Distribution of Avaddon Ransomware using RigEK in Korea (extension: *.avdn) - ASEC

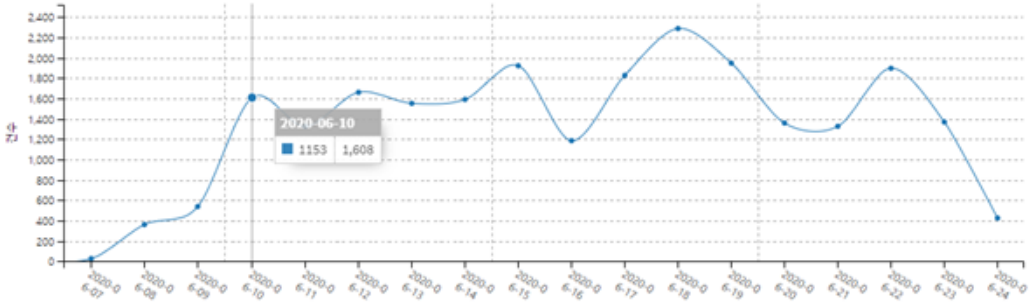
By ATCP

Published: 2020-06-24 · Archived: 2026-04-05 15:28:54 UTC

In early June, a new ransomware dubbed Avaddon was introduced in two articles (see link below). Since June 8, the number of distributed malware using RigEK (Rig Exploit Kit) has increased exponentially in Korea, and Avaddon ransomware is also being distributed.

- (June 7) sensorstechforum.com/avaddon-virus-remove/
- (June 8) www.bleepingcomputer.com/news/security/new-avaddon-ransomware-launches-in-massive-smiley-spam-campaign/

The following figure shows the number of V3 behavior-detection logs for RigEK. 1153 represents No. of behavior-detection rule and this figure shows that the number of cases started skyrocketing starting from June 8.



The number of behavior-based detection cases for RigEK

Users must be aware of Avaddon ransomware which is among various RigEK-based malwares that being distributed. The execution flow is designed to proceed in the order of: “iexplore.exe -> cmd.exe -> wscript.exe -> ransomware.exe” upon connecting to a vulnerable web page.

Upon running the ransomware, it checks the keyboard layout and excludes 0x419 0x485 0x444 0x422 (Russian / Sakha / Tatar / Ukrainian) from encryption. Also, it changes the value of the registry below, allowing a malicious file to run with administrator authority.

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAd

It sends IP info, rcid, encryption key value, name and size of a specific drive, local, language settings, and PC name before file infection.

To allow the ransomware to run continuously, it self-replicates in the %APPDATA%\Roaming\microsoft folder and adds the following registry values:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\update
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\update

The command it performs to delete backup file is shown below, and it also deletes the file that exists within the $Recycle Bin folder.

- wmic.exe SHADOWCOPY /nointeractive
- bcdedit.exe /set {default} recoveryenabled No
- bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
- vssadmin.exe Delete Shadows /All /Quiet
- wbadmin DELETE SYSTEMSTATEBACKUP
- wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest

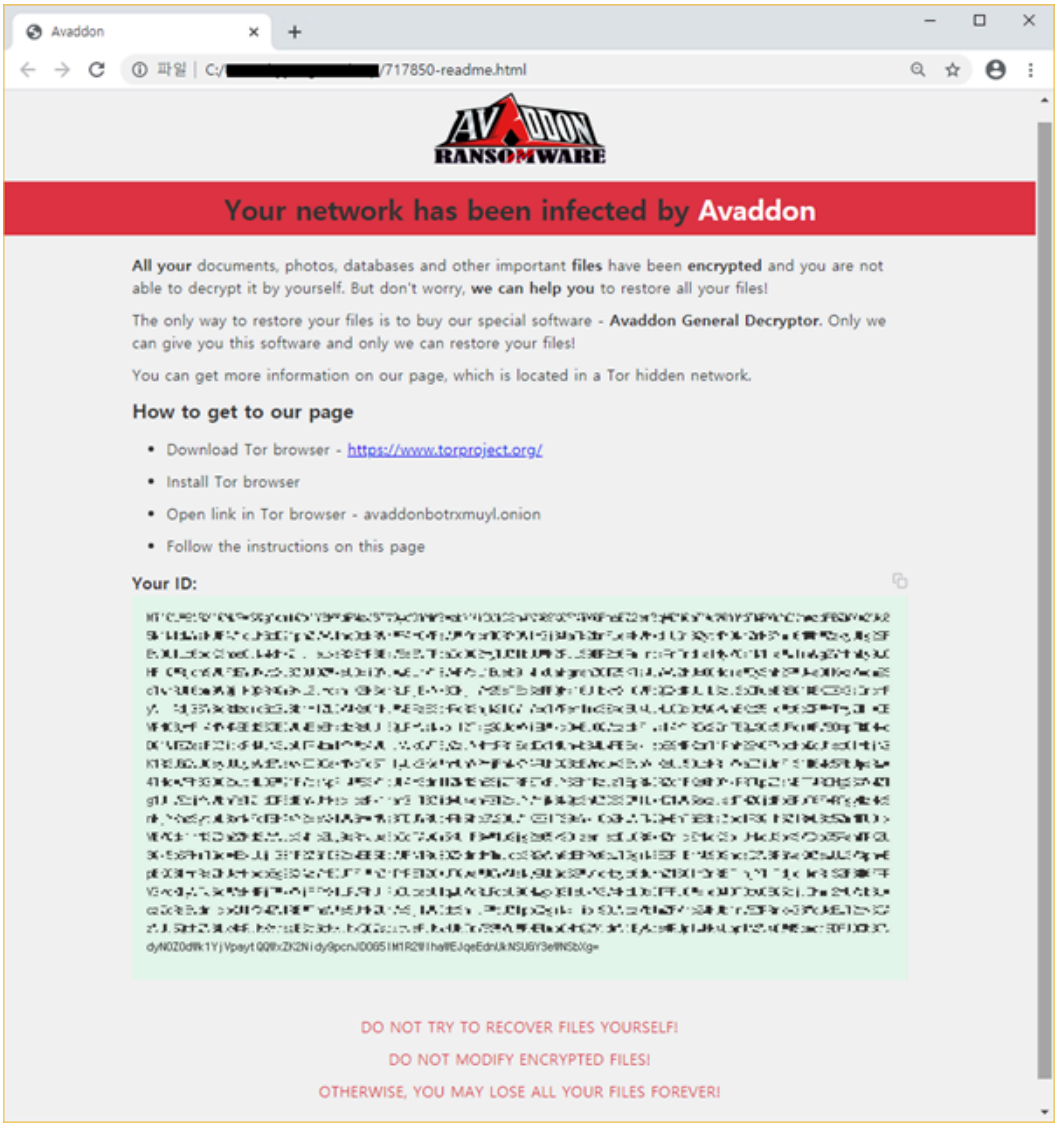
The infection exclusion folders are as follow:

- Windows, Program Files, Users\All Users, AppData, Microsoft, ProgramData

Extensions and files that are excluded from encryption are as follow:

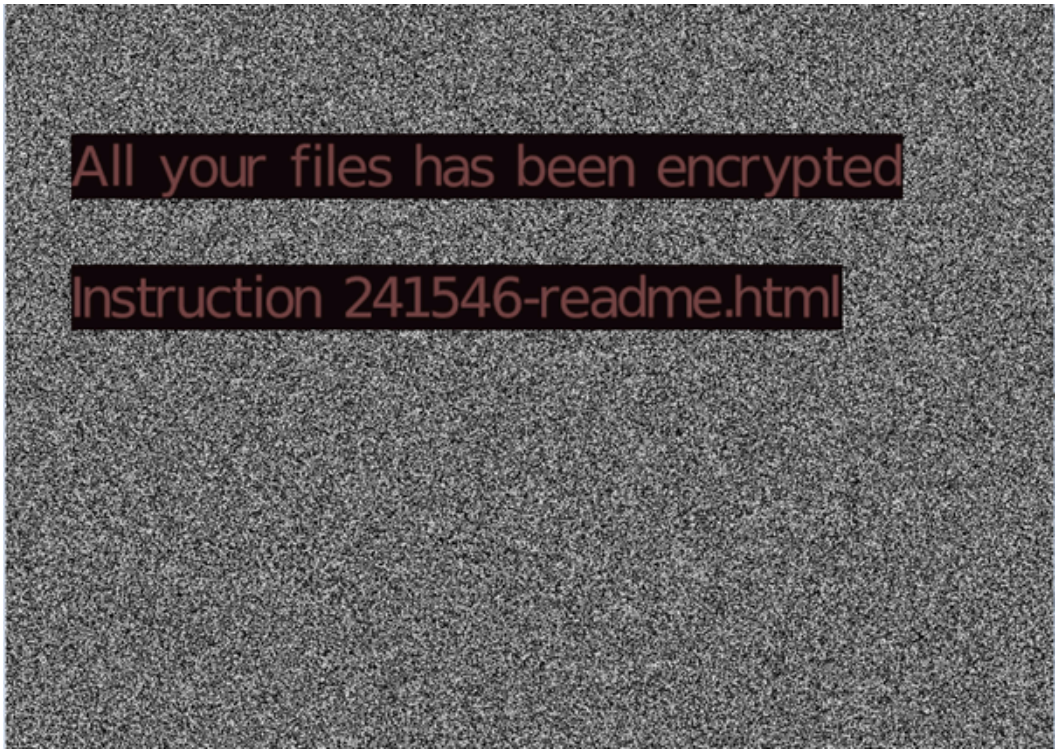
- exe, dll. sys, ini, dat, bin, lnk, avdn, -readme.html, bckgrd.bmp

When the PC is infected, the ransom note in a form of “717850-readme.html” is shown to the user and the number info is variable.



Ransom note (717850-readme.html)

Upon encryption, the ransomware adds .avdn string to the existing extension, and the changed desktop would look like the screen below.



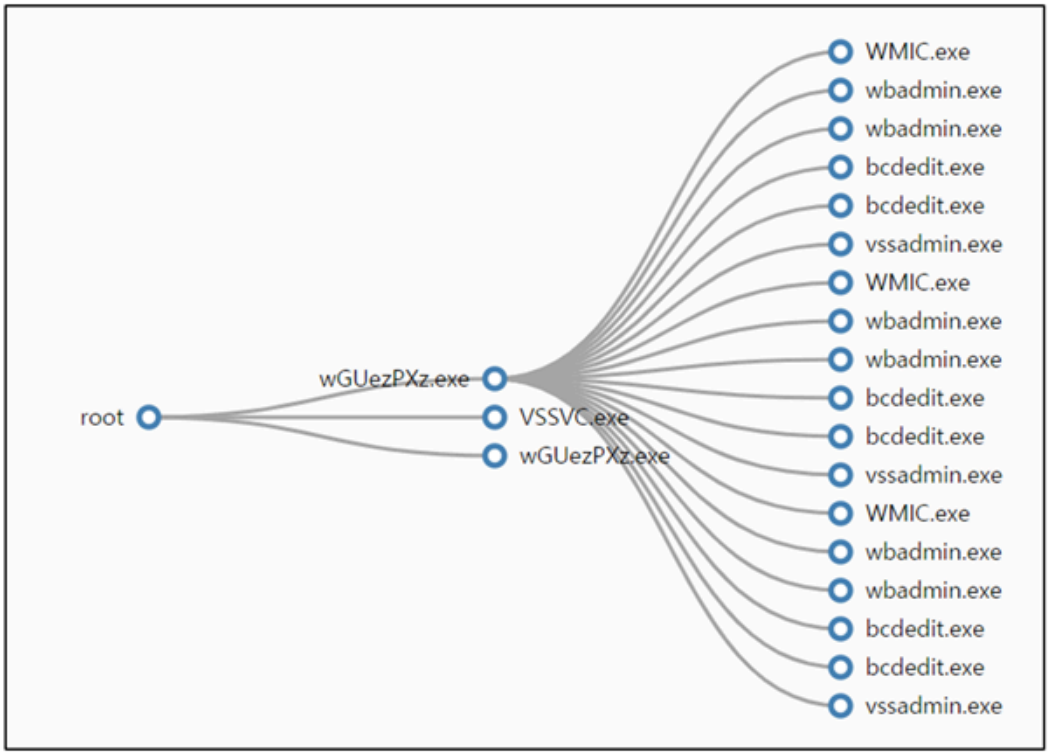
Change in desktop after encryption

Various filenames for the malware were found, and they are as follow:

- qwkka.exe
- piptu.exe
- xi9y8.exe
- xysys.exe

- onbxo.exe

ASEC analysis team can use their in-house dynamic analysis machine (RAPIT) to check the process tree structure and executed the command of Avaddon ransomware as shown below:



Process Tree structure

AhnLab's V3 products detect the malware under the following aliases:

[File Detection]

- Trojan/Win32.MalPe.R341479

[Behavior Detection]

- Malware/MDP.DriveByDownload.M1153
- Malware/MDP.Ransom.M2813

[Memory Detection]

- Win-Trojan/MalPeP.mexp

Source: https://asec.ahnlab.com/en/17411/