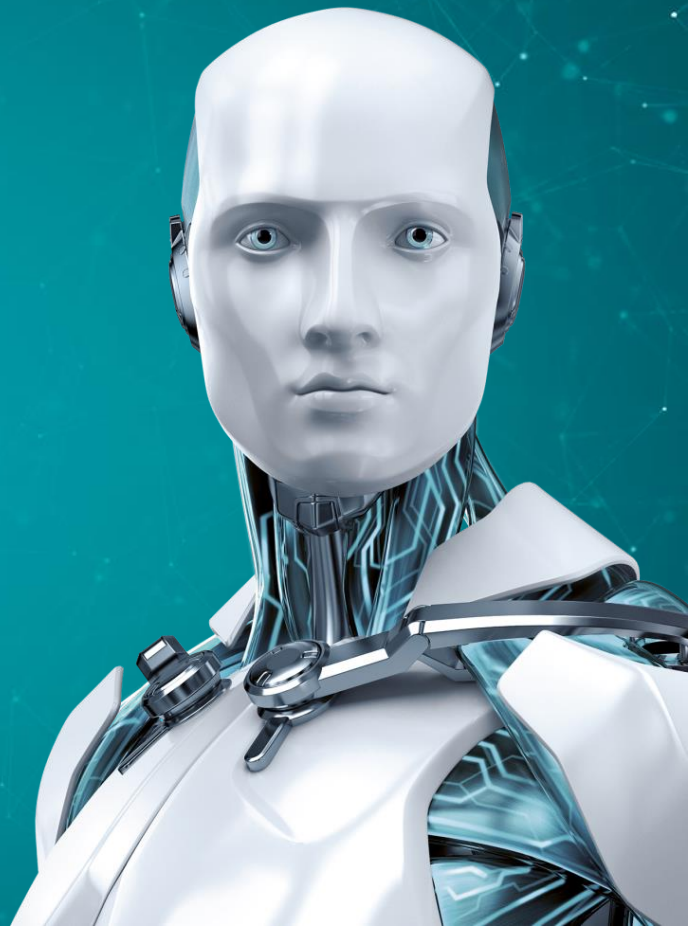
ENJOY SAFER TECHNOLOGY™

From HackingTeam to hacked team to… ?



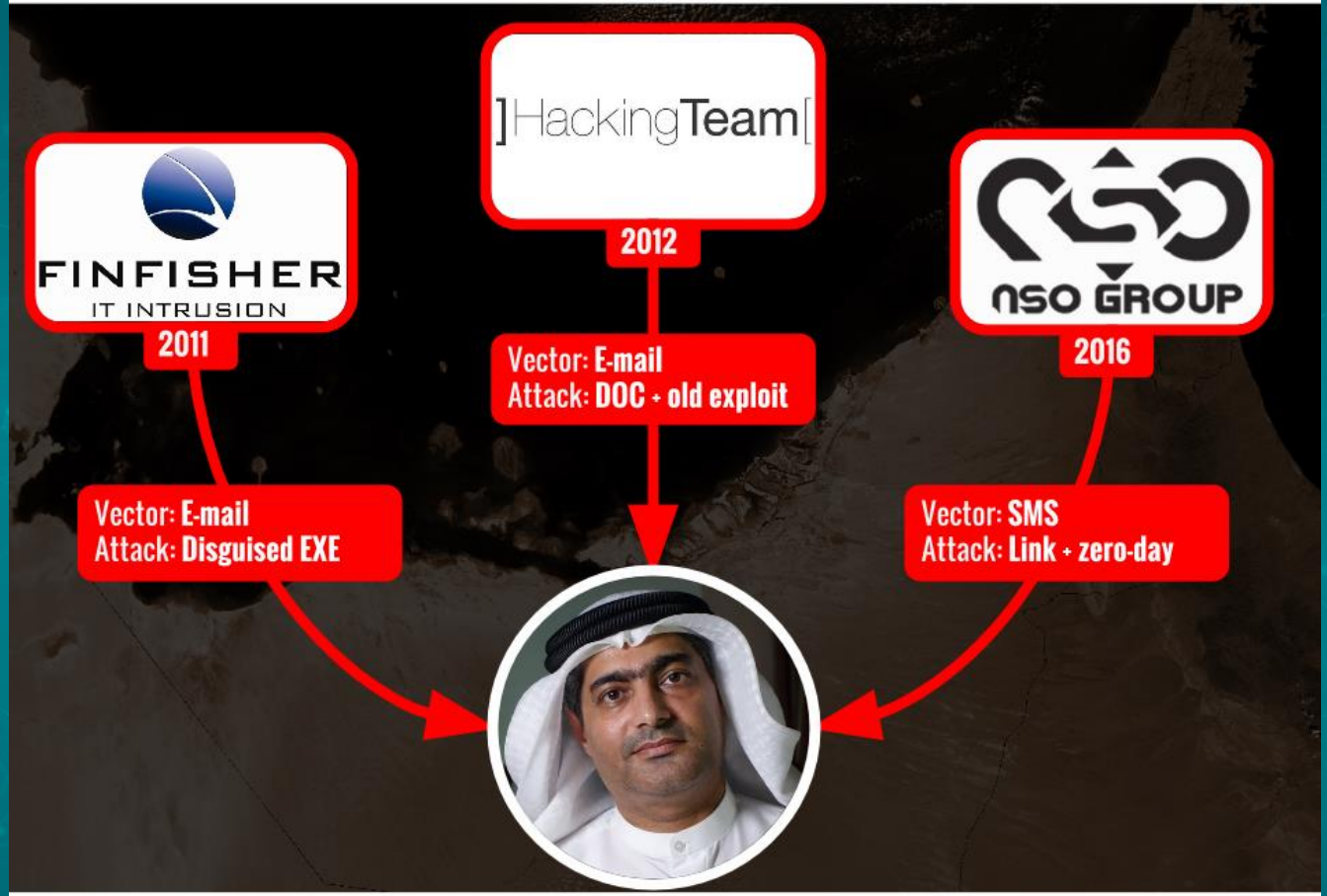
Filip Kafka | Malware researcher

2003
Hacking Team founded

July 2012
Dr. Web attributes the malware to Hacking Team

February 2014
The Citizen Lab reveals that Hacking Team was selling to oppressive governments

THREE "LAWFUL INTERCEPT" PRODUCTS USED AGAINST MANSOOR



From: Marczak & Scott-Railton
The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender

CITIZEN LAB 2016

2003
Hacking Team founded

July 2012
Dr. Web attributes the malware to Hacking Team

February 2014
The Citizen Lab reveals that Hacking Team was selling to oppressive governments

July 2015
Hacking Team hacked


]HT[
Hacked Team @hackingteam · 3h
Since we have nothing to hide, we're publishing all our e-mails, files, and source code mega.co.nz/#!Xx1IhChT!rbB...
infotomb.com/eyyxo.torrent

HACKED: FinFisher

Email-ID	65846
Date	2014-08-10 06:28:45 UTC
From	d.vincenzetti@hackingteam.com
To	list@hackingteam.it

Email Body | Raw Email

FinFisher, a wannabe competitor of ours, has been severely hacked.

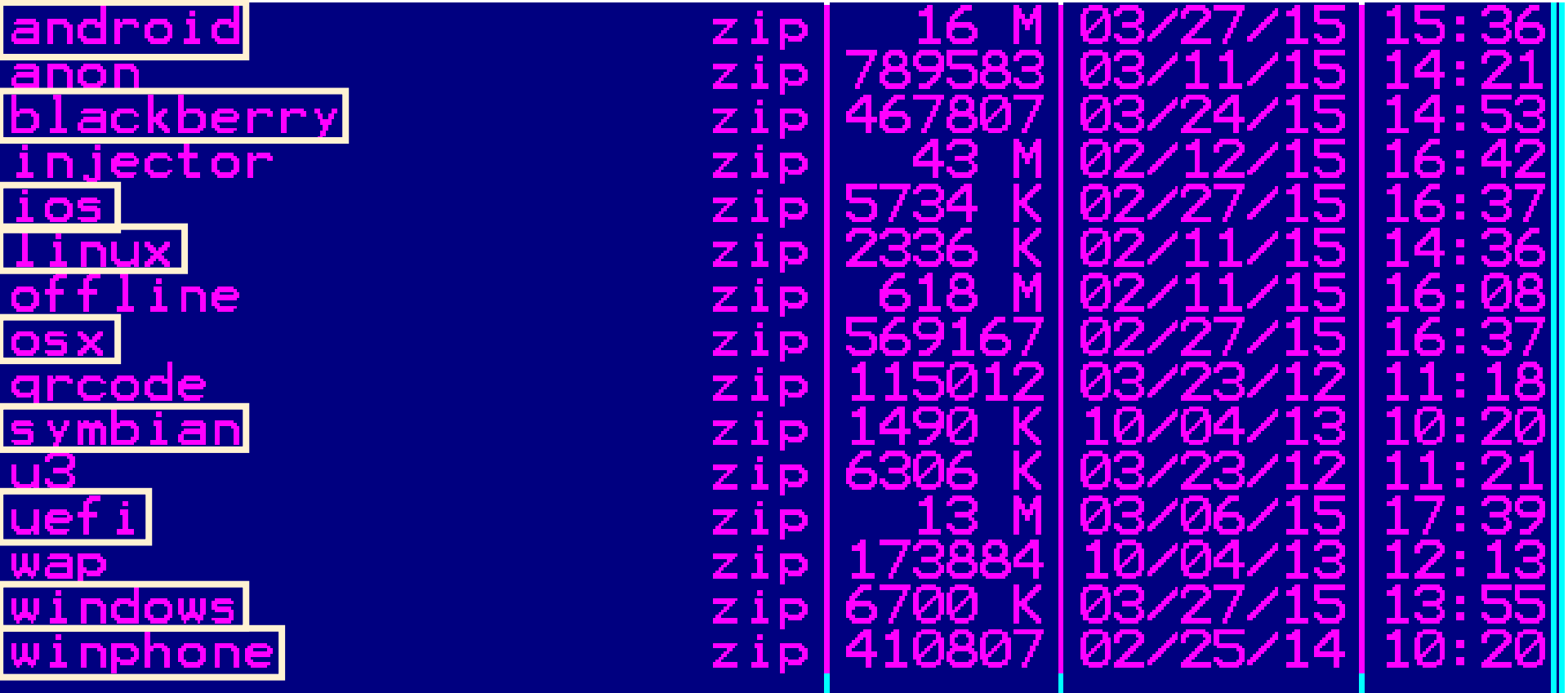
You can find information about it everywhere, just google "finfisher hacked".

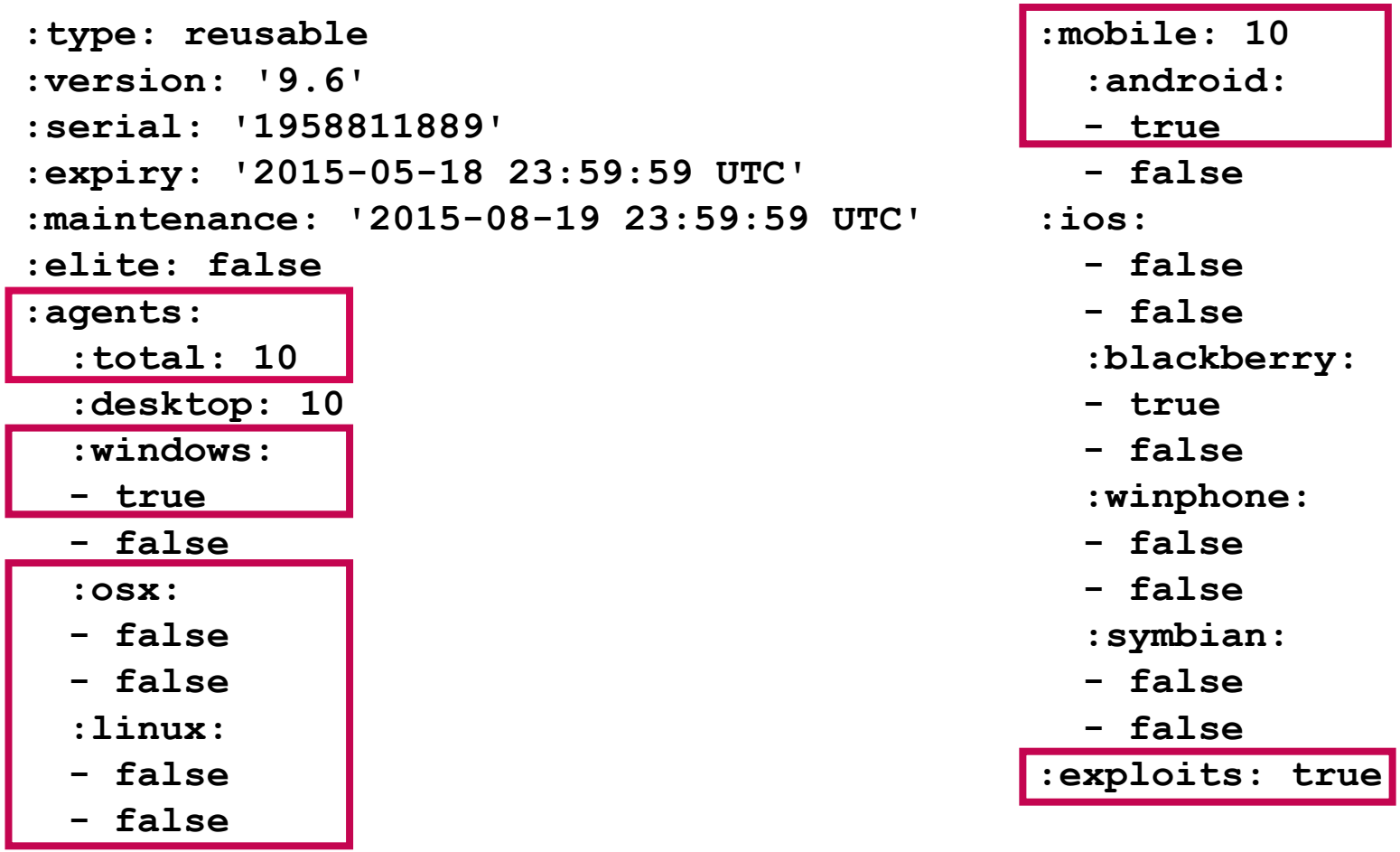
Here is an article: http://www.zdnet.com/top-govt-spyware-company-hacked-gammas-finfisher-leaked-7000032399/

FYI,
David

--
David Vincenzetti
CEO

Remote Control System (Galileo)




:type: reusable
:version: '9.6'
:serial: '1958811889'
:expiry: '2015-05-18 23:59:59 UTC'
:maintenance: '2015-08-19 23:59:59 UTC'
:elite: false
:agents:
:total: 10
:desktop: 10
:windows:
- true
- false
:osx:
- false
- false
:linux:
- false
- false
:mobile: 10
:android:
- true
- false
:ios:
- false
- false
:blackberry:
- true
- false
:winphone:
- false
- false
:symbian:
- false
- false
:exploits: true

2003
Hacking Team founded

July 2012
Dr. Web attributes the malware to Hacking Team

February 2014
The Citizen Lab reveals that Hacking Team was selling to oppressive governments

July 2015
Hacking Team hacked

January 2016
Callisto Group sample built from leaked source code (*reported by F-Secure in April 2017*)

April 2016
Hacking Team claims to have recovered from the hack in a statement on their website

June 2016
Hacking Team receives new funding (*reported by LaStampa*) from a Saudi investor (*reported by Motherboard in January 2018*)

May 2017
Mexico's prosecutor's office purchases Hacking Team spyware (*reported by El Diario in August 2018*)

February 2018
ESET analyses new samples

Distribution vector of modified HT spyware

- “Requirement for Diplomatic Passport Service.pdf.t.exe”
- “Note Verbale No 00023AM-ADD2017 du 17 janvier 2017 .exe”
- “Petition 2017 rasdt.....t.exe”
- “rawshi nawaxoy harim kurdstan.exe”

Distribution vector of modified HT spyware

- “Requirement for Diplomatic Passport Service.pdf.t.exe”
  - Origin: mfa.gov.et@gmail.com

Windows agents

- 1st stage: Scout
- 2nd stage: Soldier or Elite
- VMProtected

Scout

- 1st agent to be deployed
- Installs, checks if other instances are already running
- AV bypass tricks
- Collects basic information on the computer
- Watches possible upgrades of itself / to Soldier / to Elite

Soldier

- 2nd stage
- Collected data encrypted, packed and stored in registry. Later sent to C&C by another thread
- Advanced software architecture → improved
- Proper memory management, error handling

Functionality of Soldier

IMs

Emails

Files

Geolocation

Photos

Contacts

Functionality of Soldier

- Collecting information from social networks
- Clipboard stealing
- Stealing passwords from browsers
- Taking screenshots
- Recording with camera

Functionality of Soldier

- Collecting information from social networks
- Clipboard stealing
- Stealing passwords from browsers
- Taking screenshots
- Recording with camera
- Geolocation

Functionality of Soldier

- Collecting information from social networks
- Clipboard stealing
- Stealing passwords from browsers
- Taking screenshots
- Recording with camera
- Geolocation
- URLs

Functionality of Soldier

- Collecting information from social networks
- Clipboard stealing
- Stealing passwords from browsers
- Taking screenshots
- Recording with camera
- Geolocation
- URLs
- New: recording Skype calls, keylogging, screenshot-on-click, scheduling uninstallation

Technical details - Soldier’s configuration


```
{"camera":{"enabled":false,"repeat":0,"iter":0},"position":{"enabled":false,"repeat":0},"screenshot":{"enabled":true,"repeat":120},"photo":{"enabled":false},"file":{"enabled":false},"addressbook":{"enabled":false},"chat":{"enabled":false},"clipboard":{"enabled":false},"device":{"enabled":true},"call":{"enabled":false},"messages":{"enabled":false},"password":{"enabled":false},"keylog":{"enabled":false},"mouse":{"enabled":false},"url":{"enabled":false},"sync":{"host":"149.154.153.223","repeat":120},"uninstall":{"date":null,"enabled":false}}
```

Is it really Hacking Team?

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;
```

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
```

PRE-LEAK

```
void __cdecl AppendRandomData_old(int a1, unsigned int a2)
{
  unsigned int v2; // esi@1
  unsigned int v3; // eax@1

  v2 = 0;
  v3 = GetTickCount();
  srand(v3);
  dword_422F1C = 0;
  if ( a2 > 0 )
  {
    do
      *(_BYTE *)(v2++ + a1) = rand();
    while ( v2 < a2 );
  }
}
```

POST-LEAK

```
void __cdecl AppendRandomData(BYTE *pbBuffer, DWORD dwLen)
{
  HCRYPTPROV phProv; // [esp+0h] [ebp-4h]@1

  phProv = 0;
  if ( CryptAcquireContextW(&phProv, 0, 0, 1u, CRYPT_INITIATOR|CRYPT_VERIFYCONTEXT) )
  {
    CryptGenRandom(phProv, dwLen, pbBuffer);
    CryptReleaseContext(phProv, 0);
  }
  else
  {
    AppendRandomData_old((int)pbBuffer, dwLen);
  }
}
```

PRE-LEAK

```
VOID MySleep(ULONG uTime)
{
        //HANDLE hThread = GetCurrentThread();
        //WaitForSingleObject(hThread, uTime);
        Sleep(uTime);
}
```

POST-LEAK

```
; int __cdecl mySleep(DWORD dwMilliseconds)
mySleep proc near

dwMilliseconds= dword ptr  4

push    esi
xor     eax, eax
push    eax; lpName
push    eax; bInitialState
push    1; bManualReset
push    eax; lpEventAttributes
call    ds:CreateEventW
push    [esp+4+dwMilliseconds]; dwMilliseconds
mov     esi, eax
push    esi; hHandle
call    ds:WaitForSingleObject
push    esi; hObject
call    ds:CloseHandle
pop     esi
retn
mySleep endp
```

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

Issued to: Ziber Ltd

Issued by: thawte SHA256 Code Signing CA

Valid from 7/ 9/ 2017 **to** 7/ 10/ 2018

Install Certificate... | Issuer Statement

Learn more about certificates

OK

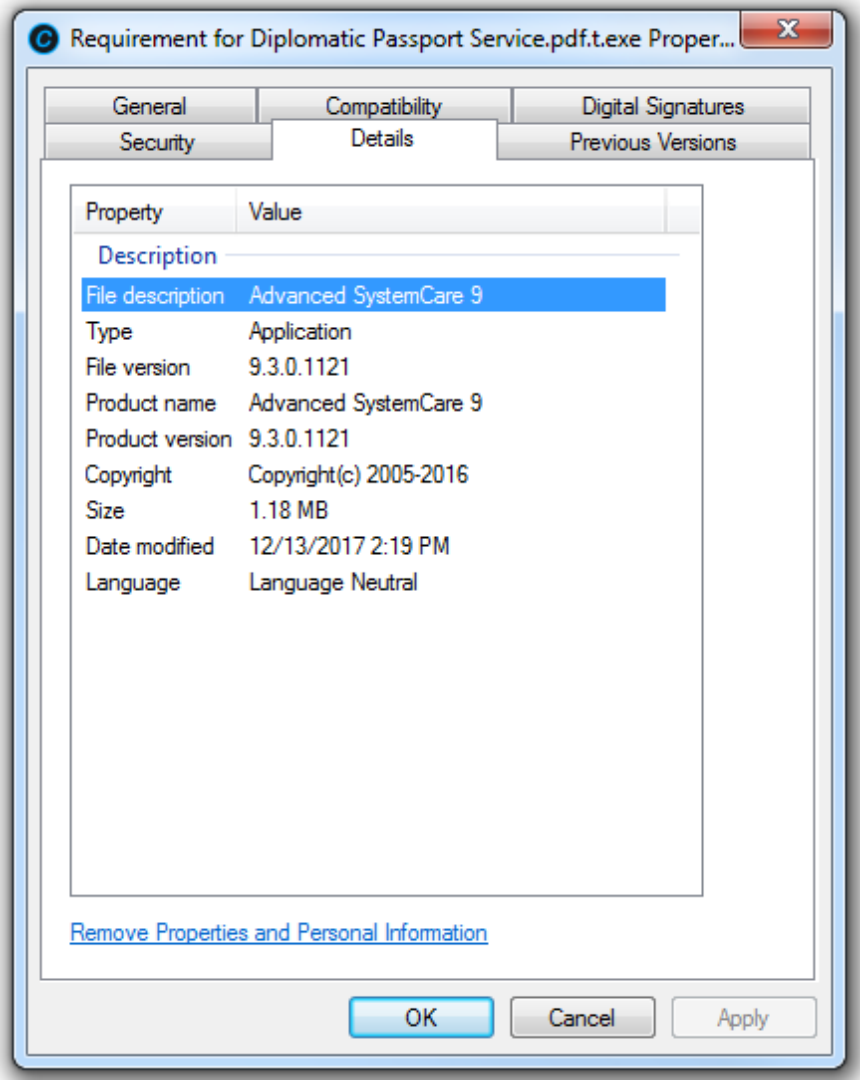
Certificate issued to	Validity period
Valeriano Bedeschi	8/13/2015 – 8/16/2016
Raffaele Carnacina	9/11/2015 – 9/15/2016
Megabit, OOO	6/8/2016 – 6/9/2017
ADD Audit	6/20/2016 – 6/21/2017
Media Lid	8/29/2016 – 8/30/2017
Ziber Ltd	7/9/2017 – 7/10/2018

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
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

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
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

Scout name

```
From: 9.4.0
To:   9.4.1
scout_names = [
    {name: '8169Diag', version: '2.0.2.3', de
    , company: 'Realtek Semiconductor Corpora
    2012 Realtek Semiconductor Corporation' }
    {name: 'CCleaner', version: '4.14.00.4707
    'Piriform Ltd', copyright: 'Copyright (c)
    {name: 'Linkman', version: '8.9.3.1', des
    copyright: '(c) 1997-2014 by Outertech' }
    {name: 'PCSwift', version: '1.0.0.0', des
     copyright: 'Copyright (c) 2014 PGWARE LL
    {name: 'PerfTune', version: '2.1.408.35',
    Corporation', copyright: 'Copyright(c) 20
    {name: 'SystemOptimizer', version: '8.2.0
    , company: 'Digeus, Inc.', copyright: 'Co
]
```



Scout name

```
From: 9.4.0
To:   9.4.1
scout_names = [
    {name: '8169Diag', version: '2.0.2.3', desc: 'Realtek NIC Diagnostic Utility'
    , company: 'Realtek Semiconductor Corporation', copyright: 'Copyright (C)
    2012 Realtek Semiconductor Corporation' },
    {name: 'CCleaner', version: '4.14.00.4707', desc: 'CCleaner', company:
    'Piriform Ltd', copyright: 'Copyright (c) 2005-2014 Piriform Ltd' },
    {name: 'Linkman', version: '8.9.3.1', desc: 'Linkman', company: 'Outertech',
    copyright: '(c) 1997-2014 by Outertech' },
    {name: 'PCSwift', version: '1.0.0.0', desc: 'PCSwift', company: 'PGWARE LLC',
     copyright: 'Copyright (c) 2014 PGWARE LLC' },
    {name: 'PerfTune', version: '2.1.408.35', desc: 'PerfTune', company: 'Intel
    Corporation', copyright: 'Copyright(c) 2010 Intel Corporation' },
    {name: 'SystemOptimizer', version: '8.2.0.0', desc: 'Digeus System Optimizer'
    , company: 'Digeus, Inc.', copyright: 'Copyright (c) Digeus 2005-2010' }
]
```

Export name

```
/*      ------------- PUNTO 6 CRISIS PROCEDURE - EXPORT NAME -------

        EXPORT HISTORY
                        jfk31d1QQ
                        reuio841001a
                        pqjjslanf
                        robertlee
(RCS 9.4)       eflmakfil
(RCS 9.5)   hardreset
*/


PWCHAR expprochd(PULONG pSynchro) // questa viene richiamata dai meltati
{
```

User agent

```
/*      ------------- PUNTO 3 CRISIS PROCEDURE - USER_AGENT---------

        USER_AGENT HISTORY

                        Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0
                        Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.7.10) Gecko/20050716
                        Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
(RCS 9.4)       Mozilla/5.0 (Windows NT 6.1; rv:27.3) Gecko/20130101 Firefox/27.3
(RCS 9.5)   Mozilla/5.0 (Windows NT 6.1; WOW64; rv:29.0) Gecko/20120101 Firefox/29.0
*/

#define USER_AGENT L"Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)"
```

URL sync

```
/*      ------------- PUNTO 4 CRISIS PROCEDURE - URL SYNC ----------

        POST_PAGE HISTORY

                          /rss.asp
(RCS 9.4)        /home.php
(RCS 9.5)    /default.asp
*/

#define POST_PAGE  L"/index.php"
```

Export name

- 15 – “compatibility”
- 17 – “_ZN4DecC1Ev”
- 18 – “IsPointerDeviceAccessible”
- 21 – “GetMemSize”
- 22 < “IsProcessParent”

User agents

- 15 – Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.107 Safari/537.36
- 17 – Mozilla/5.0 (compatible, MSIE 11, Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
- 18 – Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.116 Safari/537.36
- 25 – Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko
- 28 – Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36

Names

- 15 – BoostSpeed
- 18 – CPUID Hardware Monitor
- 27 – Advanced SystemCare 9
- 27 – Toolwiz Care
- 30 – NVIDIA Control Panel Application
- 30 – MS One Drive

URL sync

- 15 – /update.cfm
- 17 – /default.html
- 18 – /local.aspx
- 21 – /home.html
- >22 – /index.html

Post-hack HT findings

- Non-technical reports on HT post hack activities
- Digital certificates, started with HT co-founder
- Very good knowledge of the code – changes, which wouldn’t be done by somebody reusing the code
- Smooth versioning of the spyware
- Frequent changes – typical HT procedures:
  - changes in the code at exactly the same places where HT developers were doing it (Crisis procedures)
  - masquerading by a legitimate application – description and icon

Why they didn’t rewrite their products completely?

New HackingTeam activity

- New spyware sign with digital certificates issued to companies:
  - Auxira Ltd
  - IKB SERVICE UK LTD

Conclusion

- Worth tracking – questionable customers, potential for 0days, even UEFI rootkit, …
- Still in business => everyone can survive a data breach?
- Big and evolving business
- No need to steal certificates – buy their own instead

ENJOY SAFER TECHNOLOGY™

Filip Kafka

Malware researcher

filip.kafka@eset.com, @filip_kafka

www.eset.com | www.welivesecurity.com