BKDR_URSNIF.SM - Threat Encyclopedia | Trend Micro (US)

By Analysis by: Sabrina Lei Sioting

Archived: 2026-04-05 21:28:43 UTC

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

It executes commands from a remote malicious user, effectively compromising the affected system.

Arrival Details

This backdoor 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 backdoor drops the following copies of itself into the affected system:

- %User Profile%\nah_{4 random characters}.exe

(Note: *%User Profile%* is the current user's profile folder, which is usually C:\Documents and Settings\{user name} on Windows 2000, XP, and Server 2003, or C:\Users\{user name} on Windows Vista and 7.)

It adds the following mutexes to ensure that only one of its copies runs at any one time:

- xmas_mutex

Autostart Technique

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

HKEY_CURRENT_USER\SOFTWARE\Microsoft\
Windows\CurrentVersion\Run
nah_Shell = "%User Profile%\nah_{4 random characters}.exe"

Other System Modifications

This backdoor adds the following registry entries as part of its installation routine:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\
Windows\CurrentVersion
nah_opt_reserv = "{BLOCKED}13.106 "

HKEY_CURRENT_USER\SOFTWARE\Microsoft\
Windows\CurrentVersion

nah_opt_forms = "/system/prinimalka.py/forms"

HKEY_CURRENT_USER\SOFTWARE\Microsoft\
Windows\CurrentVersion
nah_opt_options = "/system/prinimalka.py/options"

HKEY_CURRENT_USER\SOFTWARE\Microsoft\
Windows\CurrentVersion
nah_opt_command = "/system/prinimalka.py/command"

HKEY_CURRENT_USER\SOFTWARE\Microsoft\
Windows\CurrentVersion
nah_opt_file = "/system/prinimalka.py/cookies"

HKEY_CURRENT_USER\SOFTWARE\Microsoft\
Windows\CurrentVersion
nah_opt_ss = "/cgi-bin/trash.py"

HKEY_CURRENT_USER\SOFTWARE\Microsoft\
Windows\CurrentVersion
nah_opt_pstorage = "/cgi-bin/trash.py"

HKEY_CURRENT_USER\SOFTWARE\Microsoft\
Windows\CurrentVersion
nah_opt_certs = "/cgi-bin/trash.py"

HKEY_CURRENT_USER\SOFTWARE\Microsoft\
Windows\CurrentVersion
nah_opt_idproject = "000055"

HKEY_CURRENT_USER\SOFTWARE\Microsoft\
Windows\CurrentVersion"
nah_opt_pauseopt = "1200"

Backdoor Routine

This backdoor executes the following commands from a remote malicious user:

- Archive and upload file(s)
- Capture screenshot
- Clear cookies
- Download and Execute other files
- List running process
- Reboot the affected system
- Steal certificates and cookies
- Update/Download a configuration file

- Upload a log file which contains stolen information

It connects to the following URL(s) to send and receive commands from a remote malicious user:

- http://{BLOCKED}3.2/system/prinimalka.py/command

Stolen Information

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

- http://{BLOCKED}3.2/system/prinimalka.py/forms

NOTES:

It checks the existence of the following registry key:

HKEY_CURRENT_USER\Software\Classes\FirefoxHTML\shell\open\command

If it exists, it gets the folder location of *firefox.exe* and creates the following file:

- {folder location}\chrome\amba.jar

Oncethe file mentioned above is executed, it drops the following file:

- {folder location}\chrome\amba.js - detected as JS_URSNIF.DJ

It also modifies the following file to point to *amba.jar*:

- {folder path}\chrome\browser.manifest

It injects itself into all running processes to remain memory-resident except for the following processes:

- svchost.exe
- [System Process]
- System
- smss.exe
- winlogon.exe
- lsass.exe
- avp
- csrss.exe
- services.exe

It hooks the following API calls to hide its behavior on the affected system:

- CreateProcessA
- CreateProcessW
- FindFirstFileA
- FindNextFileA
- FindFirstFileW

- FindNextFileW
- RegEnumValueA
- RegEnumValueW

It hooks the following API calls to search for network traffic for a predetermined HTML elements:

- InternetCloseHandle
- InternetQueryDataAvailable
- InternetReadFile
- InternetReadFileExA
- HttpSendRequestA
- HttpSendRequestW
- HttpOpenRequestW
- HttpOpenRequestAl

It attempts to steal sensitive online banking information, such as user names and passwords from the following financial institutions:

- trade
- schwab
- fidelity
- paypal
- wamu bank
- wellsfargo
- suntrust
- usaa
- wachovia

It does this by injecting certain HTML codes to the site.

Step 2

Remove the malware/grayware file dropped/downloaded by BKDR_URSNIF.SM

JS_URSNIF.DJ

Step 3

Since this malware cannot be removed in normal and safe mode, it is necessary to restart using the Windows Recovery Console. To restart the system using the Windows Recovery Console:

• On Windows XP and Server 2003 systems:

1. Click Start>Run. In the Open input box, type **secpol.msc** and press Enter.
2. In the left panel, double-click *Local Policies>Security Options*.
3. In the right panel, double-click *Recovery Console: Allow floppy copy and access to all drives and folders*.
4. Select *Enabled* and click OK.

5. Insert the Windows Installation CD into the CD drive, then restart your computer.
6. When prompted, press any key to boot from the CD.
7. On the main menu, type **r** to go to the Recovery Console.
8. Type the number that corresponds to the drive and directory that contains Windows (usually C:\WINDOWS) and press Enter.
9. Type the Administrator password and press Enter.
10. In the input box, type the following then press Enter:
    SET AllowAllPaths = TRUE
    del %User Profile%\nah_{4 random characters}.exe
11. Type **exit** and press Enter to restart the system normally.

• On Windows Vista and 7 systems:

1. Insert your Windows Installation DVD in the DVD drive, then Press the restart button.
2. When prompted, press any key to boot from the DVD.
3. Depending on your Windows Installation DVD, you might be required to select the installation language. Then on the Install Windows window, choose your language, locale, and keyboard layout or input method. Click Next, then click *Repair your computer*.
4. Select *Use recovery tools that can help fix problems starting Windows.* Select your installation of Windows. Click Next.
5. If the Startup Repair window appears, click Cancel, Yes, then Finish.
6. In the System Recovery Options window, click Command Prompt.
7. In the Command Prompt window, type the following then press Enter:
   del %User Profile%\nah_{4 random characters}.exe
   (Note: In Windows 7, all local drives will be assigned one more than normal. For example, the C: drive becomes D:.)
8. Type **exit** and press Enter to close the Command Prompt window.
9. Click Restart to restart the system normally.

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

- In *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
  - **nah_Shell = "%User Profile%\nah_{4 random characters}.exe"**
- In *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion*
  - **nah_opt_reserv = "{BLOCKED}13.106"**
- In *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion*
  - **nah_opt_forms = "/system/prinimalka.py/forms"**

- In *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion*
  - **nah_opt_options = "/system/prinimalka.py/options"**
- In *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion*
  - **nah_opt_command = "/system/prinimalka.py/command"**
- In *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion*
  - **nah_opt_file = "/system/prinimalka.py/cookies"**
- In *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion*
  - **nah_opt_ss = "/cgi-bin/trash.py"**
- In *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion*
  - **nah_opt_pstorage = "/cgi-bin/trash.py"**
- In *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion*
  - **nah_opt_certs = "/cgi-bin/trash.py"**
- In *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion*
  - **nah_opt_idproject = "000055"**
- In *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion"*
  - **nah_opt_pauseopt = "1200"**

Step 5

Search and delete this file

[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. {folder location}\chrome\amba.jar

Step 6

Scan your computer with your Trend Micro product to delete files detected as BKDR_URSNIF.SM. 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.

Step 7

Restore deleted/modified files and/or registry entries from backup

***Note:** Only Microsoft-related files/keys/values will be restored. If this malware/grayware also deleted registry keys/values related to programs that are not from Microsoft, please reinstall those programs on your computer.

{folder path}\chrome\browser.manifest

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

---

Source: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/BKDR_URSNIF.SM?_ga=2.129468940.1462021705.1559742358-1202584019.1549394279