Tracking Traces of Malware Disguised as Hancom Office Document File and Being Distributed (RedEyes) - ASEC

By ATCP

Published: 2023-05-24 · Archived: 2026-04-05 17:58:30 UTC

AhnLab Security Emergency response Center (ASEC) has confirmed the distribution of malware disguised as Hancom Office document files. The malware that is being distributed is named “Who and What Threatens the World (Column).exe” and is designed to deceive users by using an icon that is similar to that of Hancom Office. Decompressing the compressed file reveals a relatively large file with a size of 36,466,238 bytes. AhnLab Endpoint Detection and Response (EDR) is capable of detecting such attack techniques through its trace data, and it allows users to check the data required to investigate the related breach case.

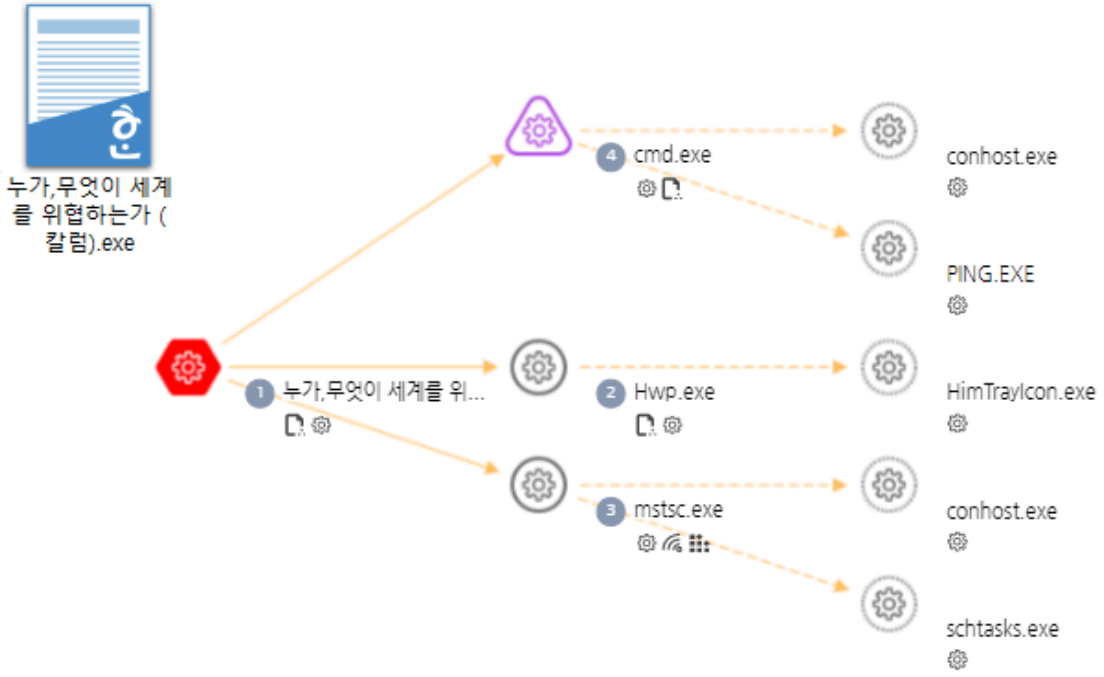
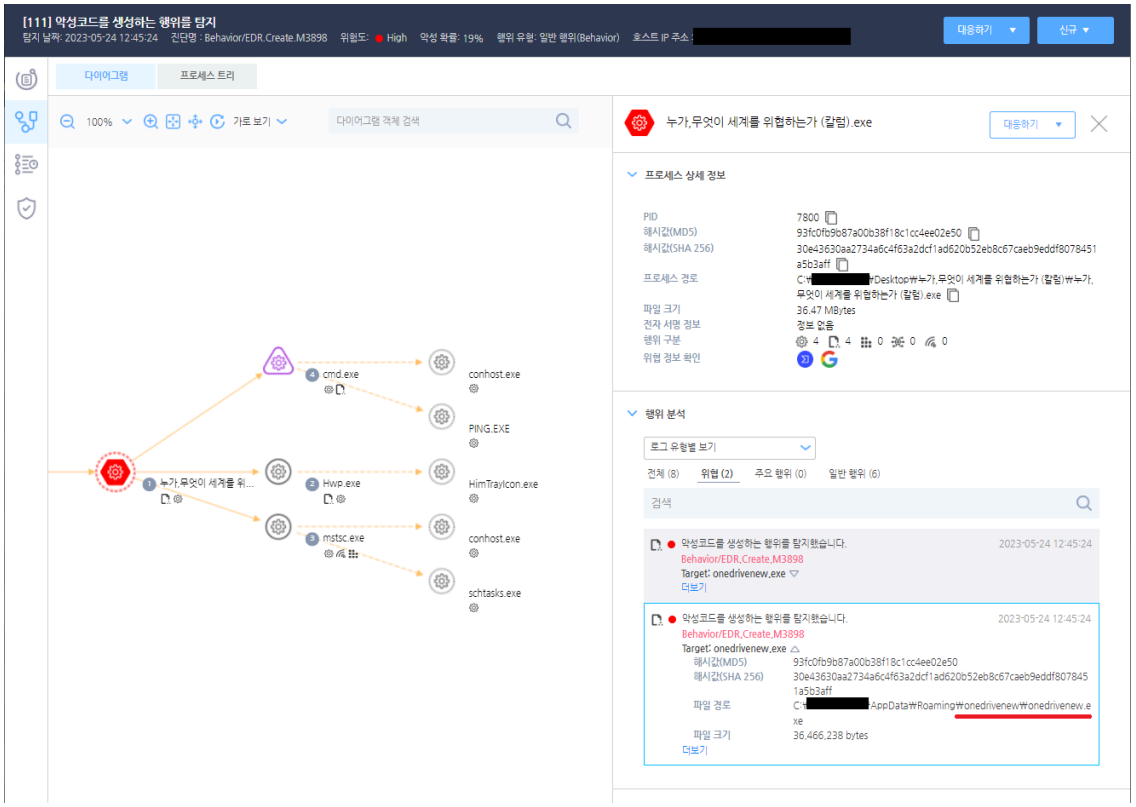
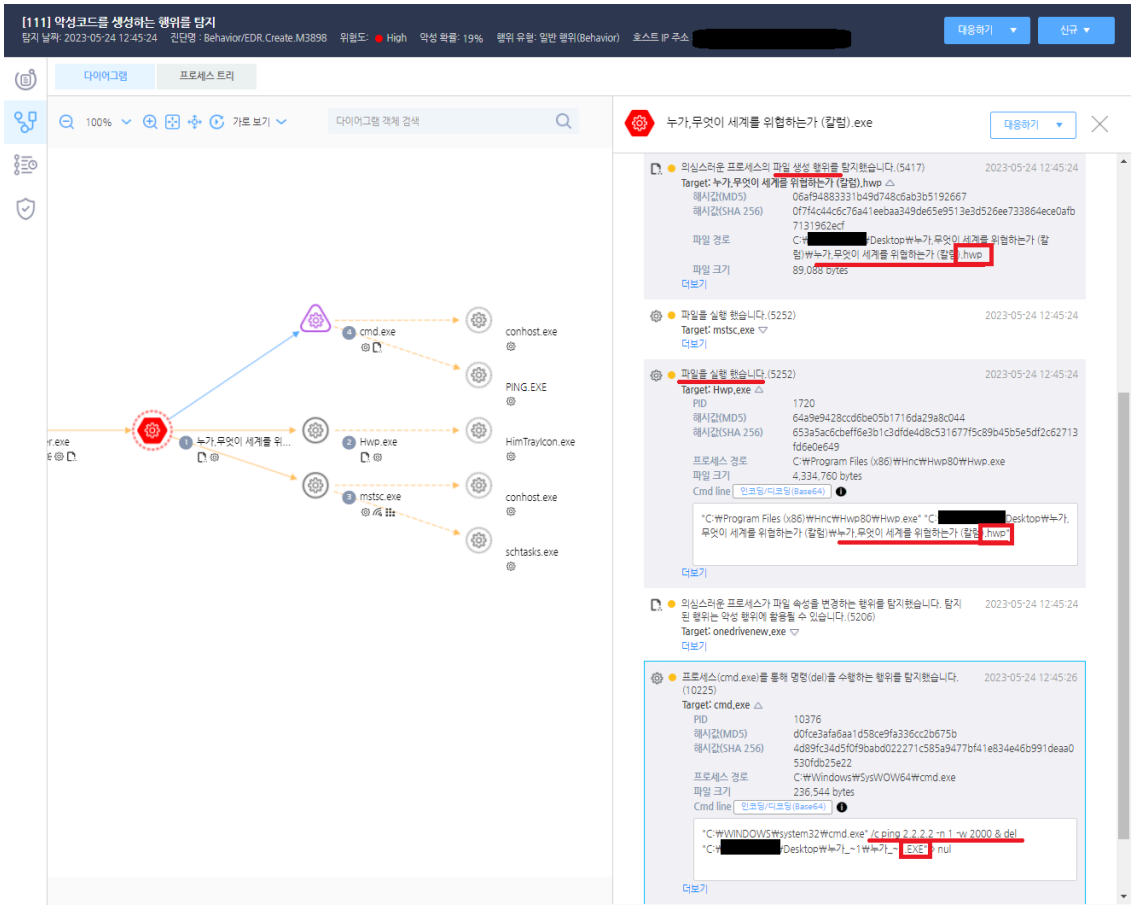


Figure 1 depicts the icon of the malware and its overall execution. It provides a visual representation of which processes are used when the malware is executed.





Figures 2 and 3 show the trace data of key behaviors within the overall flow of the malware. In Figure 2, a trace can be observed of the malware creating a folder named onedrivenew in the AppData directory and self-copying itself with the filename onedrivenew.exe to appear as a normal file. In Figure 3, a trace can be seen of the malware creating and executing a normal Hancom Office file with the same filename as the malware within the same directory where the malware was executed. The malware is injected and executed within the normal Windows process called mstsc.exe. The original file is deleted using the cmd command.

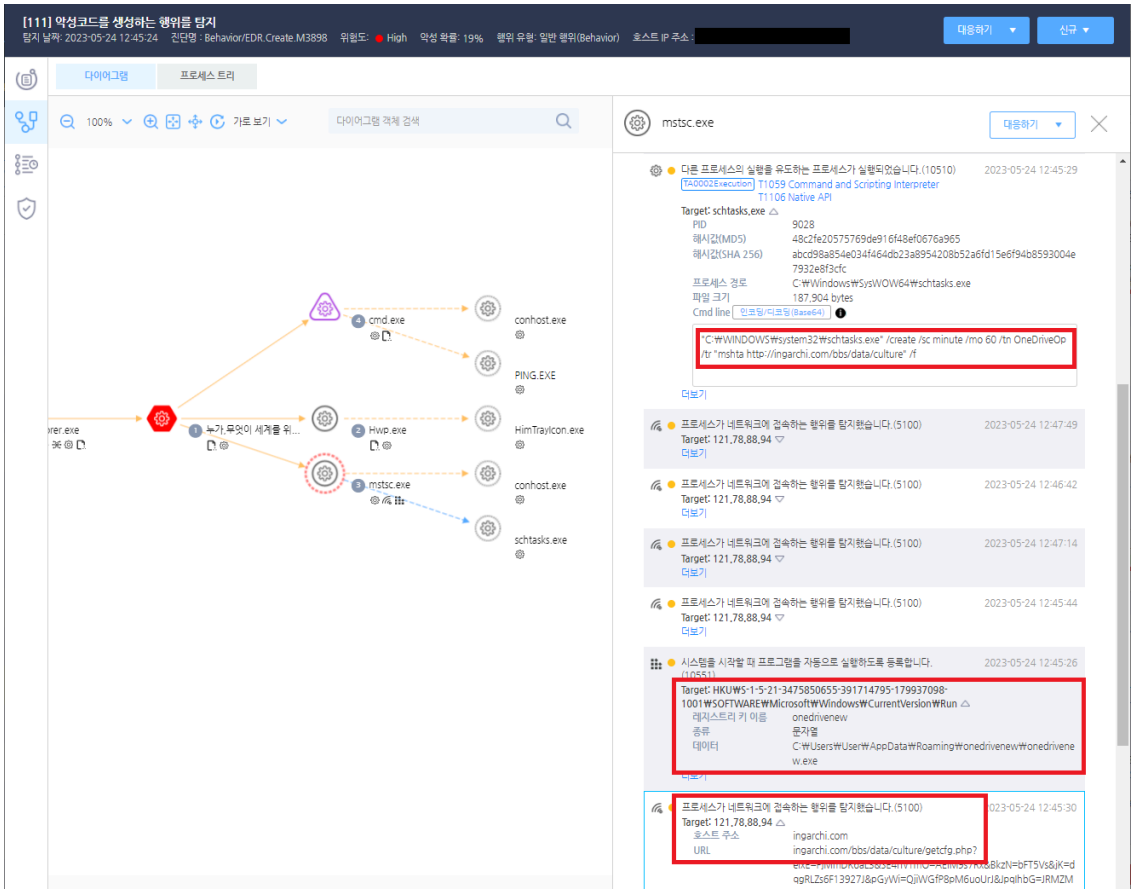


Figure 4 displays the trace data of mstsc.exe being executed after being injected with malware. The malware registers its file with the name onedrivenew under the Run key in order to make it run after the system is rebooted. Afterward, it uses the schtasks.exe command to register the file to the task scheduler with the name OneDriveOp to connect to a certain URL every 60 minutes using the normal Windows file mshta.exe. The URL registered in the task scheduler appears to be a normal homepage, but it contains a web shell. The inserted web shell has been confirmed to be similar to the one posted in “Targeted Attack on a Website Developed by a Specific Web Design Company (Red Eyes and APT37)” on the **AhnLab Threat Intelligence Platform**.

When it comes to targeted attacks, there are factors that general users may struggle to deal with. Even if users find themselves exposed to such threats, AhnLab EDR can provide trace data for appropriate responses.

[File Detection]
– Trojan/Win.Agent.R580958 (2023.05.24.02)

MD5

93fc0fb9b87a00b38f18c1cc4ee02e50

Additional IOCs are available on AhnLab TIP.

URL

http[:]//ingarchi[.]com/bbs/data/culture

http[:]//ingarchi[.]com/bbs/data/culture/getcfg[.]php

Additional IOCs are available on AhnLab TIP.

To learn more about **AhnLab EDR**'s advanced behavior-based detection and reponse, please click the banner below

Source: https://asec.ahnlab.com/en/53377/