Qakbot Being Distributed via OneNote - ASEC

By ATCP

Published: 2023-02-15 · Archived: 2026-04-05 16:49:17 UTC

Back in January, AhnLab ASEC published an analysis report on a malware strain that was being distributed through Microsoft (MS) OneNote.

As mentioned in the report, there has recently been an increasing number of cases where commodity malware like Qakbot stopped using MS Office Macro, their past distribution method, and instead started to use OneNote to execute their malware.

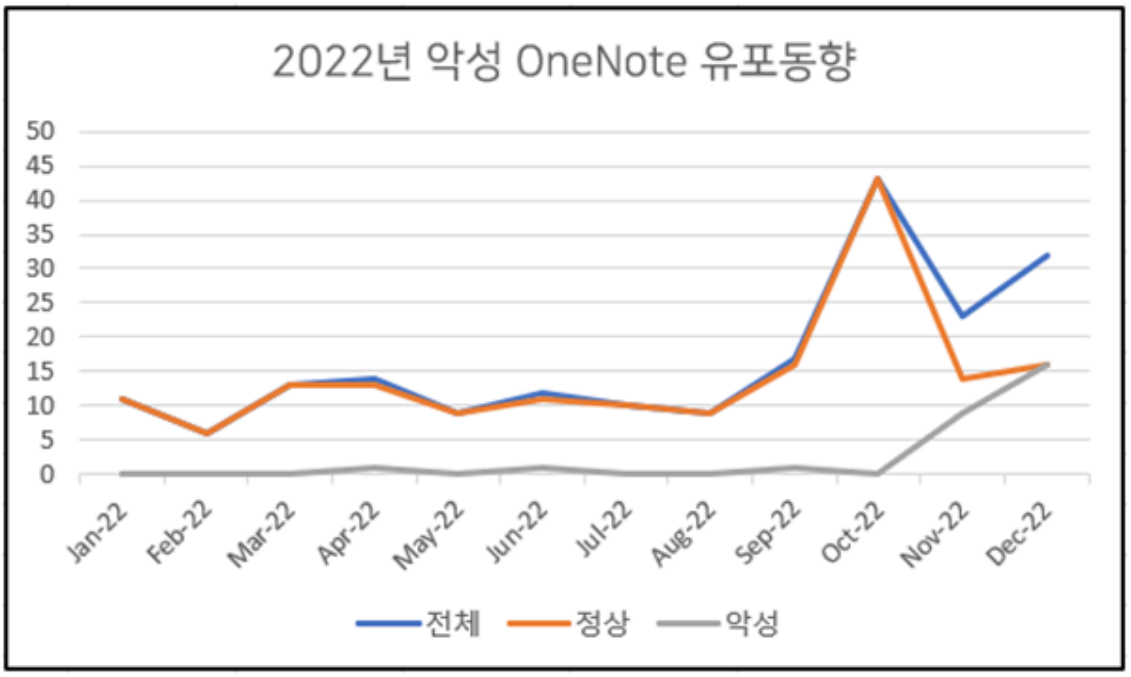

Figure 1. Distribution trend of malicious OneNote files in 2022

If you look at the Qakbot distribution via OneNote case that happened on February 1st, the threat actor distributed the OneNote malware as an attachment to an Outlook email as shown in Figure 2.

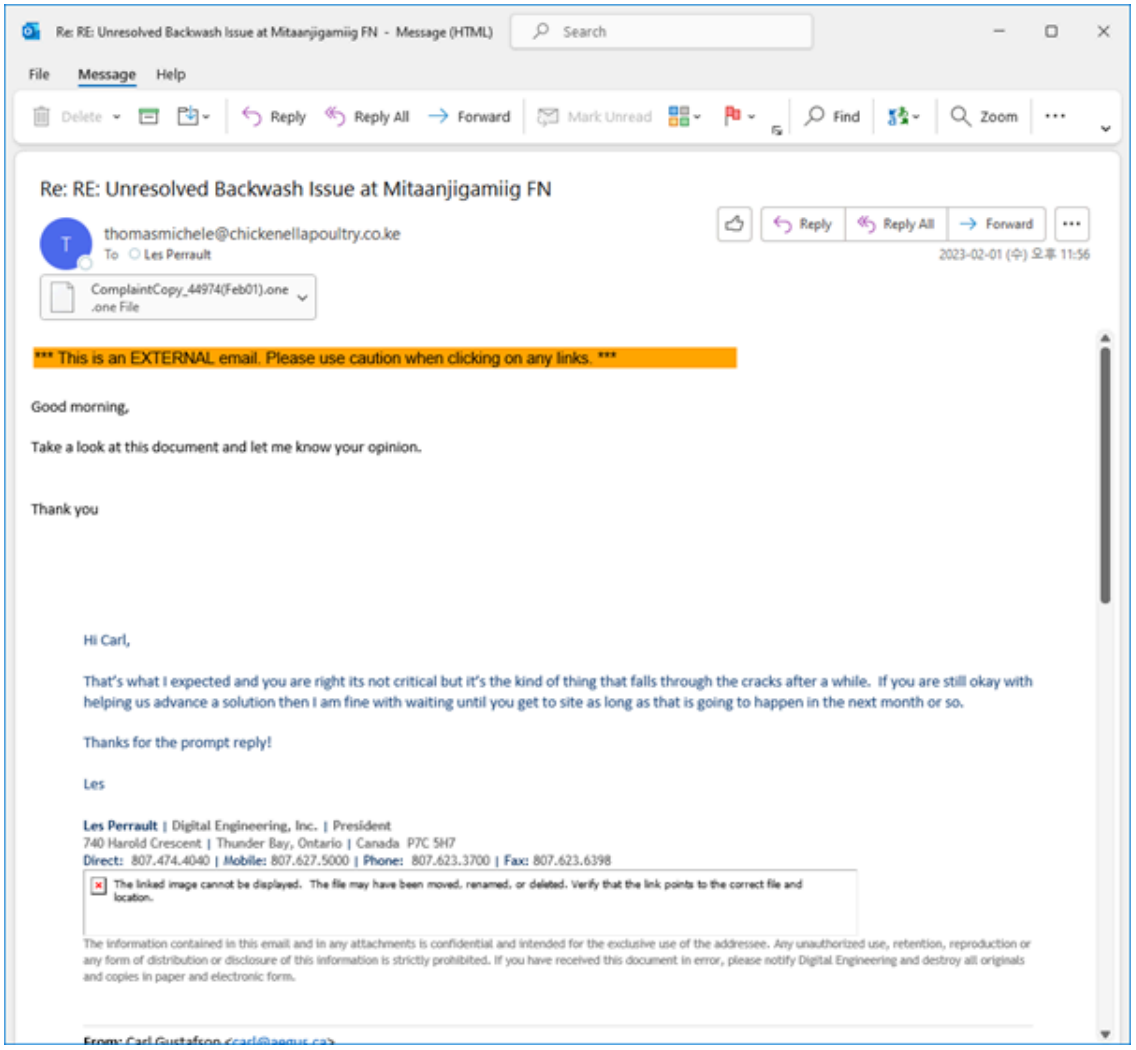

Figure 2. OneNote malware attached to an Outlook email (ComplaintCopy_44974(Feb01).one)

When users open the attachment, it prompts them to click the “Open” button like in the typical MS Office Macro malware. As shown in Figure 3, however, there is actually a hidden HTA (HTML Application) object near the “Open” button. Thus, users are led to believe they had clicked the “Open” button when they had actually executed the HTA object.

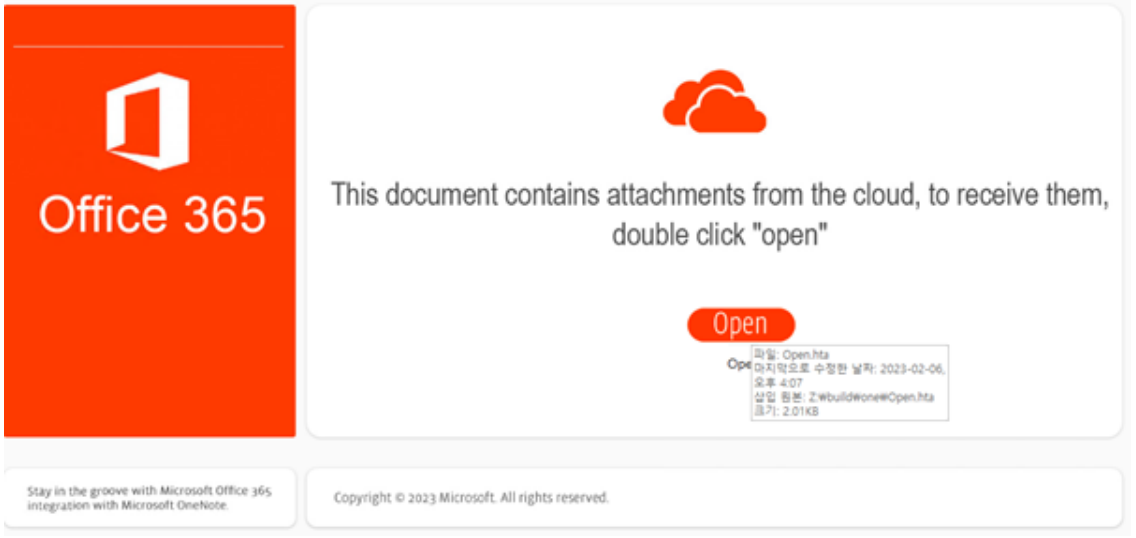

Figure 3. Malicious HTA object (Open.hta) embedded in OneNote

When a user clicks the “Open” button, the HTA file attached as an object to the OneNote is generated in a temporary path. Afterward, the mshta process, which is an HTA extension connection program, is used to ultimately execute the malicious HTA file. A malicious VBS code is included within the HTA and Qakbot is downloaded through curl, a normal Windows utility. Finally, Qakbot is executed by rundll32.exe.

- OUTLOOK.EXE -> ONENOTE.EXE -> ONENOTEM.EXE ->mshta.exe -> curl.exe -> rundll32.exe

Figure 4. Process tree diagram displayed on AhnLab EDR analysis screen

AhnLab EDR (Endpoint Detection and Response) records and detects the behavior information of OneNote format malware threats. Therefore, EDR managers can check if their company’s infrastructure is at risk of OneNote related malware by performing an EDR history search.

- How to check for OneNote threat logs: Event -> EDR Behavior -> Define Period -> Search for EDR threats (ONENOTE.EXE)

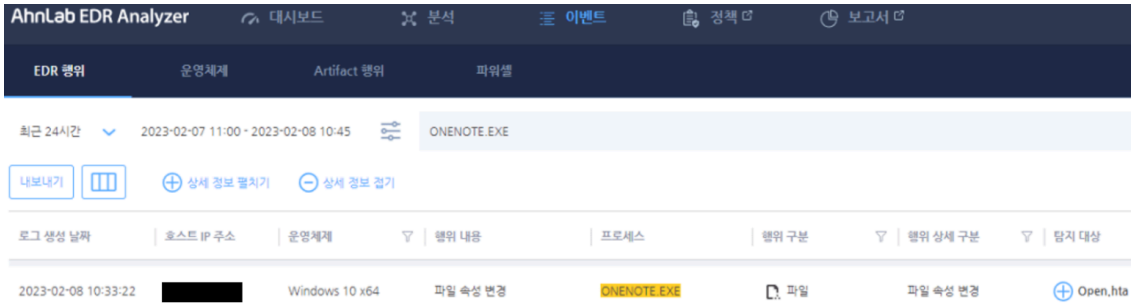

Figure 5. Checking the EDR behavior log (ONENOTE.EXE creates the Open.hta file)

The Open.hta file that can be seen in Detection Target is the actual malicious script.

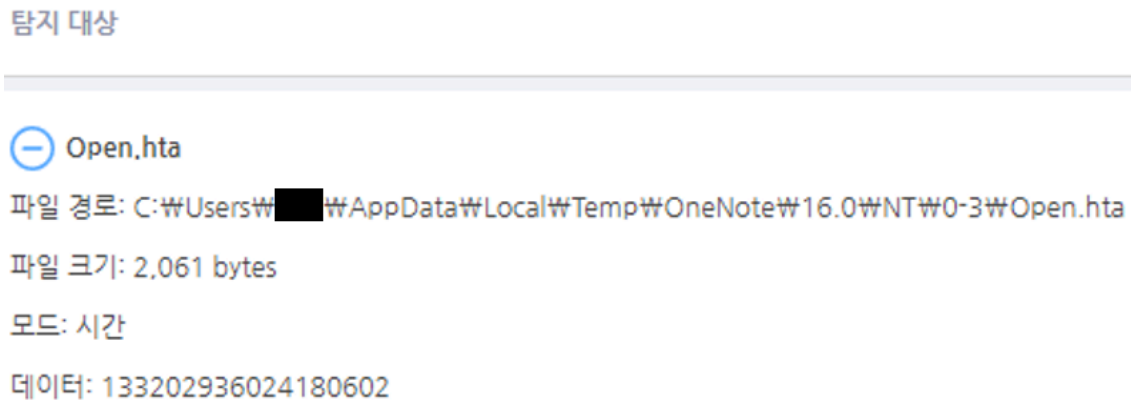

Figure 6. Open.hta file path

The following is the OneNote threat information that can be checked on the AhnLab EDR analysis screen.

[**MITRE ATT&CK Information**]

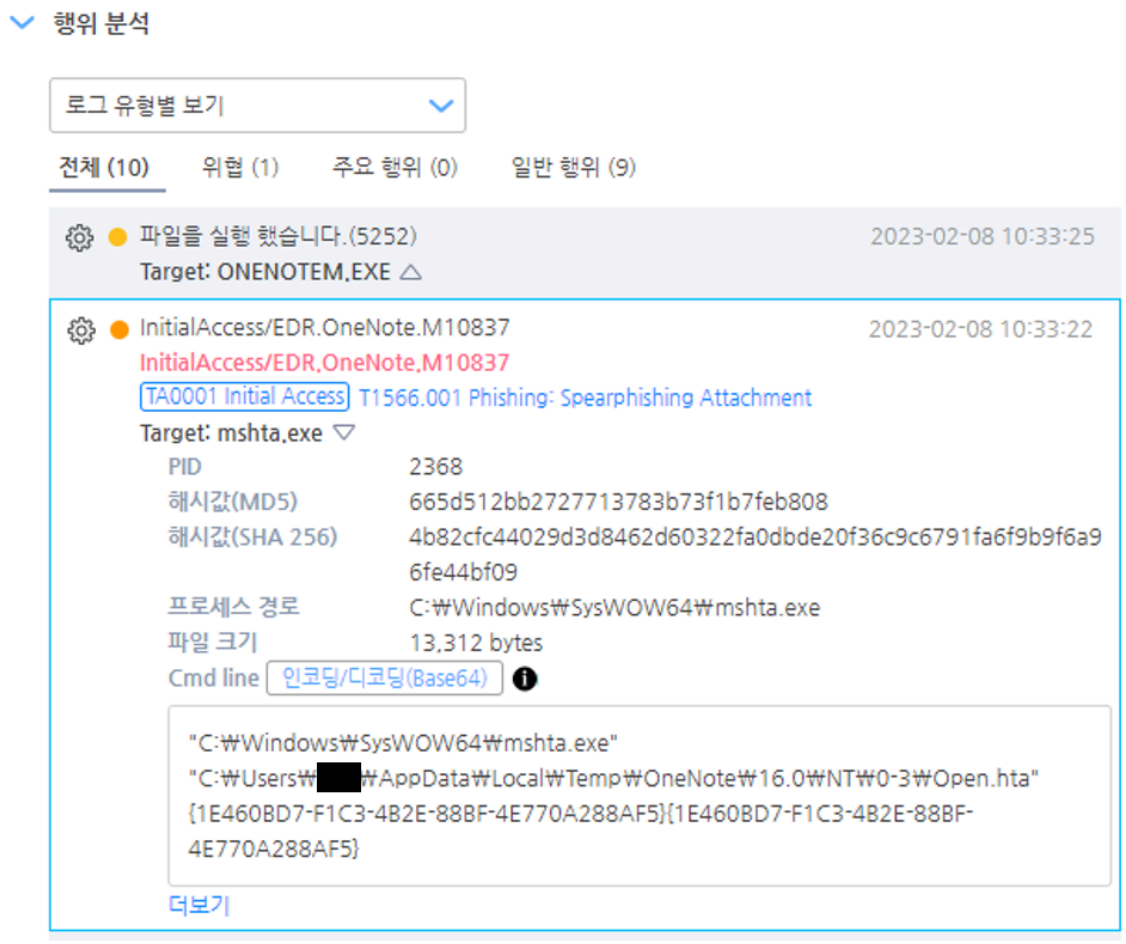

Figure 7. MITRE ATT&CK information (Detected on initial infiltration through spear phishing attachment)

[**File, Registry, Process, and Network-Related Artifact Information**]

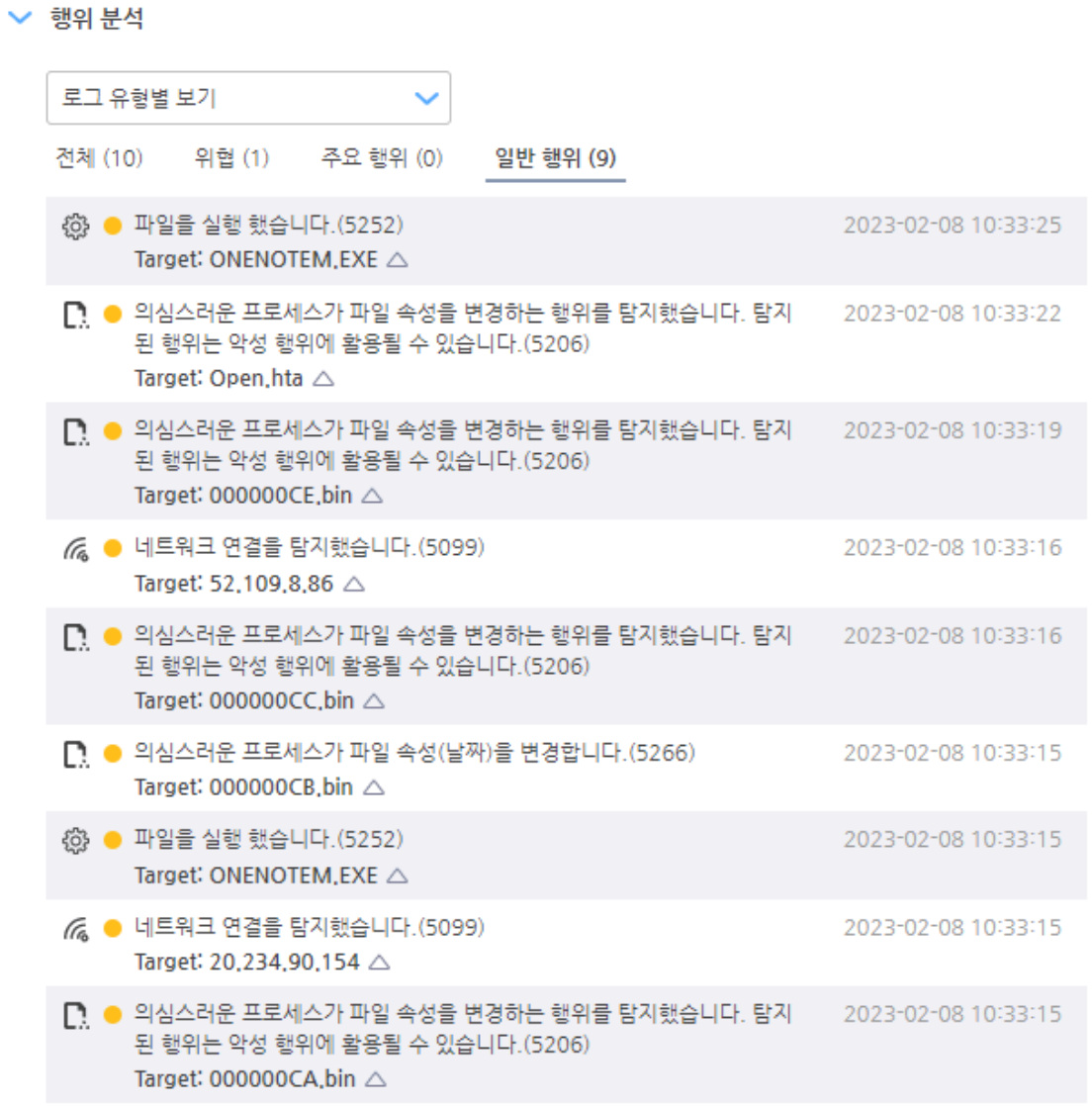

Figure 8. Artifact information

In this OneNote malware case, the HTA file that is an object within the OneNote is what performs the actual malicious behavior. Therefore, EDR managers can check the information related to the threat file, like the information shown in Figure 6, to learn where an HTA file was created and use the information to collect evidential files.

There is a case where Qakbot ultimately infected an organization with ransomware after infiltrating their system and carrying out lateral movement, so it is advised to quarantine a PC's network first if Qakbot is detected early on in order to prevent further harm.

[Network Quarantine Method Using EDR]

Figure 9. Agent response using EDR

AhnLab V3 and EDR products detect this OneNote threat with the aliases below.

[File Detection]

Downloader/HTA.Generic.S2106 (2023.02.03.03)

[Behavior Detection]

InitialAccess/EDR.OneNote.M10837

Execution/EDR.Curl.M10842

[IOC]

MSG : 8b46417297995d5a9a705b54303ace30

HTA : bc6e2129bbd64375c9254fbd17ab5f14

C&C : hxxp://139.99.117.17/31828.dat

The MITRE ATT&CK mapping of the Qakbot that was distributed via OneNote is as follows.

- T1566.002 Phishing: Spearphishing Link, Sub-technique
- T1218.005 System Binary Proxy Execution: Mshta
- T1218.011 System Binary Proxy Execution: Rundll32
- T1105 Ingress Tool Transfer

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.
