URSNIF: The Multifaceted Malware

By By: Trend Micro March 27, 2015 Read time: 2 min (621 words)

Published: 2015-03-27 · Archived: 2026-04-05 17:11:48 UTC

The URSNIF malware family is primarily known for being a data-stealing malware, but it's also known for acquiring a wide variety of behavior. Known URSNIF variants include backdoors (BKDR_URSNIF.SM), spyware (TSPY_URSNIF.YNJ), and file infectors (PE_URSNIF.A-O). ***December 2014: Rise in URSNIF infections brought about by file infection routines*** In December 2014 we discussed a rise in URSNIF infections, primarily in North America, which were due to the addition of file infection to URSNIF's routines. The virus inserts the host file into its resource section, instead carrying out typical file infection routines like patching host files (via inserting malicious code). These variants targeted the following files:

- *.PDF (detected as PE_URSNIF.A-O)
- *.MSI (detected as PE_URSNIF.A1)
- *setup*.exe (detected as PE_URSNIF.A2)

February 2015: Another URSNIF outbreak seen The February outbreak showed that the malware widened its scope and improved its stealth mechanism. The URSNIF variants are detected as PE_URSNIF.B-O and PE_URSNIF.B. It uses strings already found in legitimate system files for its properties such as its file name, folder name, and registry entries. This is done to hide itself alongside other legitimate system files. The file names it uses are a combination of legitimate system file names; for example, the malware will name itself *cmdlnsta.exe*, a combination of legitimate file names *cmdl32.exe* and *rwinsta.exe*. URSNIF was known to exhibit this behavior before it became a file infector. It also injects its code separately into each target process, perhaps to avoid memory scanners. We also noted that the hardcoded strings in this URSNIF wave are the same ones found in the December variants. ***March 2015: URSNIF variants seen infecting more file types*** URSNIF variants seen this month (PE_URSNIF.E-O and PE_URSNIF.E) have further widened their scope. This new wave now infects more file types, including Microsoft Office documents, spreadsheets, and presentation files. It uses strings from system files (as the earlier variants did), and uses existing folder names to name the dropped files in order to trick fool users into running them. This technique was not particularly effective, as it did not hide the original folder. The table below compares the recent URSNIF variants:

	Pre-file infector	**December 2014**	**February 2015**	**March 2015**
Infected files	None	*.PDT, *.MSI, *SETUP*.EXE	*.PDF, *.MSI, *.EXE	*.PDF, *.MSI, *.EXE, *.PPT, *.PPTX, *.DOC, *.DOCX, *.XLS, *.XLSX

Name used in removable drive propagation	None	*Temp.exe*	*Temp.exe*	*{Folder Name}.exe*
Use random strings for file names?	Yes	No	Yes	Yes
Inject routines separately?	No	No	Yes	No
Polymorphic?	No	Yes	Yes	Yes

URSNIF's known hooking functions URSNIF is traditionally also known for hooking various executable files in order to monitor browsers. It hooks *WS2_32.DLL* and *KERNEL32.DLL* or *CHROME.DLL* to monitor Google Chrome, *NSS3.DLL* and *NSPR4.DLL* to monitor Mozilla Firefox, and *WININET.DLL* to monitor Internet Explorer. It also monitors other browsers like Opera and Safari. Recent URSNIF variants have significantly modified the exact system APIs that it's been hooking for years. Hooking these APIs allows the malware to perform a wide variety of information theft, such as taking screenshots, by intercepting the data contained in various normal commands. Together with the hooked APIs, this allows for powerful information theft capabilities. The list of hooked APIs is below.

2012-2013	**2013-2014**	**2014-2015**
InternetReadFile	InternetReadFile	HttpOpenRequestA
InternetReadFileExA	InternetReadFileExA	HttpOpenRequestW
InternetReadFileExW	InternetReadFileExW	HttpSendRequestA
HttpSendRequestA	HttpSendRequestA	HttpSendRequestW
HttpSendRequestW	HttpSendRequestW	HttpQueryInfoA
HttpOpenRequestA	HttpQueryInfoA	HttpQueryInfoW
HttpOpenRequestW	HttpQueryInfoW	InternetReadFile
InternetConnectA	HttpAddRequestHeadersA	InternetReadFileExA
InternetConnectW	HttpAddRequestHeadersW	InternetReadFileExW
InternetQueryDataAvailable	InternetConnectA	InternetQueryDataAvailable
	InternetConnectW	PR_Read
	InternetQueryDataAvailable	PR_Write

	PR_Read	PR_Close
	PR_Write	PR_Poll
	PR_Close	PR_Available
	WSARecv	LoadLibraryA
	WSASend	LoadLibraryW
	Closesocket	LoadLibraryExA
	LoadLibraryExW	LoadLibraryExW
	ssl_write	
	ssl_read	
	ssl_close	

URSNIF has been constantly evolving in recent months, showing multiple faces of itself and displaying a wide variety of behavior. It shows no clear signs of dying down, which means that the malware will continue to pose risks to users across various segments.
