PE_URSNIF.A2 - Threat Encyclopedia | Trend Micro (US)

Archived: 2026-04-05 18:16:54 UTC

This is the detection for the infected .EXE and .PDF files related to the URSNIF variant that steals information. The said information-stealing infector (detected as PE_URSNIF.A-O) has affected countries such as US and UK.

To get a one-glance comprehensive view of the behavior of this Spyware, refer to the Threat Diagram shown below.

Arrival Details

This malware arrives via the following means:

- MSI files infected by PE_URSNIF.A-O

Installation

This spyware adds the following folders:

- %All Users Profile%\Application Data\SoftwareProtectionPlatform

(Note: *%All Users Profile%* is the All Users folder, where it usually is C:\Documents and Settings\All Users on Windows 2000, Windows Server 2003, and Windows XP (32- and 64-bit); C:\ProgramData on Windows Vista (32- and 64-bit), Windows 7 (32- and 64-bit), Windows 8 (32- and 64-bit), Windows 8.1 (32- and 64-bit), Windows Server 2008, and Windows Server 2012.)

It drops the following files:

- %System%\wsauth.exe - mother file detected as PE_URSNIF.A-O
- %Application Data%\SoftwareProtectionPlatform\sppc.exe - mother file detected as PE_URSNIF.A-O

(Note: *%System%* is the Windows system folder, where it usually is C:\Windows\System32 on all Windows operating system versions.. *%Application Data%* is the Application Data folder, where it usually is C:\Documents and Settings\{user name}\Application Data on Windows 2000, Windows Server 2003, and Windows XP (32- and 64-bit); C:\Users\{user name}\AppData\Roaming on Windows Vista (32- and 64-bit), Windows 7 (32- and 64-bit), Windows 8 (32- and 64-bit), Windows 8.1 (32- and 64-bit), Windows Server 2008, and Windows Server 2012.)

Its DLL component is injected to the following process(es):

- explorer.exe
- iexplore.exe
- firefox.exe
- chrome.exe
- services.exe

Autostart Technique

This spyware registers itself as a system service to ensure its automatic execution at every system startup by adding the following registry entries:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\wsauth
ImagePath = "%System%\wsauth.exe -s"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\wsauth
DisplayName = "Windows Software Protection"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\wsauth
Description = "This windows service enables the download, installation and enforcement of digital licenses for

Windows and Windows applications. If the service is disabled, the operating system and licensed applications may run in a notification mode. It is strongly recommended that you not disable the Software Protection Service."

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

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run
dumpnsta = "%Application Data%\SoftwareProtectionPlatform\sppc.exe"

It registers as a system service to ensure its automatic execution at every system startup by adding the following registry keys:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\wsauth

File Infection

This spyware infects the following files:

- *.pdf - detected as PE_URSNIF.A1
- *.msi - detected as PE_URSNIF.A2
- setup.exe

  It infects these files found in all removable and network drives

This is the Trend Micro detection for files infected by:

- PE_URSNIF.A-O

Propagation

This spyware drops copies of itself in the following drives:

- removable drives
- network drives

It drops copies of itself in network drives such as the following:

- {drive letter}:\Temp.exe

It drops the following copy(ies) of itself in all removable drives:

- {drive letter}:\Temp.exe

Information Theft

This spyware gathers the following data:

- System Information (Please see notes for more details)
- Running processes and services

- Installed device drivers
- Programs installed
- Screenshots

Stolen Information

This spyware sends the gathered information via HTTP POST to the following URL:

- where {domain} can be any of the following:
    - com
    - net
    - org
    - info
- http://{random letters}.{domain}/pki/mscorp/crl/msiwww2.crl
- http://{random letters}.{domain}/pki/mscorp/crl/MSIT%20Machine%20Auth%20CA%202(1).crl

Other Details

This spyware does the following:

- It hooks the following WININET.DLL exported functions when the DLL component is loaded in IEXPLORE.EXE to monitor network traffic:
    - HttpOpenRequestA
    - HttpOpenRequestW
    - HttpSendRequestA
    - HttpSendRequestW
    - HttpQueryInfoA
    - HttpQueryInfoW
    - InternetReadFile
    - InternetReadFileExA
    - InternetReadFileExW
    - InternetQueryDataAvailable
- It hooks the following NSS3.DLL or NSPR4.DLL exported functions when the DLL component is loaded in FIREFOX.EXE to monitor network traffic:
    - PR_Read
    - PR_Write
    - PR_Close
    - PR_Poll
    - PR_Available
- It hooks unnamed functions exported by CHROME.DLL when the DLL component is loaded in CHROME.EXE to monitor network traffic.
- If CHROME.DLL is not found, it will hook the following APIs exported by KERNEL32.DLL:
    - LoadLibraryA
    - LoadLibraryW

    - LoadLibraryExA
    - LoadLibraryExW
- It will drop and execute a temporary file, %User Temp%\~{random}.tmp, which is responsible in injecting its embedded DLL component to the said processes stated above. The temporary file will terminate and delete itself, afterwards. This dropped component is detected as TSPY_URSNIF.SM3.

(Note: *%User Temp%* is the user's temporary folder, where it usually is C:\Documents and Settings\{user name}\Local Settings\Temp on Windows 2000, Windows Server 2003, and Windows XP (32- and 64-bit); C:\Users\{user name}\AppData\Local\Temp on Windows Vista (32- and 64-bit), Windows 7 (32- and 64-bit), Windows 8 (32- and 64-bit), Windows 8.1 (32- and 64-bit), Windows Server 2008, and Windows Server 2012.)

NOTES:

It issues the following commands in Command Prompt (cmd) to gather its stolen information:

- systeminfo
- tasklist /SVC (enumerate processes and services)
- driverquery (gather information on installed drivers)
- reg.exe query *"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall" /s* (gather installed programs)

Systeminfo will return the following system information:

- Host Name
- OS Name, Version, Manufacturer, Configuration and Build Type
- Registered Owner and Organization
- Product ID
- Original Install Date
- System Up Time
- System Manufacturer, Model and type
- Processor(s)
- BIOS version
- Windows and System directory
- Boot Device
- System and Input Locale
- Time Zone
- Total and Available Memory
- Virtual Memory information (Max, Available, In Use)
- Page file locations
- Domain
- Logon server
- Hotfix(s)
- Network card(s)

The information gathered will be saved to temporary file %User Temp%\~{random}.tmp, which serves as its stolen information dump/log file. After the file is sent to its C&C server, the malware deletes it.

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

Remove malware/grayware files dropped/downloaded by PE_URSNIF.A2. (Note: Please skip this step if the threats listed below have already been removed.)

- PE_URSNIF.A1
- TSPY_URSNIF.SM3
- PE_URSNIF.A-O

Step 4

Restart in Safe Mode

[Learn More]

Step 5

Delete this registry key

[Learn More]

=Important: Editing the *Windows Registry* incorrectly can lead to irreversible system malfunction. Please do this only if you know how to or you can seek your system administrator’s help. You may also check out this Microsoft article first before modifying your computer's registry.

- In *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*
  - **wsauth**

Step 6

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 articleopen on a new tab first before modifying your computer's registry.

- In *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run*
  - **dumpnsta = "%Application Data%\SoftwareProtectionPlatform\sppc.exe"**

Step 7

Search and delete this folder

[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.

- %Application Data%\SoftwareProtectionPlatform

Step 8

Search and delete these files

[Learn More]

There may be some files that are hidden. Please make sure you check the *Search Hidden Files and Folders* checkbox in the "More advanced options" option to include all hidden files and folders in the search result.

- %User Temp%\~{random}.tmp

Step 9

Restart in normal mode and scan your computer with your Trend Micro product for files detected as PE_URSNIF.A2. 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 pageopen on a new tab for more information.

Did this description help? Tell us how we did.open on a new tab

---