Trojan.Win32.AZORUIT.A

July 25, 2019

(Kaspersky)

PLATFORM: Windows

OVERALL RISK RATING:

DAMAGE POTENTIAL:

DISTRIBUTION POTENTIAL:

REPORTED INFECTION:

INFORMATION EXPOSURE:

Low Medium High Critical

Threat Type: Trojan	Destructiveness: No	Encrypted:	In the wild: Yes

OVERVIEW

TECHNICAL DETAILS

SOLUTION

MINIMUM SCAN ENGINE: 9.850
FIRST VSAPI PATTERN FILE: 14.800.05
FIRST VSAPI PATTERN DATE: 08 Feb 2019
VSAPI OPR PATTERN FILE: 14.801.00
VSAPI OPR PATTERN DATE: 09 Feb 2019

Step 1

Before doing any scans, Windows 7, Windows 8, Windows 8.1, and Windows 10 users must disable *System Restore* to allow full scanning of their computers.

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

Deleting Scheduled Tasks

The following **{Task Name} - {Task to be run}** listed should be used in the steps identified below:

- Name:GoogleUpdateTaskMachineCore
  Action:%ProgramFiles%\Google\Update\GoogleUpdate.exe /c
  Trigger:At log on of any user At 7:00 PM every day
- Name:GoogleUpdateTaskMachineUA
  Action:%ProgramFiles%\Google\Update\GoogleUpdate.exe /ua /installsource

For Windows 2000, Windows XP, and Windows Server 2003:

- Open the Windows Scheduled Tasks. Click Start>Programs>Accessories> System Tools>Scheduled Tasks.
- Locate each **{Task Name}** values listed above in the Name column.
- Right-click on the said file(s) with the aforementioned value.
- Click on Properties. In the Run field, check for the listed **{Task to be run}**.
- If the strings match the list above, delete the task.

For Windows Vista, Windows 7, Windows Server 2008, Windows 8, Windows 8.1, and Windows Server 2012:

- Open the Windows Task Scheduler. To do this:
  • On *Windows Vista, Windows 7,* and *Windows Server 2008*, click *Start*, type *taskschd.msc* in the *Search* input field, then press *Enter*.
  • On *Windows 8, Windows 8.1,* and *Windows Server 2012*, right-click on the lower left corner of the screen, click *Run*, type *taskschd.msc*, then press *Enter*.
- In the left panel, click *Task Scheduler Library*.
- In the upper-middle panel, locate each **{Task Name}** values listed above in the Name column.
- In the lower-middle panel, click the Actions tab. In the *Details* column, check for the **{Task to be run}** string.
- If the said string is found, delete the task.

Step 4

Delete this registry key

[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 article first before modifying your computer's registry.

- In *HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services*
  - localNETService
- In *HKEY_LOCAL_MACHINE\SOFTWARE*
  - localNETService

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.

- %User Temp%\{random}.dat
- %ProgramData%\localNETService\localNETService.exe
- %Temp%\{random}.dat

Step 6

Scan your computer with your Trend Micro product to delete files detected as Trojan.Win32.AZORUIT.A. 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

- Home and Home Office Support
- Business Support

Step 7

Restore this file from backup only Microsoft-related files will be restored. If this malware/grayware also deleted files related to programs that are not from Microsoft, please reinstall those programs on you computer again.

- %Program Files%\Google\Update\GoogleUpdate.exe

Did this description help? Tell us how we did.