Win32/Neshta.A | ESET Virusradar

web.archive.org/web/20220119114002/https:/www.virusradar.com/en/Win32_Neshta.A/description

Win32/Neshta [Threat Name] go to Threat

Win32/Neshta.A [Threat Variant Name]

Category	virus
Size	41472 B
Aliases	Virus.Win32.Neshta.a (Kaspersky)
	W32/HLLP.41472.e.virus (McAfee)
	Virus:Win32/Neshta.A (Microsoft)
	W32.Neshuta (Symantec)

Short description

Win32/Neshta.A is a file infector.

Installation

When executed, the virus creates the following files:

- %temp%\tmp5023.tmp
- %windir%\directx.sys
- %windir%\svchost.com (41472 B, Win32/Neshta.A)

The following Registry entry is set:

> [HKEY_CLASSES_ROOT\exefile\shell\open\command]
> "(Default)" = "%windir%\svchost.com "%1" %*"

This causes the virus to be executed along with any program.

Executable file infection

Win32/Neshta.A is a file infector.

The virus searches local drives for files with the following file extensions:

> .exe

The virus infects the files by inserting its code at the beginning of the original program.

The size of the inserted code is 41472 B .

It also infects files stored on removable and network drives.

It avoids files which contain any of the following strings in their path:

- %temp%
- %windir%
- \PROGRA~1\

Several other criteria are applied when choosing a file to infect.

When an infected file is executed, the original program is being dropped into a temporary file and run.

The original file is stored in the following location:

```
%temp%\3582-490\%filename%
```

Other information

It contains the following text:

```
Delphi-
the best. Fuck off all the rest. Neshta 1.0 Made in Belarus. Прывітанне усім ~цікавым~ беларус_кім дзяучатам. Аляксандр Рыгоравіч, ва
2005] yours [Dziadulja Apanas]
```