Appendix: Analysis of the Mokes/SmokeBot backdoor from the incident

This is a technical analysis of the Mokes/SmokeBot malware sample involved in the incident.

Sample technical information:

MD5: a82c0575f214bdc7c8ef5a06116cd2a4
Size: 793,088 bytes

The file is a self-extracting CAB archive. Contents of the embedded CAB archive:

```
 File size | Date       | Name
-----------+------------+-------------
    600697 | 05.11.2013 | steam.exe
    229376 | 05.11.2013 | setup.exe
```

The "setup.exe" from the CAB archive acts as a replacement of the original "setup.exe" installation program for the Microsoft Office 2013 suite. The CAB SFX is configured to run both executables from the archive, “steam.exe” and “setup.exe”.
The purpose of these files is as following:

- "steam.exe" malicious dropper
- "setup.exe" - Office 2013 installation bootstrapper

The self-extracting CAB executable appears to be based on the legitimate "IExpress" toolset.

Decoy executable, "setup.exe"

Technical information:

```
SHA256          08378aca35beaba76b9cb6458678052427eacb67ac3f91c7b4e6897115df3938
MD5             9e1709c39f3620ef599321c0fdde0658
Compiled        2012.09.29 18:47:49 (GMT), 10.10
Type            AMD64 Windows GUI EXE
Size            229376 bytes
```

This binary is an Office 2013 installation bootstrapper that loads the legit installation library "setup.dll".

Internal version information suggests this is a Microsoft Corporation's "setup.exe", version 15.0.4420.1017 taken from the Microsoft Office 2013 installation disk. However, the digital signature does not validate.

Malicious dropper, "steam.exe"

Technical information:

```
SHA256        6317e69c9adfb17b7787e888cead25fd583c84511de94d35eeabc35feb3c0209
MD5           8bc78aa3dd8cb46ea5021ae6e72be094
Compiled      2012.06.09 13:19:49 (GMT), 9.0
Type          I386 Windows GUI EXE
Size          600697 bytes
Internal name WINRAR.SFX
```

This is a RAR SFX (self-extracting) archive. Contents of the embedded RAR archive:

```
Size   |  Date     | Name
-------+-----------+----------
   9736  2013-11-05 65159.QHR
 750320  2012-01-29 lvku.exe
     56  2013-11-05 2929830.vbs
7170716  2013-11-05 2293423.SGY
     82  2013-11-05 35118.YEN
```

The comment section that controls the behaviour of the executable is obscured by random strings placed between actual commands. The meaningful part of the comments is the following, instructing the program to execute the Visual Basic script file from the archive:

```
Silent=1
Overwrite=2
Path=%userprofile%\hvgpj
Setup="2929830.vbs"
```

The VBS file (“`2929830.vbs`”) is a one-liner executing the next stage from the archive:

```
CreateObject("WScript.Shell").Run "lvku.exe 2293423.SGY"
```

AutoIt runtime environment, "lvku.exe"

Technical information:

```
SHA256        fb73a819b37523126c7708a1d06f3b8825fa60c926154ab2d511ba668f49dc4b
MD5           71d8f6d5dc35517275bc38ebcc815f9f
Compiled      2012.01.29 21:32:28 (GMT), 10.0
```

```
Type          I386 Windows GUI EXE
Size          750320 bytes
```

The "lvku.exe" is an AutoIt scripting language interpreter. It executes the scripts provided by the GUI or as a command line parameter, in this case the malicious script file "2293423.SGY". The EXE file is signed by "AutoIt Consulting Ltd." on 2012.01.29. This component is not malicious, but it is used to execute the malicious script.

Malicious AutoIt script, "2293423.SGY"

Technical information:

```
SHA256        8073570cd92f34052448381089a4819614b7791a0ac5bdf0ee534a43adb959e8
MD5           90863477d05cff43e74072c11cef61cb
Type          AutoIt script
Size          7170716 bytes
```

Once started, the script checks if there is an active process for an executable named "avastui.exe", and if present, delays its execution by 20 seconds. It also ensures that its process is not being debugged and that it is run from the location "%USERPROFILE%\hvgpj" or any other subdirectory (not the root directory of any disk), otherwise it triggers a critical error condition causing the "blue screen of death" and forcing the OS to reboot.

The script reads its configuration from an external file named "35118.YEN" located in the same directory. According to the settings, it creates the files "start.vbs" and "start.cmd" in the same directory and next:

- attempts to create a shortcut "start.lnk" pointing to the "start.vbs" file in the startup folder
- creates a registry value "hvgpj" in the registry key "HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce", the value pointing to the "start.vbs" script

The script then reads the contents of the file named "65159.QHR" from its directory, decrypts the data using RC2 with the key "hvgpj" and injects the resulting PE file in a new process, created from one of following three executables:

- %WINDOWS%\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
- %WINDOWS%\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
- %path to the default Internet browser executable%

The payload is written into the target process and then executed. The PE loader code is based on AutoIt scripts available on several public AutoIt forums, i.e.:

- hxxp://autoit-script.ru/index.php?topic=5338.0
- hxxs://www.autoitscript.com/forum/topic/99412-run-binary/?page=8

Binary loader, "65159.QHR"

Technical data:

```
MD5    (original)    1d9872a6698cb9e4991a65a3ae155a15
SHA256 (original)
ad4bfbe93da44a05dc2f3ba7fe0545d1c4ae4f37cec1e7945ba1662fdd5abd0e
Size   (original)    9736
```

This file is encrypted with RC2. The metadata for the decrypted executable follows:

```
SHA256         9e1a0a47aae6058dd4e931b1eced5cd6948b84bc9fdf6f1169db04c358ec904b
MD5            a9fb872545e1581c7896434196857cc2
Compiled       2012.11.13 11:08:11 (GMT), 5.12
Type           I386 Windows GUI EXE
Size           9728
```

The executable was created with MASM 6 and consists of a single ".text" section containing both code and data. It employs several anti-debugging and anti-sandbox techniques, such as:

- if the application is being debugged
- if the application's filename contains the string "sample" in it
- if the system volume's serial number is equal to 0xCD1A40 (appears to be used by ThreatExpert)
- if the name of the first disk device contains the strings corresponding to common virtualization solutions: "virtual", "vmware", "qemu"
- if the current process contains a loaded copy of libraries named "dbghelp" or "sbiedll"

The module starts a new process for "svchost.exe" and injects the next stage of the malware into that process.

The entrypoint of the process is modified to directly execute the injected payload. The payload is a shellcode that decompresses a DLL file embedded into its body using apLib and calls its export, "Work".

Final backdoor, "Stub.dll"

Technical information:

```
SHA256         c752074f51882960ffa5e5fe0e4881bbae147c10ad0d68089d8458128b1eff61
MD5            c7f6cc7cbbb293f9c90bfcad187bef31
Compiled       1992.06.19 22:22:17 (GMT), 2.25
Type           I386 Windows GUI DLL
Size           13824
Internal name Stub.dll
```

The final backdoor checks if the system has an available internet connection by sending HTTP GET requests to "http://windowsupdate.microsoft.com/" every 10 minutes and waiting for a “long enough” page reply (>9 bytes).

Next, it generates a unique bot ID based on the serial number of the system volume, CRC32 of the computer name and a unique DWORD identifier hardcoded in the body of the module.

To receive commands, it connects to one of the C&C servers:

- hxxp://xvidmovies.in/dir/index.php
- hxxp://freecodecs.in/dir/index.php

An optional configuration file, located in %APPDATA%\%unique 6 hex chars%\%unique 6 hex chars%.dat, may contain an encrypted URL of an additional C&C server. The hexadecimal string is unique for each user and is based on the bot ID.

The data sent by the bot is a set of HTTP parameters encoded in a POST request, encrypted and then base64-encoded. The bot uses the system default User-Agent string for HTTP requests, or a "Mozilla/4.0" as a default value.

Depending on the response from the C&C server, the bot can:

- Write a C&C update file to disk
- Load a DLL
- Execute the "Regsvr32.exe" application to register a DLL
- Execute an arbitrary file

The C&C server may also provide an arbitrary number of DLL plugins, each expected to export a function called "Work". All these plugins are loaded and activated in memory.

These functionalities give the operators full access to an infected machine.

Additional information

The top sample described here was first seen in the wild by Kaspersky users on 2013-11-06 08:41. The filename and folder where it was detected was "microsoft office 2013 professional plus x64 (64 - bit)\setup.exe", file container: office-2013-ppvl-x64-en-us-oct2013.iso.

Analysis of Smoke Bot C&C servers

Xvidmovies[.]in

According to whois history, this domain was first registered on 19-Apr-2012 22:15:11 UTC. The initial registrant had the following information:

```
Registrant Name:Yasir shah
Registrant Organization:
Registrant Street1:sidsons building preedy street saddar karachi
Registrant Street2:
Registrant Street3:
Registrant City:MUMBAI
Registrant State/Province:mahrashtra
Registrant Postal Code:74400
Registrant Country:IN
Registrant Phone:+91.3333160834
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant Email:gemini.yasu@gmail.com
```

The domain was renewed on 24-Apr-2013, for a period of one more year:

```
Created On:19-Apr-2012 22:15:11 UTC
Last Updated On:03-May-2013 20:22:50 UTC
Expiration Date:19-Apr-2014 22:15:11 UTC
Sponsoring Registrar:Dynadot LLC (R117-AFIN)
```

The domain expired in April 2014 and was picked up by a different threat actor. The new registration had the following information:

```
Created On:04-Jul-2014 23:58:23 UTC
Last Updated On:04-Jul-2014 23:58:24 UTC
Expiration Date:04-Jul-2015 23:58:23 UTC
Sponsoring Registrar:Webiq Domains Solutions Pvt. Ltd. (R131-AFIN)
Status:CLIENT TRANSFER PROHIBITED
Status:TRANSFER PROHIBITED
Status:ADDPERIOD
Registrant ID:DI_22666182
Registrant Name:Zhou Lu
Registrant Organization:Zhou Lu
Registrant Street1:Room 503
Registrant Street2:
Registrant Street3:
Registrant City:shaoyang
Registrant State/Province:Hunan
Registrant Postal Code:422000
Registrant Country:CN
Registrant Phone:+86.13973960749
Registrant Phone Ext.:
Registrant FAX:
```

```
Registrant FAX Ext.:
Registrant Email:zhoulu823@gmail.com
```

The domain was under the control of “Zhou Lu” until July 2015, when it expired again and was deleted. We’ve sinkholed it for research purposes on 25 Oct 2017.

During September - November 2014, in which the incident involving the presumed NSA employee took place, the domain was under the control of the “Zhou Lu” actor.

Freecodecs[.]in

This domain has a longer history than xvidmovies[.]in. It was first registered on 2-Dec-2007 19:07:25 UTC. The initial registrant had the following information:

```
Registrant Name:O.Sudarsono
Registrant Organization:DXM
Registrant Street1:Perintis Kemerdekaan 4
Registrant Street2:
Registrant Street3:
Registrant City:Purwokerto
Registrant State/Province:Jawa Tengah
Registrant Postal Code:53252
Registrant Country:ID
Registrant Phone:+062.281635768
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant Email:onosoed@yahoo.com
```

Upon the expiration of the first registration (2008) the domain was extended for another year, until it finally expired on 22-Dec-2009.

The domain was picked again on 16-Apr-2010 by another entity:

```
Registrant Name:faisal shah
Registrant Organization:
Registrant Street1:sidsons building preedy street saddar karachi
Registrant Street2:
Registrant Street3:
Registrant City:MUMBAI
Registrant State/Province:mahrashtra
Registrant Postal Code:74400
Registrant Country:IN
Registrant Phone:+91.3333160834
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant Email:ffaisalshah@hotmail.com
```

Upon expiration, the domain was registered again, this time by “Yasir Shah”, on 16 Apr 2010, for a period of two years:

```
Created On:16-Apr-2010 22:17:32 UTC
Last Updated On:19-Feb-2012 19:21:20 UTC
Expiration Date:16-Apr-2012 22:17:32 UTC

Registrant Name:Yasir shah
Registrant Organization:
Registrant Street1:sidsons building preedy street saddar karachi
Registrant Street2:
Registrant Street3:
Registrant City:MUMBAI
Registrant State/Province:mahrashtra
Registrant Postal Code:74400
Registrant Country:IN
Registrant Phone:+91.3333160834
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant Email:gemini.yasu@gmail.com
```

It should be noted that Yasir Shah also registered the other C&C domain, Xvidmovies[.]in. It was further renewed for two more years, until 16-Apr-2014 when the domain expired and was deleted. Unlike the first, this domain was not active at the time of the September - November 2014 incident.

References:

- https://blog.fox-it.com/tag/ësmoke-loader/
- http://stopmalvertising.com/rootkits/analysis-of-smoke-loader.html
- https://blog.fortinet.com/2014/11/12/the-rebirth-of-dofoil