Gheg: Marshal8e6

Contact Us 877.369.8686 MARSHAL8e6

Gheg

March 17, 2009

Aliases

- Tofsee
- Mondera

Comments

Gheg, also known as Tofsee or Mondera, came across our radar in October 2008. It is not as sophisticated as some of the other bots like Rustock or Srizbi, for example it does not use a rootkit to hide itself. But it does a reasonable job sending spam at approximately 7000 messages per hour per bot using a template-based spamming engine. Gheg tends to concentrate on pharmeceutical spam, using an Outlook Express template formatted in either plaintext or HTML.

Features

- Template Based spamming engine
- Uses port 443 (SSL) to send and receive encrypted commands, spam templates and download executable files.

Spamming Rate

7,000 msgs per hour per bot

Command and Control

The Gheg bot connects to its control server using a non-standard SSL connection on port 443. Samples we have analyzed connect to 208.72.168.140, establishing a connection to its control server using the HTTP request like the one below:

> GET /1464 HTTP/1.0
> Host: <C&C server IP Address>
>
> GET /3164 HTTP/1.0
> Host: <C&C server IP Address>

After a successful connection, Gheg receives encrypted commands and spam templates from the control server.

Malware Behavior on Host

Gheg drops a copy of itself in the following folder:

- %userprofile% (C:\Documents and Settings\<username>)
- %SystemRoot%\system32\ (C:\Windows\System32)

The malware filename format is 4-6 random characters with .EXE extension, for example:

- %UserProfile%\rkux.exe
- %SystemRoot%\system32\cvfjt.exe

A batch file was temporarily created to delete the main executable, it uses the following format:

> %temp%\removeme<4 random digit>.bat (where %temp% is Windows default temporary folder).

To automatically execute the trojan in the system start-up, it adds the following registry entries:

- HKEY_Local_Machine\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
  "Userinit" = "%SystemRoot%\system32\userinit.exe, %userprofile%\<random filename of malware.exe>"
- HKEY_Local_Machine\Software\Microsoft\Windows\CurrentVersion\Run
  "<Random>.exe" = " %SystemRoot%\system32\<random>.exe"

Gheg also lowers Internet Explorer Security settings by modifying the following registry entries:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
  WarnOnPost = hex:00,00,00,00,
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2
  - MinLevel = dword:00000000

- RecommendedLevel = dword:0000000
- 1004 = dword:00000000
- 1201 = dword:00000000
- 1609 = dword:00000000

Gheg also sets itself to bypass the Windows firewall by using NETSH command (netsh firewall set allowedprogram "<name of malware>") and to identify itself in the infected machine, Gheg creates a mutex named "ghegdjf" - from which its name derives.

Last Reviewed: April 20, 2009 by Rodel Mendrez