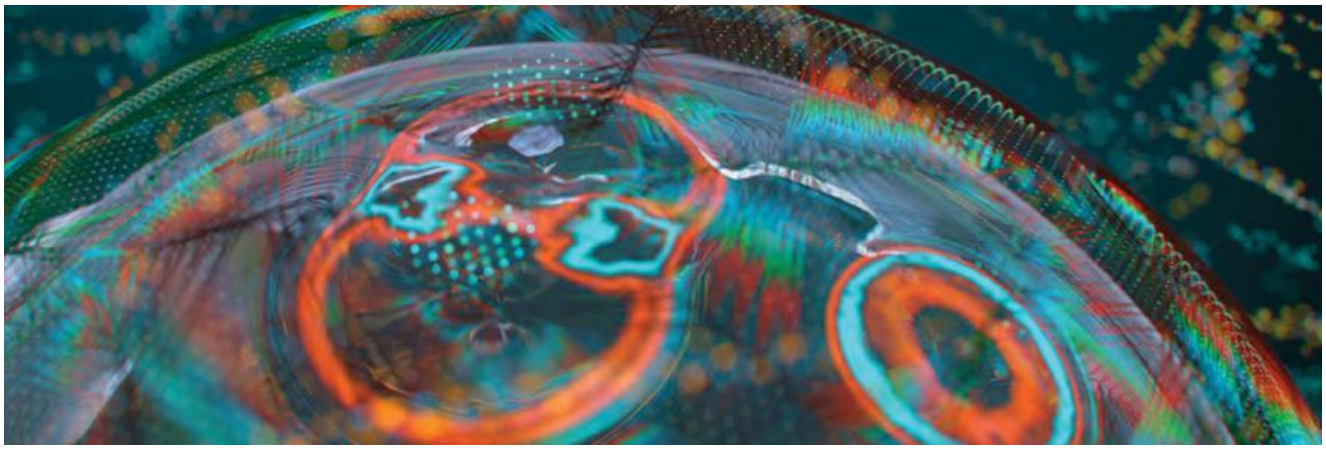
Threat Spotlight: Neshta File Infector Endures

threatvector.cylance.com/en_us/home/threat-spotlight-neshta-file-infector-endures.html

Tatsuya Hasegawa



RESEARCH & INTELLIGENCE / 10.29.19 / Tatsuya Hasegawa

Executive Overview

Neshta is an older file infector that is still prevalent in the wild. It was initially observed in 2003 and has been previously associated with BlackPOS malware. It prepends malicious code to infected files. This threat is commonly introduced into an environment through unintentional downloading or by other malware. It infects Windows executable files and may attack network shares and removable storage devices.

In 2018 Neshta predominantly targeted the manufacturing industry, but attacked the finance, consumer goods, and energy sectors as well. To achieve persistence Neshta renames itself to svchost.com then modifies the registry so it runs each time an .exe file is launched. This threat is known to collect system information and use POST requests to exfiltrate data to attacker-controlled servers. The Neshta binaries used in our analysis did not demonstrate the data exfiltration behaviour or functionality.

Technical Analysis

This section describes the symptoms of a Neshta infection. We picked samples of the Neshta virus uploaded to VirusTotal in 2007, 2008, and 2019.

We analyzed files with these SHA-256 hashes:

- 29fd307edb4cfa4400a586d38116a90ce91233a3fc277de1cab7890e681c409a
- 980bac6c9afe8efc9c6fe459a5f77213b0d8524eb00de82437288eb96138b9a2

- 539452719c057f59238e123c80a0a10a0b577c4d8af7a5447903955e6cf7aa3d
- a4d0865565180988c3d9dbf5ce35b7c17bac6458ef234cfed82b4664116851f2
- 46200c11811058e6d1173a2279213d0b7ccde611590e427b3b28c0f684192d00
- c965f9503353ecd6971466d32c1ad2083a5475ce64aadc0b99ac13e2d2c31b75

Static File Analysis

Neshta's code is compiled by Boland Delphi 4.0. The file size is usually 41,472 bytes.

As any Delphi binary, Neshta has four writable sections (DATA, BSS, .idata, and .tls) and three sharable sections (.rdata, .reloc, and .rsrc):

Figure 1: Section header features

In addition, Neshta code displays interesting fingerprint strings - see Figure 2, below:

"*Delphi-the best. F*** off all the rest. Neshta 1.0 Made in Belarus. Прывітанне усім ~цікавым~ беларус_кім дзяучатам. Аляксандр Рыгоравіч, вам таксама :) Восень-кепская пара... Аліварыя - лепшае піва! Best regards 2 Tommy Salo. [Nov-2005] yours [Dziadulja Apanas]"*
The Belarusian strings say: *" Hello everyone ~ ~ interesting belarus_kim girls. Alexander G., you too :) osen- bad couple ... Alivaryya - the best beer!"*

Figure 2: Neshta's fingerprint strings

File Infection

Neshta's main feature is its file infector which searches local drives for .exe files. Neshta targets ".exe" files making exceptions for the ones that contain any of the following strings in their short path:

- %Temp%
- %SystemRoot% (usually C:\Windows)
- \PROGRA~1\

The infection flow summary is described below and shown in Figure 3.

Neshta:

1. Reads 41,472 (0xA200) bytes from the beginning of target original file.
2. Creates two sections and allocates memory with the attribute of PAGE_READWRITE on the original file's beginning and bottom.

3. Inserts its malicious header and code at the beginning of the original file. The written data is 41,472 bytes.
4. Writes the encoded original header and code to the file, which is 41,472 bytes in size.

These actions enable the malicious code to launch as soon as the infected file is executed:

Figure 3: File Infection

When the infected file is executed, the original program is dropped into %Temp%\3582-490\ <filename> and run by the WinExec API.

Persistence

Neshta drops itself to C:\Windows\svchost.com and installs itself into the registry using the following parameters:

Registry key: HKLM\SOFTWARE\Classes\exefile\shell\open\command
Registry value: (Default)
Value: %SystemRoot%\svchost.com "%1" %*

This registry change directs the system to run Neshta each time an .exe file is launched. The "%1" %* points to the launched .exe file. In addition, Neshta creates a named mutex to check for the existence of another running instance:

MutexPolesskayaGlush.*<0x90>svchost.com<0x90>exefile\shell\open\command‹À "%1" %*œ‘@*

Another dropped file is “directx.sys” which is sent to %SystemRoot%. This is a text file (not a kernel driver) which contains the path of the last infected file to run. It is updated every time an infected file is executed.

BlackBerry Cylance Stops Neshta

BlackBerry Cylance uses artificial intelligence-based agents trained for threat detection on millions of both safe and unsafe files. Our automated security agents block Neshta based on countless file attributes and malicious behaviors instead of relying on a specific file signature. BlackBerry Cylance, which offers a predictive advantage over zero-day threats, is trained on and effective against both new and legacy cyberattacks. For more information, visit https://www.cylance.com.

Appendix

Indicators of Compromise (IOCs)

- Hashes
  - 29fd307edb4cfa4400a586d38116a90ce91233a3fc277de1cab7890e681c409a
  - 980bac6c9afe8efc9c6fe459a5f77213b0d8524eb00de82437288eb96138b9a2
  - 539452719c057f59238e123c80a0a10a0b577c4d8af7a5447903955e6cf7aa3d
  - a4d0865565180988c3d9dbf5ce35b7c17bac6458ef234cfed82b4664116851f2
  - 46200c11811058e6d1173a2279213d0b7ccde611590e427b3b28c0f684192d00
  - c965f9503353ecd6971466d32c1ad2083a5475ce64aadc0b99ac13e2d2c31b75

- Filenames
  - %SystemRoot%\svchost.com
  - %SystemRoot%\directx.sys
  - %Temp%\tmp5023.tmp

- C2s/IPs

- Mutexes
  - MutexPolesskayaGlush*.*<0x90>svchost.com<0x90>exefile\shell\open\command‹À "%1" %*œ‘@

- Interesting strings
  - Delphi-the best. F**k off all the rest. Neshta 1.0 Made in Belarus. Прывітанне усім ~цікавым~ беларус_кім дзяучатам. Аляксандр Рыгоравіч, вам таксама :) Восень-кепская пара... Аліварыя - лепшае піва! Best regards 2 Tommy Salo. [Nov-2005] yours [Dziadulja Apanas]

SHA256	**29fd307edb4cfa4400a586d38116a90ce91233a3fc277de1cab7890e681c409a**
Type	PE32 executable (GUI) Intel 80386, for MS Windows
Size	41472
Timestamp	1992:06:20 07:22:17+09:00
ITW names	Svchost[.]com

Tatsuya Hasegawa

About Tatsuya Hasegawa

Senior Threat Researcher at BlackBerry Cylance

Tatsuya Hasegawa is a Senior Threat Researcher in APAC at BlackBerry, and is responsible for malware analysis and sandbox technology. He has practical experience in the both managed security service provider as a security analyst and CSIRT as an incident handler. His certifications include: GREM, GCIH, GCFA, GXPN, GPEN and CISSP.

Back