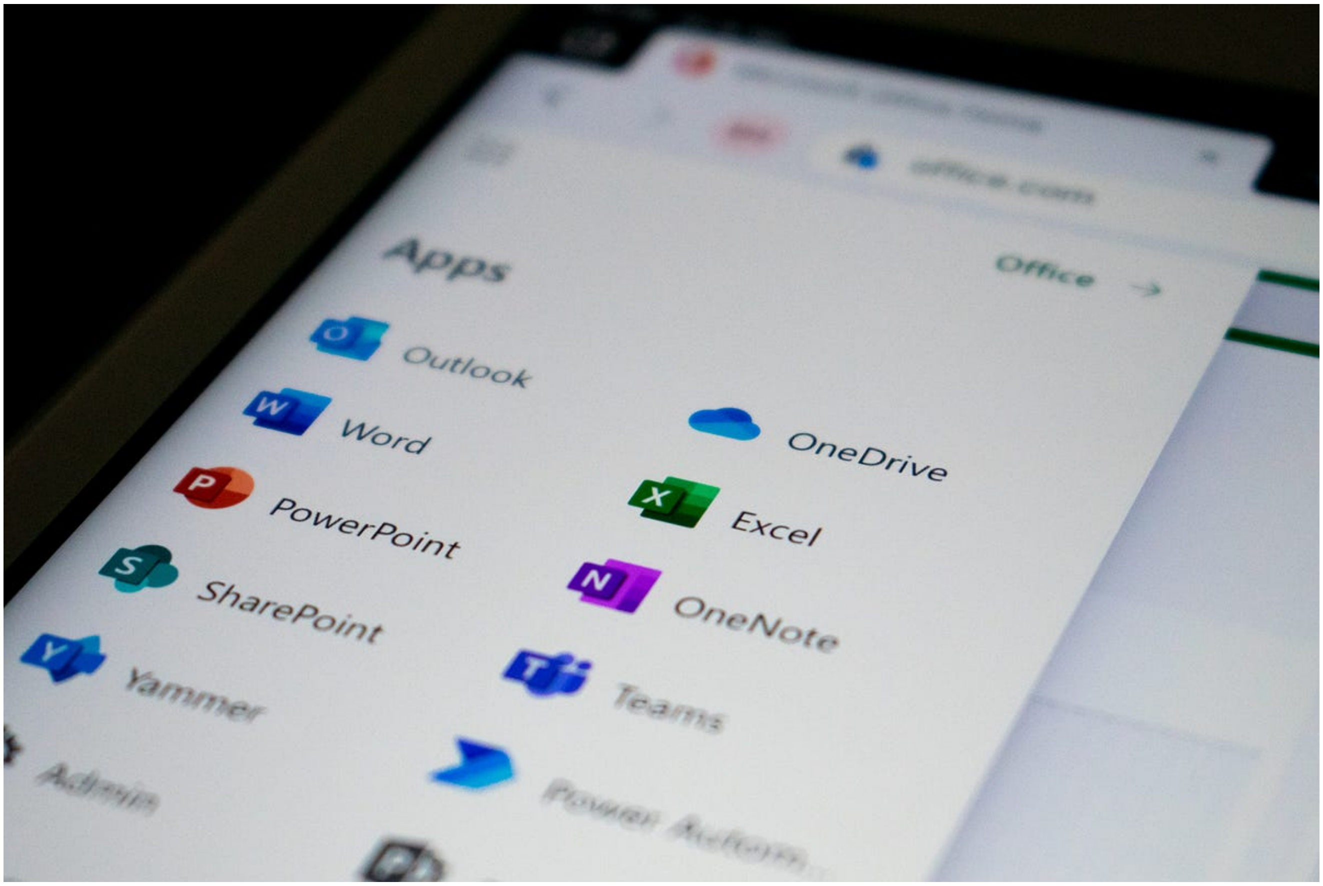
Kimsuky group appears to be exploiting OneNote like the cybercrime group

medium.com/s2wblog/kimsuky-group-appears-to-be-exploiting-onenote-like-the-cybercrime-group-3c96b0b85b9f

S2W

March 20, 2023



S2W

Mar 17

·

4 min read

Author: BLKSMTH | S2W TALON

> *: Mar 17, 2023*

Photo by on

Executive Summary

- We have confirmed that the Kimsuky group is distributing malware using a malicious OneNote (.ONE) file, which cybercriminals have widely used.
- When viewed, the ONE file displays an image of the and asks the target to fill out a privacy agreement document in order to pay them for participating in a survey.
- The HWP file is a simple image, not a real attachment, and double-clicking on its location executes a malicious VBS script hidden behind the image to download additional malware.
- While the final payload is unavailable, the Kimsuky group is believed to be behind this malicious OneNote campaign due to the parameters the group has used to distribute the malware and its fake email disguised as a form of compensation.

Technical Details

On March 17, 2023, a OneNote file containing a malicious script was uploaded on Virustotal impersonating the *Institute for Peace and Democracy at Korea University*. The file was submitted from South Korea. The OneNote file asks survey participants to fill out a hangul word processor(.HWP) document (Personal Information Use Agreement) in order to receive recompense. To do this, the image contains a .hwp file icon and file name disguised as a download, and the user is encouraged to double-click it. The double-click triggers the execution of a malicious VBS file hidden behind the image, which then downloads additional malware from an external server.

Figure 1. The image is seen when opening OneNote
When the image is moved as shown below, the VBS file icon appears behind it, and the previously known exploitation method of OneNote is applied in the same way. At this time, the same VBS files are arranged in a row, which is to ensure that the VBS file is executed even if the victim presses any part of the file.

Figure 2. Malicious VBS scripts behind the image
When the script is executed, the obfuscated code is executed and additional files are downloaded from the address below. No additional downloads were made at the time of analysis. The downloaded HWP file will be stored in the Downloads path(%Userprofile%\Downloads\personal.hwp), which is presumed to be a normal document to appear as if the target downloads the document normally.

Figure 3. Embedded VBS script code

- Download HWP file: hxxp[:]//delps.scienceontheweb[.]net/ital/info/sample.hwp
- Download malware : hxxp[:]//delps.scienceontheweb[.]net/ital/info/list.php?query=1

In addition to downloading additional files, access specific registries and change values as shown below.

- HKCU\Software\Microsoft\Internet Explorer\Main => no => 1
- HKCU\Software\Microsoft\Edge\IEToEdge => 0

The Kimsuky group has been distributing malware by sending phishing e-mails containing false compensation for several years. The image in OneNote discovered this time also deals with the same theme. In addition, the URL that the VBS script requests to download is the same as the address format used when distributing the Babyshark malware, and the hosting server that the Kimsuky group frequently uses is used for the same purpose.

> Address format has been used by the Kimsuky group: hxxp[:]//[URL]/

This URL format has already been disclosed in the past and has been attributed to the Kimsuky group.

In addition, the server that downloads the additional malware resolves to **185.176.43[.]98**, which the Kimsuky group has been using continuously.

Conclusion

- We've seen a number of recent cases of cybercrime-related malware such as Qakbot, Redline Stealer, and AsyncRAT being distributed by attaching malicious OneNote files to emails, but this is the first time we've seen it utilized by an APT group from North Korea.
- However, there is a possibility that it is a test stage before full-scale use in that a number of strings " were confirmed in the script.
- Microsoft mentioned on March 10th that they will introduce an option for embedded files to prevent malware infection due to malicious OneNote files, and it is highly likely that the Kimsuky group will be used as a new distribution method until the introduction.
- In order to prevent malware infection from malicious OneNote, if a suspicious OneNote file is attached to an e-mail received from outside, care must be taken not to open the file.

IoC

- aa756b20170aa0869d6f5d5b5f1b7c37 (OneNote)
- f2a0e92b80928830704a00c91df87644 (VBS)
- hxxp[:]//delps.scienceontheweb[.]net/ital/info/sample.hwp
- hxxp[:]//delps.scienceontheweb[.]net/ital/info/list.php?query=1