TROJ64_WOWLIK.VT

trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj64_wowlik.vt

Analysis by: Alvin John Nieto

- 
  Threat Type: Trojan
- 
  Destructiveness: No
- 
  Encrypted: Yes
- 
  In the wild: Yes

OVERVIEW

Infection Channel: Downloaded from the Internet, Dropped by other malware

This Trojan arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.

TECHNICAL DETAILS

File Size: 24,064 bytes

File Type: DLL

Memory Resident: Yes

Initial Samples Received Date: 10 Apr 2014

Payload: Connects to URLs/IPs

Arrival Details

This Trojan arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.

Installation

This Trojan injects codes into the following process(es):

- %Windows%\explorer.exe
- %System%\dllhost.exe

(Note: *%Windows%* is the Windows folder, which is usually C:\Windows.. *%System%* is the Windows system folder, which is usually C:\Windows\System32.)

Autostart Technique

This Trojan adds the following registry entries to enable its automatic execution at every system startup:

HKEY_CURRENT_USER\Software\Classes\
clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\inprocserver32
[Default] = "\\?\globalroot\Device\{Harddisk volume #}\{malware path}\{malware name}"

HKEY_CLASSES_ROOT\CLSID\{fbeb8a05-beee-4442-804e-409d6c4515e9}\
InProcServer32
[Default] = "\\?\globalroot\Device\{Harddisk volume #}\{malware path}\{malware name}"

(Note: The default value data of the said registry entry is *%System%\SHELL32.dll*.)

Other Details

This Trojan connects to the following possibly malicious URL:

> http://{URL declared in 'wow.ini'}/cmd?version=1.5&aid={value}&id={GUID}&os={OS version}_{service pack}_{architecture}

It requires the existence of the following files to properly run:

> wow.ini

NOTES:

This Trojan sets the attribute of itself to *Hidden*.

This Trojan may connect to the URLs declared *wow.ini* for the following purposes:

- Update the configuration file
- Update itself
- Load additional modules

SOLUTION

Step 1

Before doing any scans, Windows XP, Windows Vista, and Windows 7 users must disable *System Restore* to allow full scanning of their computers.

Step 2

Identify and delete files detected as TROJ64_WOWLIK.VT using either the Startup Disk or Recovery Console

[Learn More]

Step 3

Delete this registry value

[Learn More]

Important: Editing the *Windows Registry* incorrectly can lead to irreversible system malfunction. Please do this step only if you know how or you can ask assistance from your system administrator. Else, check this Microsoft article first before modifying your computer's registry.

In *HKEY_CURRENT_USER\Software\Classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\inprocserver32*
[Default] = "\\?\globalroot\Device\{Harddisk volume #}\{malware path}\{malware name}"

Step 4

Restore this modified registry value

[Learn More]

Important: Editing the *Windows Registry* incorrectly can lead to irreversible system malfunction. Please do this step only if you know how or you can ask assistance from your system administrator. Else, check this Microsoft article first before modifying your computer's registry.

In *HKEY_CLASSES_ROOT\CLSID\{fbeb8a05-beee-4442-804e-409d6c4515e9}\InProcServer32*
From: **[Default] = "\\?\globalroot\Device\{Harddisk volume #}\{malware path}\{malware name}"**
To: **[Default] = "%System%\SHELL32.dll"**

Step 5

Scan your computer with your Trend Micro product to delete files detected as TROJ64_WOWLIK.VT. If the detected files have already been cleaned, deleted, or quarantined by your Trend Micro product, no further step is required. You may opt to simply delete the quarantined files. Please check this Knowledge Base page for more information.

Did this description help? Tell us how we did.