Worm.Win32.PYFILEDEL.AA

trendmicro.com/vinfo/us/threat-encyclopedia/malware/worm.win32.pyfiledel.aa

Analysis by: Carl Maverick Pascual

- 
  Threat Type: Worm
- 
  Destructiveness: Yes
- 
  Encrypted:
- 
  In the wild: Yes

OVERVIEW

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

It drops copies of itself in removable drives. These dropped copies use the names of the folders located on the said drives for their file names.

TECHNICAL DETAILS

Arrival Details

This Worm 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 Worm drops a copy of itself in the following folders using different file names:

%System Root%\boots\syswin.exe

(Note: *%System Root%* is the Windows root folder, where it usually is C:\ on all Windows operating system versions.)

It adds the following processes:

- tasklist.exe /fo csv
- %System Root%\boots\syswin.exe

(Note: *%System Root%* is the Windows root folder, where it usually is C:\ on all Windows operating system versions.)

It creates the following folders:

> %System Root%\boots

(Note: *%System Root%* is the Windows root folder, where it usually is C:\ on all Windows operating system versions.)

Autostart Technique

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

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run
syswin = "%System Root%\boots\syswin.exe"

Propagation

This Worm searches for folders in all physical and removable drives then drops copies of itself inside the folder as {folder name}.EXE.

It drops copies of itself in removable drives. These dropped copies use the names of the folders located on the said drives for their file names.

Other Details

This Worm does the following:

> It modifies .exe files in all drives and directory to a size of zero byte, making it unusable.

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

Note that not all files, folders, and registry keys and entries are installed on your computer during this malware's/spyware's/grayware's execution. This may be due to incomplete installation or other operating system conditions. If you do not find the same files/folders/registry information, please proceed to the next step.

Step 3

Restart in Safe Mode

[Learn More]

Step 4

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\Microsoft\Windows\CurrentVersion\Run*
syswin = "%System Root%\boots\syswin.exe"

Step 5

Search and delete these folders

[Learn More]

Please make sure you check the *Search Hidden Files and Folders* checkbox in the More advanced options option to include all hidden folders in the search result.
%System Root%\boots

Step 6

Restart in normal mode and scan your computer with your Trend Micro product for files detected as Worm.Win32.PYFILEDEL.AA. 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.

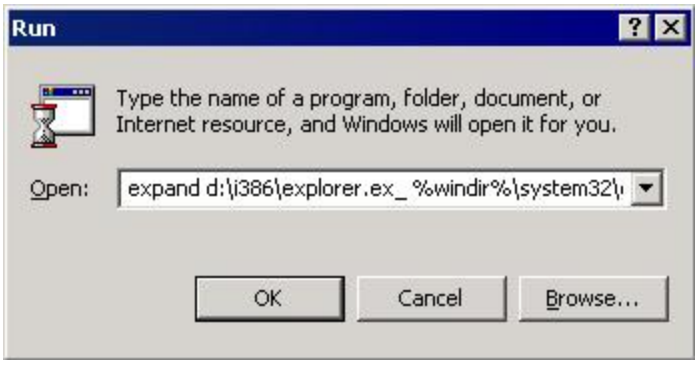
Step 7

Restore a file/s that has/have been corrupted/modified by this malware/grayware

To restore system files:

• For *Windows 2000*:

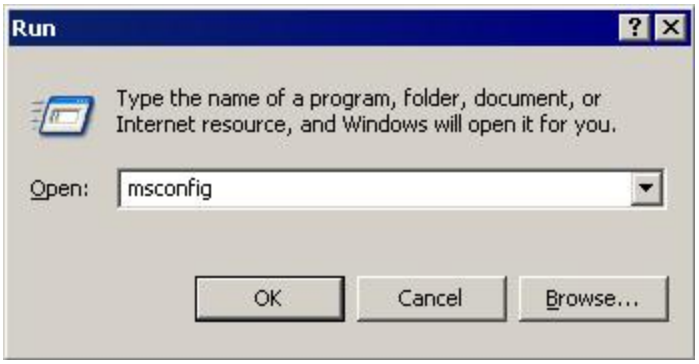
1. Insert your *Windows 2000 Installation* CD in your CD-ROM drive.
2. Click *Start>Run*.
3. In the *Open* text box, type the following then click *OK*:
   expand D:\i386\{file to restore}.ex_ %windir%\system32\{file to restore}.exe



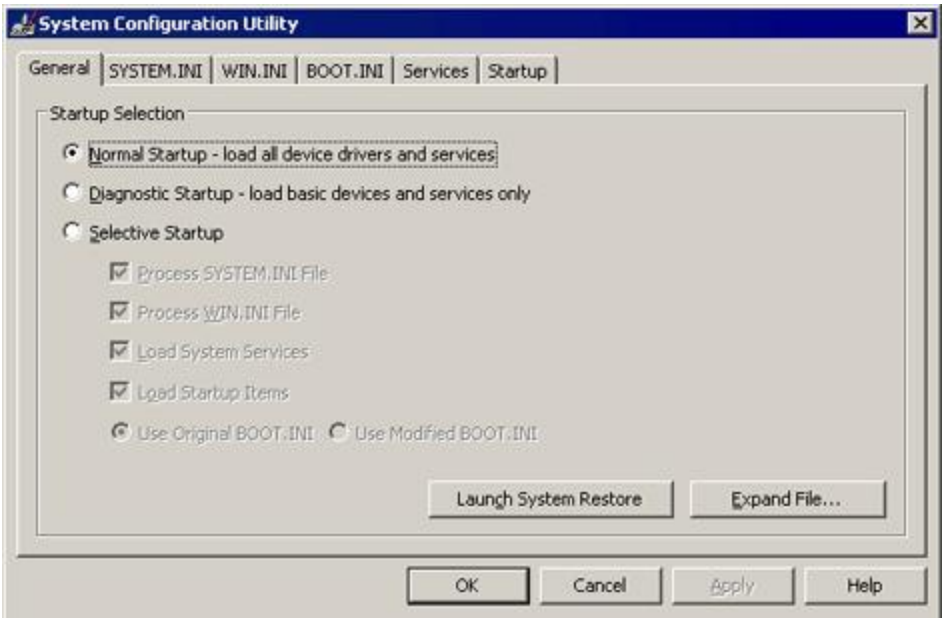
   (**Note:** In the example above, *D:* refers to the CD-ROM drive. If your CD-ROM drive is not *D:*, please change the letter accordingly. Also, the file to restore is *C:\WINNT\System32\explorer.exe*.)

• For *Windows XP* and *Windows Server 2003*:

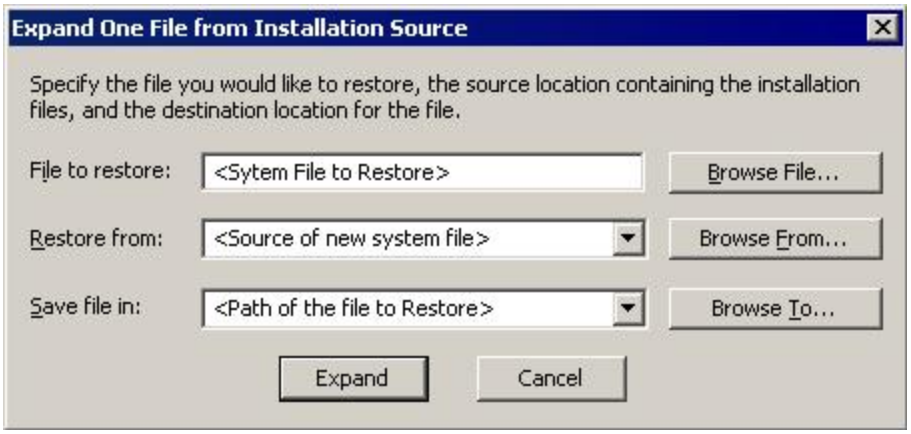
1. Click *Start>Run*.
2. In the *Open* text box, type the following then click *OK*:
   MSCONFIG



3. Make sure that the option *Normal startup - load all device drivers and services* option is selected.



4. Click the *Expand* button.
5. In the dialog box that appears, type the following:



   Wherein:

   - *File to restore* contains the path and file name of the file you wish to restore.
   - *Restore from* contains the path to the Windows CAB files. This path may vary from machine to machine. It may be in a local drive, in a network drive, or in a CD-ROM. In the local drive, it is usually in *C:\WINDOWS\OPTIONS\INSTALL*.
   - *Save file in* contains the path of the file you wish to restore (Do not include the file name).

- Click the *Expand* button.

Did this description help? Tell us how we did.