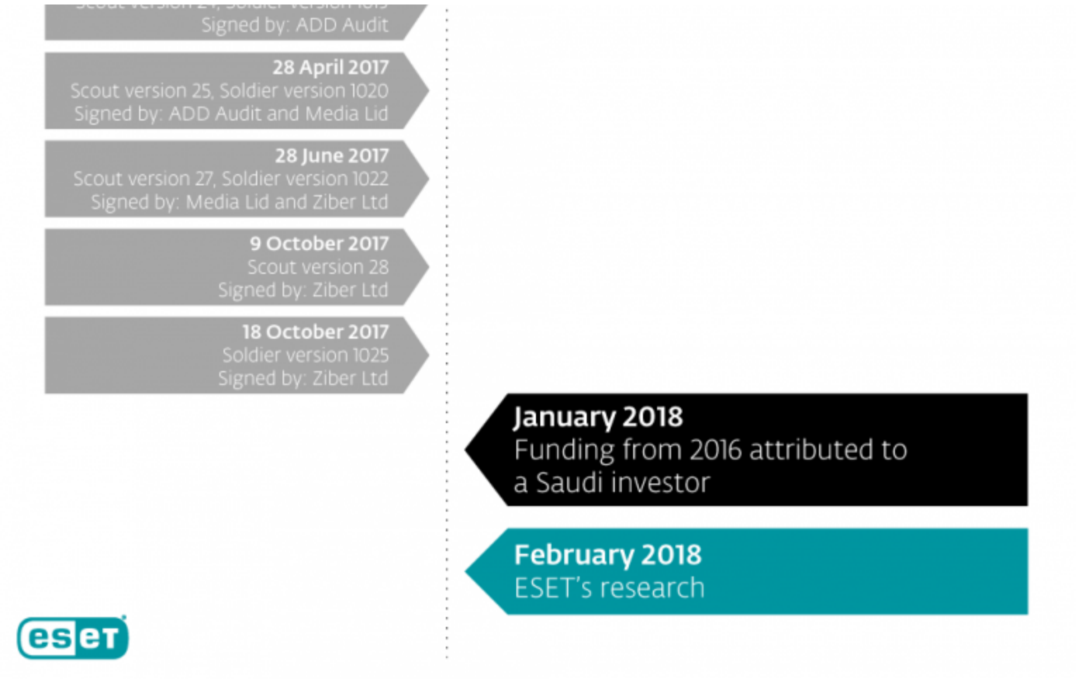


Figure 2 – Investigation timeline

Conclusion

Our research lets us claim with high confidence that, with one obvious exception, the post-leak samples we've analyzed are indeed the work of Hacking Team developers, and not the result of source code reuse by unrelated actors, such as in the case of Callisto Group in 2016.

As of this writing, our systems have detected these new Hacking Team spyware samples in fourteen countries. We choose not to name the countries to prevent potentially incorrect attributions based on these detections, since the geo-location of the detections doesn't necessarily reveal anything about the origin of the attack.

IoCs

ESET detection names
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

Samples signed by 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 samples
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

Samples signed by 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 samples
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

Samples signed by 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 samples

SHA-1 samples
27f4287e1a5348714a308e9175fb9486d95815a2
71a68c6140d066ca016efa9087d71f141e9e2806
dc817f86c1282382a1c21f64700b79fcd064ae5c

SHA-1 samples
27f4287e1a5348714a308e9175fb9486d95815a2
71a68c6140d066ca016efa9087d71f141e9e2806
dc817f86c1282382a1c21f64700b79fcd064ae5c

C&Cs
188.226.170.222
173.236.149.166

Samples signed by 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 samples
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

Samples signed by Raffaele Carnacina
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 samples
4ac42c9a479b34302e1199762459b5e775eec037
2059e2a90744611c7764c3b1c7dcf673bb36f7ab
b5fb3147b43b5fe66da4c50463037c638e99fb41
9cd2ff4157e4028c58cef9372d3bb99b8f2077ec
b23046f40fbc931b364888a7bc426b56b186d60e

SHA-1 samples
cc209f9456f0a2c5a17e2823bdb1654789fcadc8
99c978219fe49e55441e11db0d1df4bda932e021
e85c2eab4c9eea8d0c99e58199f313ca4e1d1735
141d126d41f1a779dca69dd09640aa125afed15a

C&Cs
199.175.54.209
199.175.54.228
95.110.167.74

Samples signed by Valeriano Bedeschi
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 samples
baa53ddba627f2c38b26298d348ca2e1a31be52e
5690a51384661602cd796e53229872ff87ab8aa4
aa2a408fcaa5c86d2972150fc8dd3ad3422f807a
83503513a76f82c8718fad763f63fcd349b8b7fc

C&Cs
172.16.1.206 – It is an internal address which was found in the samples.

Follow us

Sign up to our newsletter

The latest security news direct to your inbox

Email...

Submit