TLP: AMBER

Threat Trend Report on Operation Triple Tiang

Cyber Operation Targeting the Political and Diplomatic Sectors of South Korea

V1.0

AhnLab Security Emergency Response Center (ASEC)

Mar. 31, 2022

AhnLab

Classification

Publications or provided content can only be used within the scope allowed for each classification as shown below.

Classification	Distribution Targets	Precautions
TLP: RED	Reports only provided for certain clients and tenants	**Documents that can only be accessed by the recipient or the recipient department** Cannot be copied or distributed except by the recipient
TLP: AMBER	Reports only provided for limited clients and tenants	**Can be copied and distributed within the recipient organization (company) of reports** Must seek permission from AhnLab to use the report outside the organization, such as for educational purposes
TLP: GREEN	Reports that can be used by anyone within the service	**Can be freely used within the industry and utilized as educational materials for internal training, occupational training, and security manager training** Strictly limited from being used as presentation materials for the public
TLP: WHITE	Reports that can be freely used	Cite source Available for commercial and non-commercial uses Can produce derivative works by changing the content

Remarks

If the report includes statistics and indices, some data may be rounded,
meaning that the sum of each item may not match the total.

The version information of this report is as follows:

Version	Date	Details
1.0	2022-03-31	First Version

Contents

CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Operation Triple Tiang

1) Introduction

Operation Triple Tiang is an operation that has been attacking the diplomatic and political sectors of South Korea since May 2020. It has been named "Triple Tiang" because the malware used in the attack is structured into three stages with CHM, DLL, and VBS files, and the string “Tiang” was found in the early version of the malware. Tiang is an English word for the subspecies of Topi, an African antelope, and means “pole” in Indonesian. However, the purpose of the creator using this string has not been identified.

2) Attack Targets and Actual Cases

The targeted areas and sectors of this threat group's attacks are as follows.

Date	Target	Details
February 2022	Korean government organizations	The CHM file has not been detected; details are unknown. LBTServ.dll (519463908135209613 1cbdab7fe318fe) and VBE (7512c80de88ebe7646c0a97c12e7ad2a)
March 2022	Korean government organizations	Three attacks using CHM files including political content

Table 1. Major attack cases

In February and March 2022, the threat actors attacked government organizations in South Korea. Based on the bait content of other malware, their main targets seem to be political and diplomatic organizations. There have been no identified cases targeting countries other than Korea.

3) Attack Method (Attack Vectors)

While the precise attack method has yet to be identified, we can forecast attacks using an email attached with a Compiled HTML Help (CHM) file with a topic to interest the targets. When the user opens the CHM file, a normal program is executed, and a DLL file needed for execution is found and loaded. The malicious DLL file creates a malicious Visual Basic script file that executes remote commands.

4) Changes

The key timeline is as follows.

Date	Details
May 2020	EXE dropper first appeared
March 2021	DLL dropper appeared, estimated to be the beginning of attacks using CHM files
April 2021	Target-identifying variable added in the ReVBShell
October 2021	File names changed to LBTWiz32.exe and LBTServ.dll

Table 2. Timeline

The threat actor created an EXE-type malware in May 2020. The attack method and targets have not been identified. In March 2021, a DLL-type dropper was found, and it is thought to have used a CHM file in the attack. The initially used file names are vias.exe and quartz.dll. An identification variable has been added to the ReVBShell malware since April 2021 to identify attack targets. Since October 2021, the threat actor switched the file names from vias.exe and quartz.dll to LBTWiz32.exe and LBTServ.dll.

5) Major Malware

The major malware used by this threat group are as follows.

(1) EXE Dropper (2020)

The dropper which rose to the surface in May 2020 (md5: f5b2c4f6257eee31e412bbc874ba05f3) was in EXE format, and the precise method of infection has not been determined. The identified file names are wwcuserup.exe and seco2.exe, and the file size is in a range of 62-78 KB.

The malware contains the string "Tiang".

Figure 1. String "Tiang"

The main function is as follows.

```
1  int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
2  {
3    HMODULE LibraryA; // eax
4    HMODULE hModule; // [esp+4h] [ebp-8h]
5
6    hModule = LoadLibraryA(LibFileName);
7    CreateFileA_0 = (HANDLE (__stdcall *)(LPCSTR, DWORD, DWORD, LPSECURITY_ATTRIBUTES, DWORD, DWORD, HANDLE))GetProcAddress(hModule, ProcName);
8    ReadFile = (BOOL (__stdcall *)(HANDLE, LPVOID, DWORD, LPDWORD, LPOVERLAPPED))GetProcAddress(hModule, aReadfile);
9    WriteFile_0 = (BOOL (__stdcall *)(HANDLE, LPCVOID, DWORD, LPDWORD, LPOVERLAPPED))GetProcAddress(hModule, aWritefile);
10   LibraryA = LoadLibraryA(aShell32Dll);
11   ShellExecuteA = (HINSTANCE (__stdcall *)(HWND, LPCSTR, LPCSTR, LPCSTR, LPCSTR, INT))GetProcAddress(
12                                                                                       LibraryA,
13                                                                                       aShellexecutea);
14   if ( !CreateFileA_0 || !ReadFile || !WriteFile_0 || !ShellExecuteA )
15     ExitProcess(0xFFFFFFFF);
16   Loop_4016BB(34, (int)aTiangA, (int)aTiangB, (int)aTiangC);
17   Drop_40149C();
18   Drop_401000();
19   return 0;
20 }
```

Figure 2. Main function

When the main function is executed, it finds the necessary API address and generates the 1.VBS file which deletes the EXE file that is executed after a delay.

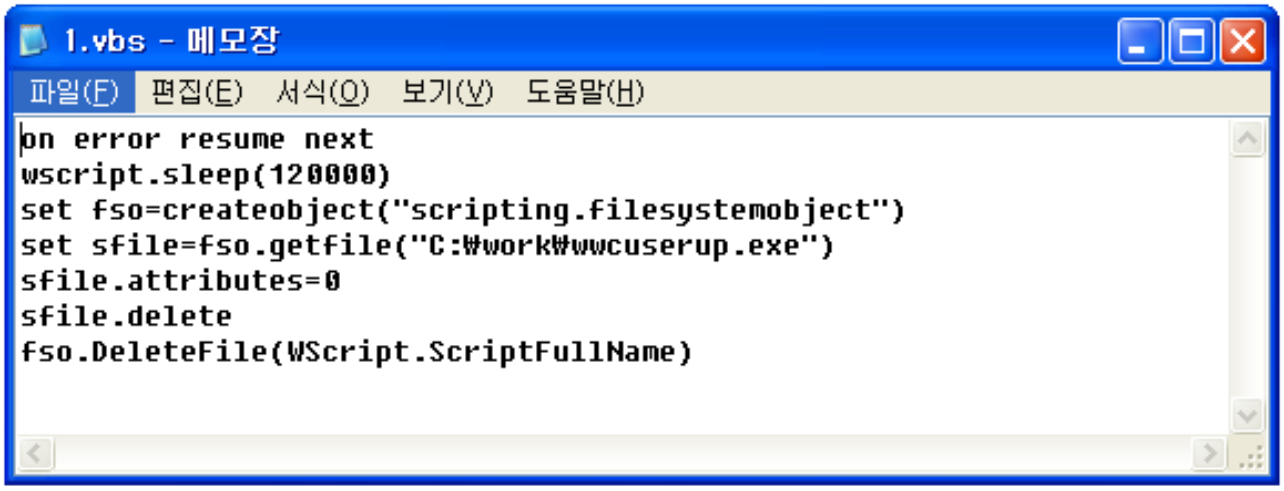

Figure 3. VB script deleting the executable file

It then creates the 2.VBE file, which is an obfuscated form of ReVBShell.

Figure 4. Content of 2.VBE

When the VBE file is decrypted, we can see the content of the VB script.

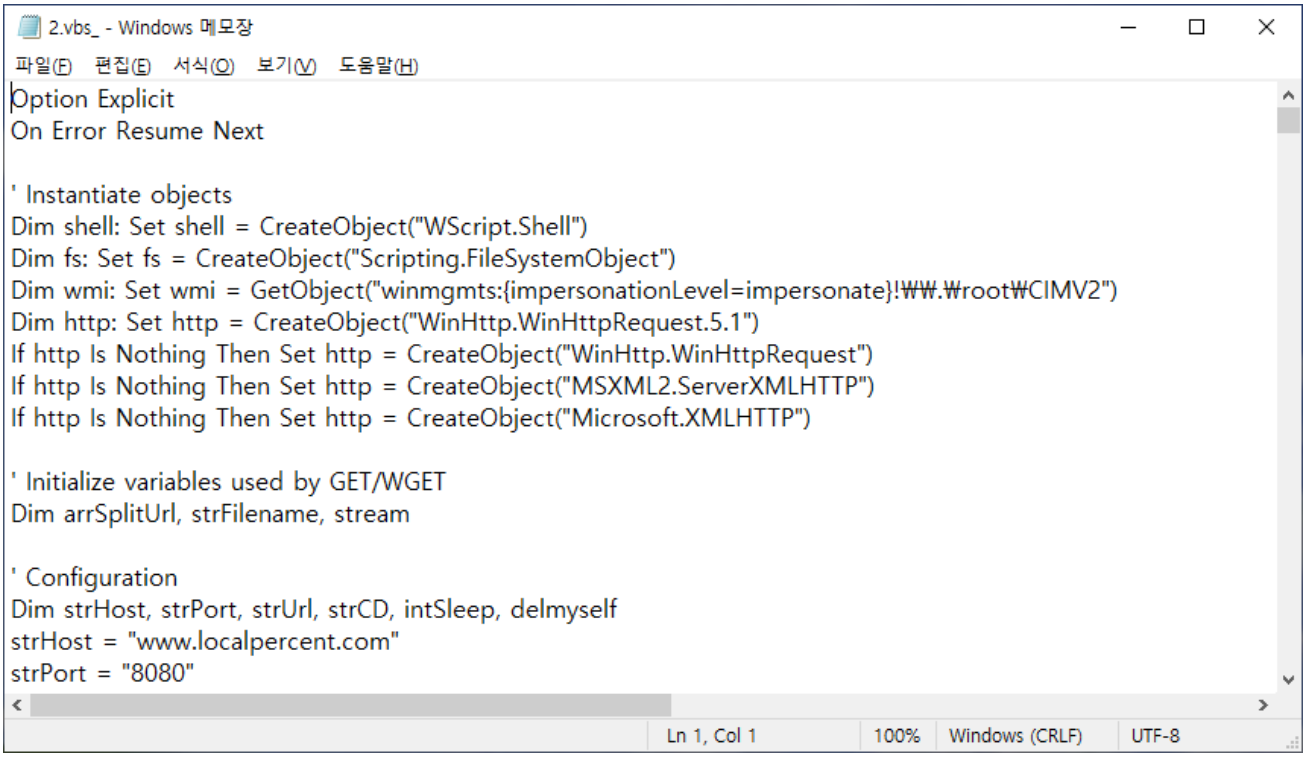

Figure 5. VB script content

(2) CHM Dropper

While CHM droppers had been first found in June 2021 (md5: 622303ba7224abf3fa79073b82e5f10f), related DLL files were being detected since March 2021; it is likely that variants existed from earlier points in time. The detected CHM file contains topics of interest to personnel in the diplomatic and political sectors.

The paths and names of the files generated by CHM dropper differ according to the time of their creation.

Date	Details
June - August 2021	Generated vias.exe and quartz.dll in the C:₩ProgramData directory
March 2022 (Presumed to be after October 2021)	Generated LBTWiz32.exe and LBTServ.dll in the C:₩Windows₩Temp directory

Table 3. File generation path for each CHM version

The CHM files detected between June and August 2021 create files in the C:₩ProgramData directory and execute vias.exe.

```
<PARAM name="Command" value="ShortCut">
 <PARAM name="Button" value="Bitmap::shortcut">
 <PARAM name="Item1" value=',C:₩₩programdata₩₩vias.exe'>
 <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><img src="LTC_na_go_009.jpg">
```

Figure 6. Files executed by CHM found in 2021

Changes were made to the CHM file detected in March 2022 so that it creates files in the C:₩Windows₩Temp directory and executes LBTWiz32.exe. The malware with the name LBTServ.dll loaded by LBTWiz32.exe had already been identified in October 2021. There is a high possibility that changes were made to the CHM file around this time.

```
</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₩₩LBTWiz32.exe'>
 <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><img src="theminjoo_006.jpg">
```

Figure 7. Files executed by CHM found in 2022

(3) DLL Dropper (since March 2021)

In March 2021, the format changed from the previous EXE dropper to the DLL file format (md5: 725cc3b6b3d96f0a4715ef1fa8fa71ca). The file size is in a range of 76-112 KB.

The identified normal file and the loaded DLL file are as follows.

Normal EXE	Loaded DLL	Details
vias.exe	quartz.dll	vias.exe is a normal DirectShow SDK Filter Graph Editor file
LBTWiz32.exe	LBTServ.dll	LBTWiz32.exe is a normal Logitech Bluetooth Wizard Host Process file

Table 4. Normal EXE and the loaded DLL

Between March and August 2021, vias.exe and quartz.dll were used, and since October 2021, LBTWiz32.exe and LBTServ.dll have been used.

The details of the main function of the malicious DLL file are as follows.

```
1  BOOL __stdcall DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
2  {
3    HMODULE v4; // [esp+0h] [ebp-21Ch]
4    CHAR Filename[264]; // [esp+4h] [ebp-218h] BYREF
5    CHAR String1[268]; // [esp+10Ch] [ebp-110h] BYREF
6
7    if ( fdwReason == 1 )
8    {
9      DisableThreadLibraryCalls(hinstDLL);
10     if ( !CountFileTemp_10002630() )            // > 18 ?
11       ExitProcess(0);
12     strcpy(String1, "LBTWiz32.exe");
13     memset(&String1[13], 0, 0xF7u);
14     memset(Filename, 0, 260);
15     GetModuleFileNameA(0, Filename, 0x104u);
16     PathStripPathA(Filename);
17     if ( !lstrcmpiA(String1, Filename) )
18       MalwareMain_10002480();
19   }
20   else if ( !fdwReason )
21   {
22     FreeLibrary_10002810(v4);
23   }
24   return 1;
25 }
```

Figure 8. Main function of the DLL file

When executed, the DLL file checks for 18 or more files in the temporary directory along with the process names. After then, it terminates the processes if they do not match the set conditions. This action is thought to be intended by the creator of the malware to serve the purpose of detecting the analysis environment.

The file patches a certain location of the process (0x401000) with a NOP command and obtains the necessary API address. Then, it makes modifications to the registry to allow the malicious DLL file to be run and creates the malicious VBE file.

```
32  v2 = LoadLibraryA("Advapi32.dll");
33  RegOpenKeyExA = (LSTATUS (__stdcall *)(HKEY, LPCSTR, DWORD, REGSAM, PHKEY))GetProcAddress(v2, "RegOpenKeyExA");
34  v3 = LoadLibraryA("Advapi32.dll");
35  RegCloseKey = (LSTATUS (__stdcall *)(HKEY))GetProcAddress(v3, "RegCloseKey");
36  v4 = LoadLibraryA("Shell32.dll");
37  ShellExecuteA = (HINSTANCE (__stdcall *)(HWND, LPCSTR, LPCSTR, LPCSTR, LPCSTR, INT))GetProcAddress(
38                                                                                      v4,
39                                                                                      "ShellExecuteA");
40  if ( !WinExec || !CreateFileA || !ReadFile || !WriteFile_0 )
41    ExitProcess(0xFFFFFFFF);
42  sub_10002160(34, (int)&unk_100091A8, (int)&unk_100091AC, (int)&unk_100091B0);// A B C
43  SetRegistry_100021B0();
44  DropExecute_100016C0();
45  ExitProcess(0xFFFFFFFF);
46 }
```

Figure 9. Registry modification and file dropping

The overall code structure is similar to EXE droppers. The VBE file created is a variant of ReVBShell, which is also just like EXE droppers.

(4) ReVBShell

The VBE file created by the malware has a length of 17-21 kb and was developed based on ReVBShell.[1]

ReVBShell is a remote control program developed with VBS. It offers features such as file management, system information such as network information and process lists, and uploading and downloading of files.

[1] https://github.com/bitsadmin/revbshell

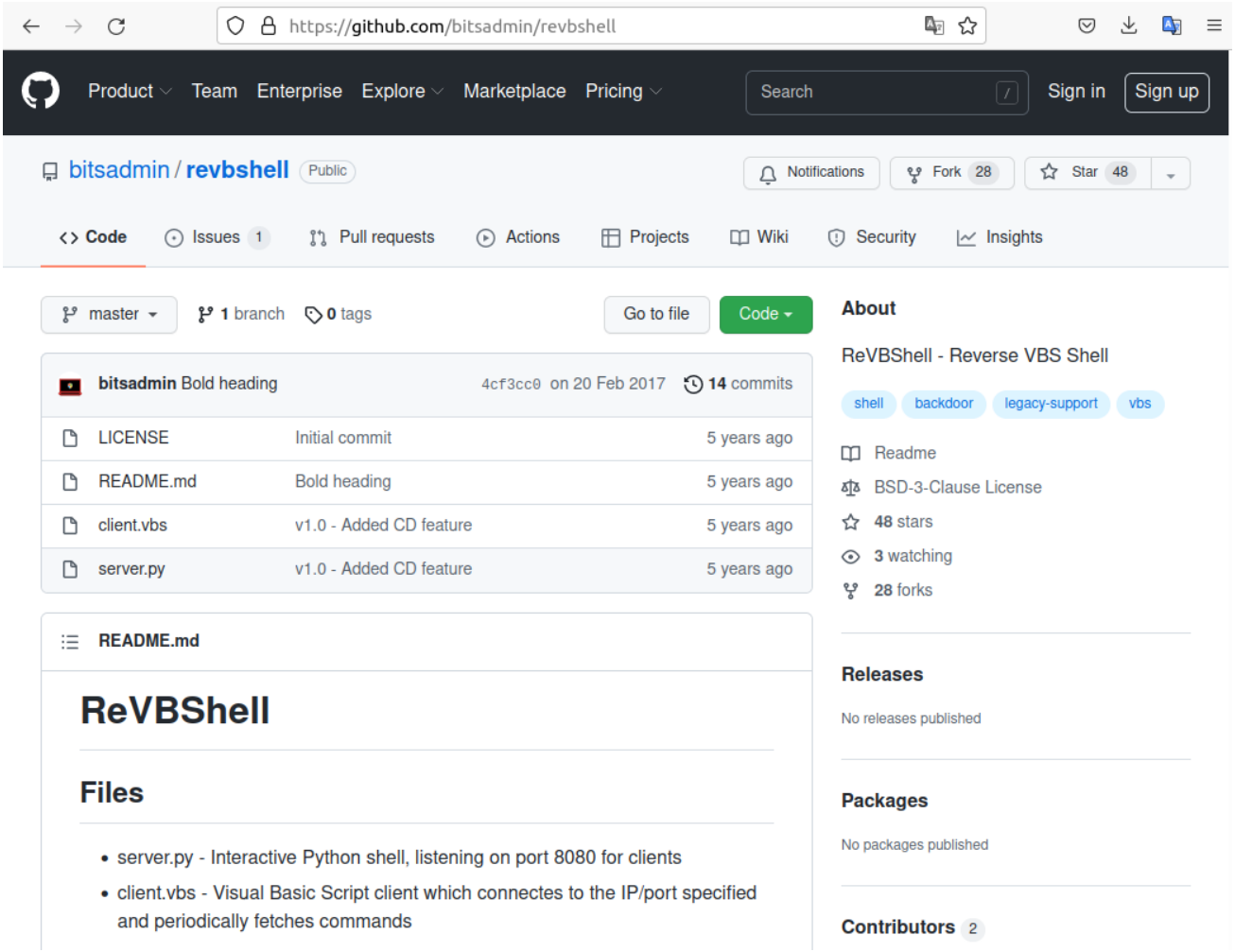

Figure 10. ReVBShell

The threat actor partially modified the ReVBShell code, adding EXEC, INTERVAL, and WMIC commands.

Command	Details
CD	Change directory
DOWNLOAD	Download file
EXEC	Execute file
GETUID	Obtain user ID
IFCONFIG	Configure network
INTERVAL	Stand by for a certain period of time
KILL	Terminate script

NOOP	Delay for a certain period of time
PS	Process list
PWD, GETWD	Obtain current path
SHELL	Send the command to cmd.exe
SLEEP	Stand by for a certain period of time
SYSINFO	System information
WGET	Download file
WMIC	Obtain network information with the WMI command (However, in most variants, this is written as a comment and unused)

Table 5. Commands of ReVBShell variants

The version created after April 2021 (md5: 4cb012d786b1e5cb465d213498de7bcf) has the variable “p_fg” added to the settings, which is thought to be a value for identifying its attack targets.

AhnLab Response Overview

The alias and the engine version information of AhnLab products are shown below. Even if the activities of this threat group have been identified recently, AhnLab products may have already diagnosed related malware in the past. While ASEC is tracking the activities of this threat group and responding to related malware, there can be variants that have not been identified and thus are not detected.

Backdoor/VBS.Agent (2022.03.22.02)
Backdoor/VBS.Generic (2022.03.23.00)
Backdoor/VBS.Revbshell (2021.08.28.00)
Downloader/VBS.Agent (2022.03.09.00)
Dropper/CHM.Agent (2022.03.11.03)
Dropper/CHM.Akdoor (2021.08.11.00)
Dropper/CHM.Generic (2022.03.11.00)
Trojan/VBE.Agent (2022.03.11.00)

Trojan/Win.Akdoor.R427606 (2021.06.26.00) Trojan/Win.Akdoor.R436386 (2021.08.11.00) Trojan/Win.Akdoor.R439076 (2021.08.28.00) Trojan/Win.Sabsik.R477071 (2022.03.11.00) Trojan/Win.Sabsik.R478979 (2022.03.22.02)

Conclusion

Operation Triple Tiang is a cyber intelligence tactic that specializes in attacking the political and diplomatic sectors of South Korea. While a clear de facto power behind these attacks has not been identified, grounds for suspicion regarding their relationship with threat actors backed by national governments of neighboring countries have been discovered. Because the threat actors use Compiled HTML Help (CHM) files in their attacks, personnel of the political and diplomatic sectors must practice caution when they receive emails with CHM file attachments.

Indicators Of Compromise (IOC)

A portion of the following IOC quotes other analysis reports, and there are some cases that could not be verified because samples could not be obtained. Updates may occur without prior notice when new information is found.

File Paths and Names

The file paths and names used by the threat group are as follows. File names of some malware or tools may be the same as those of normal files.

LBTServ.dll quartz.dll seco2.exe wwcuserup.exe

File Hashes (MD5)

The MD5 of the related files are as follows. However, sensitive samples may have been excluded.

```
040abbe3ffe5f5d719af158f7bb6b48d
08f39efbfa0926607e94e4af1048af84
1aefefbd2fdc4c2cb3d586aa16f93ad8
268cf574f311dd0098835a46443df960
3bef0ac94ee832110af749cca28bf769
3c361815b9abb650ff4f8e2e8cf29715
4072853a1d2cffce6e0ab26f6af2afeb
4651614863490ad62465b2274a4e9314
4796f56230cc349dc1a0eafbb3d5f08b
4cb012d786b1e5cb465d213498de7bcf
4f4515e057f6fca0ab1f594261af7494
5194639081352096131cbdab7fe318fe
56e8a91079640f1d2fc344f373b959b3
58fccb55d5aeb2466bea3119ae04eeb8
5c88e7b84b8a3e55ff6c79c926f6af4b
622303ba7224abf3fa79073b82e5f10f
62bb7a4c3d283a177a9eaaf3f736f549
6df48f8ee30c63bc224b44ed70354c43
709004e664697566f45a2edb56c0c834
725cc3b6b3d96f0a4715ef1fa8fa71ca
7512c80de88ebe7646c0a97c12e7ad2a
8fc953ffcd5f72735bec9ff5d814ce94
925238cfa20604c2f172813558b7e43f
9d74b04067d410c6347d95cf56fac16a
a0376453aced35b1bec1ff6e18e78c5e
a36eae00de5d9f39858de77f2e52ac55
a89c105250859d7f4bfd3a93d0b50156
b166ad04a394e3e6ae5af92d3159c2fb
b584339289a7fb150422fc70325bddfe
be5545a76ea1e53e9c4e697e29faa803
c57d48d648a65ec6e2b0c1ea64b19112
c82eb90175ea1f5e3b658ee67c431698
d253c916295834fd5754ce15fff4156a
d4fb181414913809cdabfd5acca526b8
ddfeec393cec526e4673a0f94d6bca72
e0a34d1ee863958d6a9527c170052954
e1f3f961c424a93a475ab75522802277
```

ee25e751bd00bdd4c09477095443f4be
f1afdfc5265ae4c886e0b6202ae5ef37
f5b2c4f6257eee31e412bbc874ba05f3
f78eef54ce0b18b915b6f0332ee9cb09

Related Domains, URLs, and IP Addresses

The download or C2 addresses used are as follows. http was changed to hxxp, and sensitive information may have been excluded.

alleyk.onthewifi.com
bucketnec.bounceme.net
elecinfonec.servehalflife.com
kjmacgk.ddnsking.com
kumohhic.viewdns.net
leader.gotdns.ch
mafolog.serveminecraft.net
minjoo2.servehttp.com
mintaek.bounceme.net
prparty.webhop.me
sejonglog.hopto.org
signga.redirectme.net
stjpmsko.serveblog.net
themiujoo.viewdns.net
www.localpercent.com
www.localpercent.com
www.srcenerg.com

Ports 443, 80, and 8080 are used.

MITRE ATT&CK

The MITRE ATT&CK information on this security attack is as follows. MITRE ATT&CK, which stands for Adversarial Tactics, Techniques, and Common Knowledge, incudes classified descriptions of the threat group's tactics and techniques observed. Relevant information can be found on https://attack.mitre.org/.

The MITRE ATT&CK ID corresponding to this threat group quotes from another analysis report and has additional details confirmed by AhnLab.

Tactic	ID	Description
Reconnaissance (TA0043)		
Resource Development (TA0042)		
Initial Access (TA0001)	T1566.001 (Phishing: Spearphishing Attachment)	Attach CHM file
Execution (TA0002)	T1059.005 (Command and Scripting Interpreter: Visual Basic)	
	T1204.002 (User Execution: Malicious File)	
Persistence (TA0003)	T1547.001(Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder)	
Privilege Escalation (TA0004)		

Defense Evasion (TA0005)	T1127 (Trusted Developer Utilities Proxy Execution)	Replace the DLL loaded by a normal program with a tampered one. Scan the number of files in the temporary folder and check processes to determine the analysis environment
	T1497.001 (Virtualization/Sandbox Evasion: System Checks)	
Credential Access (TA0006)		
Discovery (TA0007)		
Lateral Movement (TA0008)		
Collection (TA0009)		
Command and Control (TA0011)	T1041 (Exfiltration Over C2 Channel)	
Exfiltration (TA0010)		
Impact (TA0040)		

Table 6. MITRE ATT&CK

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
Tel : +82 31 722 8000 | Fax : +82 31 722 8901
www.ahnlab.com
www.asec.ahnlab.com/en

About ASEC

AhnLab Security Emergency Response Center(ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. The ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.

AhnLab