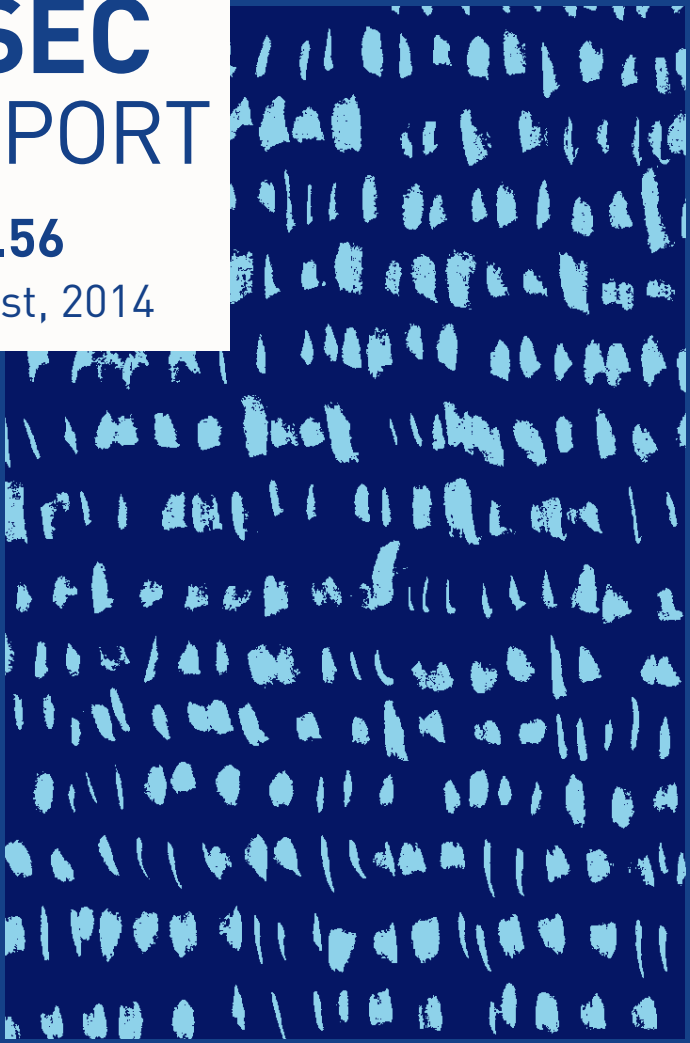
Security Trend

ASEC REPORT

VOL.56

August, 2014



AhnLab

ASEC REPORT

VOL.56 August, 2014

[ASEC (AhnLab Security Emergency Response Center) is a global security response group consisting of virus analysts and security experts. This monthly report is published by ASEC and focuses on the most significant security threats and latest security technologies to guard against such threats. For further details, please visit AhnLab, Inc.'s homepage (www.ahnlab.com).]

SECURITY TREND OF AUGUST 2014

Table of Contents

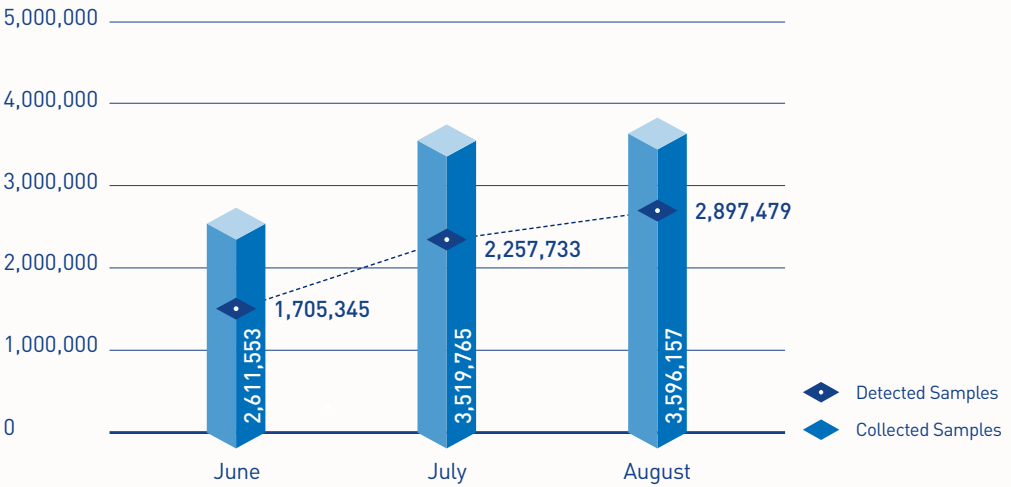
1

SECURITY STATISTICS

SECURITY STATISTICS

01
Malware Statistics

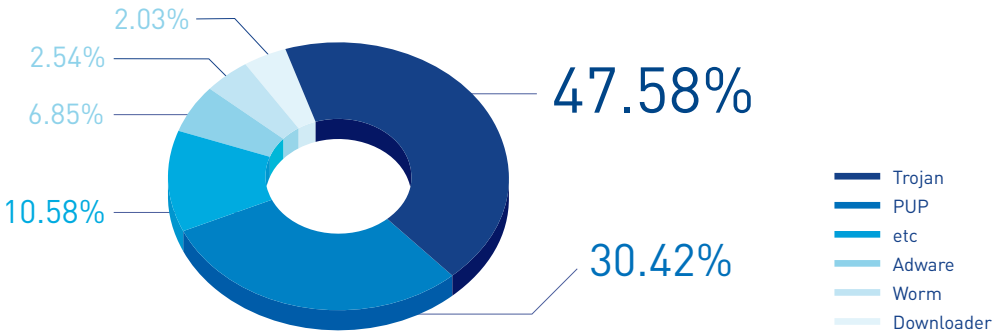
According to the ASEC (AhnLab Security Emergency Response Center), 2,897,479 malware were detected in August 2014. The number of detected malware increased by 639,746 from 2,257,733 detected in the previous month as shown in Figure 1-1. A total of 3,596,157 malware samples were collected in August.



[Figure 1-1] Malware Trend

In Figure 1-1, "Detected Samples" refers to the number of malware detected by AhnLab products deployed by our customers. "Collected Samples" refers to the number of malware samples collected autonomously by AhnLab that were besides our products.

Figure 1-2 shows the prolific types of malware in August 2014. It appears that Trojans were the most distributed malware with 47.58% of the total. It was followed by PUP(30.42%) and Adware (6.85%).



[Figure 1-2] Proportion of Malware Type in August 2014

Table 1-1 shows the Top 10 malware threats in August categorized by malicious code name. Trojan/Win32.ADH was the most frequently detected malware (145,727), followed by Trojan/Win32.OnlineGameHack (116,110).

[Table 1-1] Top 10 Malware Threats in August 2014 (by malicious code name)

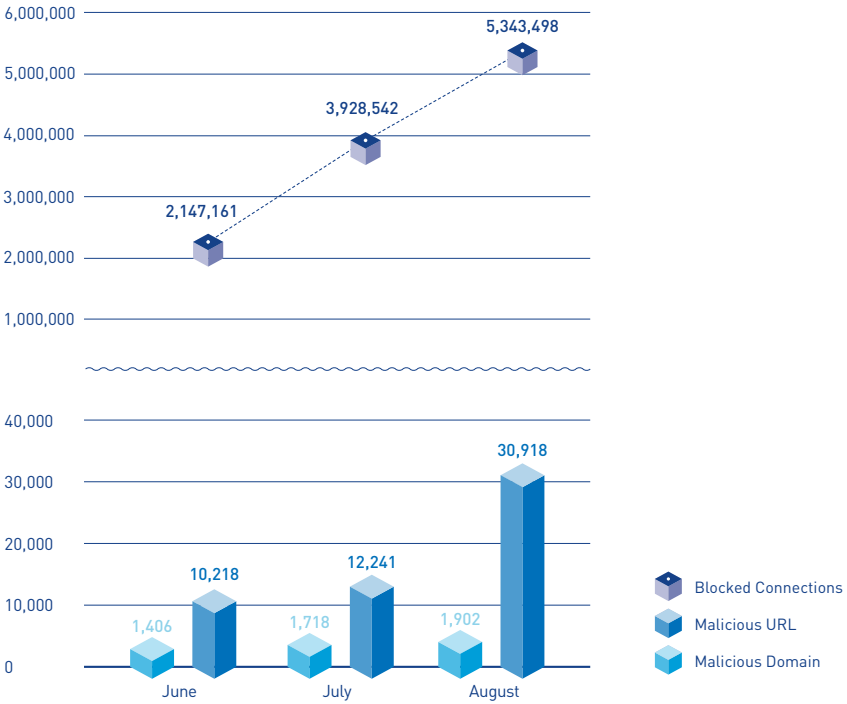
Rank	Malicious code name	No. of detections
1	Trojan/Win32.ADH	145,727
2	Trojan/Win32.OnlineGameHack	116,110
3	Adware/Win32.SwiftBrowse	108,520
4	Adware/Win32.SearchSuite	106,428
5	Trojan/Win32.Gen	100,588
6	Trojan/Win32.Agent	84,520
7	ASD.Prevention	76,275
8	PUP/Win32.IntClient	69,847
9	Trojan/Win32.Generic	61,433
10	Trojan/Win32. Agent	60,958

SECURITY STATISTICS

02

Web Security Statistics

In August 2014, a total of 1,902 domains and 30,918 URLs were comprised and used to distribute malware. In addition, 5,343,498 malicious domains and URLs were blocked. This figure is the number of blocked connections from PCs and other systems to the malicious website by AhnLab products deployed by our customers. Finding a large number of distributing malware via websites indicates that internet users need to be more cautious when accessing websites.

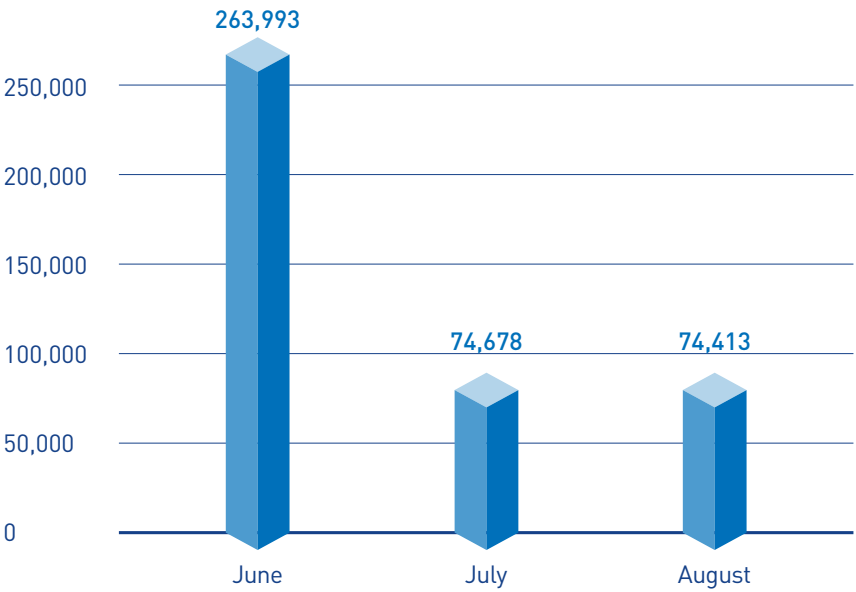


[Figure 1-3] Blocked Malicious Domains/URLs in August 2014

SECURITY STATISTICS

03 Mobile Malware Statistics

In August 2014, 74,413 mobile malware were detected as shown in Figure 1-4.



[Figure 1-4] Mobile Malware Trend

Table 1-2 shows the Top 10 mobile malware in August 2014 categorized by malicious code name. Malicious mobile codes that were installed as an Android application bundle were frequently detected, such as Android-PUP/Dowgin.

[Table 1-2] Top 10 Mobile Malware Threats in August (by malicious code name)

Rank	Malicious code name	No. of detections
1	Android-PUP/Dowgin	17,160
2	Android-Trojan/FakeInst	15,253
3	Android-Trojan/Opfake	3,889
4	Android-PUP /SMSReg	3,419
5	Android-PUP/ Wapsx	2,408
6	Android-Trojan/ SMSAgent	1,875
7	Android-PUP/ Youmi	1,783
8	Android-Trojan/SMSSend	1,694
9	Android-Trojan/Mseg	1,175
10	Android-PUP/SMSPay	1,078

2

SECURITY ISSUE

SECURITY ISSUE

01

User's PC Information Sent to Statistical Websites by Malware

Recently, a new malware that targets users' PC information has been discovered. The malware collects a user's PC information and sends it to a statistical website which shows information on infected PCs and also disables the anti-virus program on the PC. Information sent to statistical websites includes the IP address, country, infection date, OS, and security software of the infected PC as shown in Figure 2-1.

Figure 2-1 | Statistical website showing infected PC information

The files shown in Table 2-1 are generated when the malware is executed.

Table 2-1 | Generated files

C:\WINDOWS\system32\6to432.dll
C:\WINDOWS\system32\102A (3-4 digits + 1 alphabet).tmp
C:\WINDOWS\system32\102B (3-4 digits + 1 alphabet).tmp
C:\WINDOWS\system32\6to432
C:\WINDOWS\system32\Vag.tbl
C:\WINDOWS\system32\apci.sep
C:\WINDOWS\system32\ias\sysprtj.prd

It then registers the generated files "6to432.dll" and "Vag.tbl" in Services as below:

HKLM\SYSTEM\ControlSet001\Services\6to4\ImagePath
"%SystemRoot%\System32\svchost.exe -k netsvcs"

HKLM\SYSTEM\ControlSet001\Services\6to4\Start
0x2 – Auto Load

HKLM\SYSTEM\ControlSet001\Services\6to4\Parameters\ServiceDll
"C:\WINDOWS\system32\6to432.dll"

HKLM\SYSTEM\ControlSet001\Services\6to4\Start
0x2

HKLM\SYSTEM\ControlSet001\Services\net81390\ImagePath
"\??\C:\WINDOWS\system32\Vag.tbl"

HKLM\SYSTEM\ControlSet001\Services\net81390\Start
0x2

Also, a DLL file is loaded with the process and executed. Figure 2-2 shows that the DLL file is loaded on "svchost.exe." Once loaded, the DLL file accesses a specific website and generates other files.

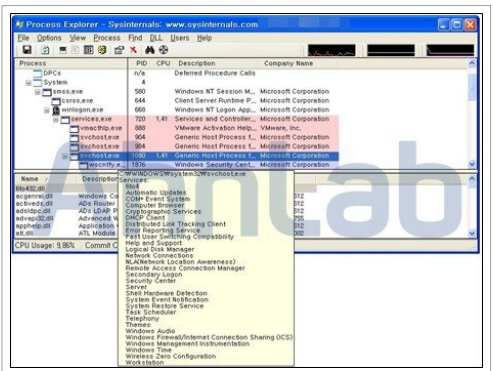


Figure 2-2 | 6to432.DLL loaded on svchost.exe

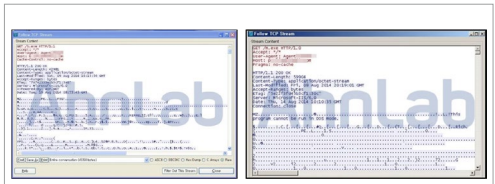


Figure 2-3 | Downloaded files from a specific website (s "_ b.exe", the left and "m.exe", the right)

The generated files, which are102A.tmp and 102B.tmp, and the downloaded files, which are m.exe and b.exe, are shown in Figure 2-4.

Figure 2-4 | "_b.exe"(left) and "102A.tmp" (right) downloaded from a specific website

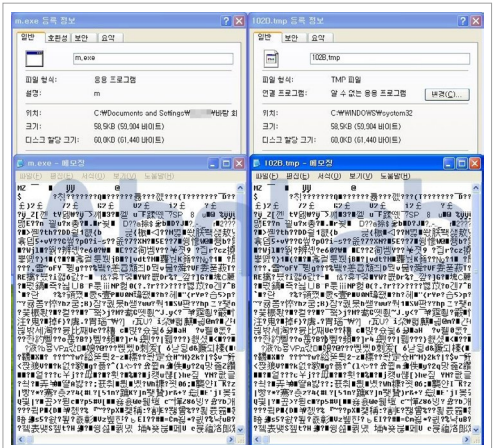


Figure 2-5 | "_m.exe" (left) and "102B.tmp" (right) downloaded from a specific website

As shown in Figure 2-6, "102B.tmp" creates a file, "Vag.tbl" that is then used to steal the user's PC information.

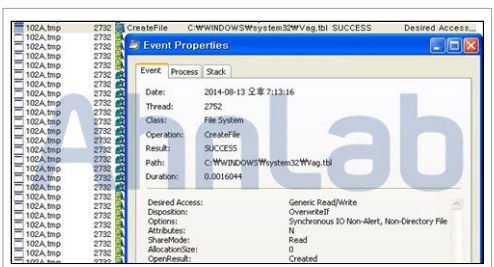


Figure 2-6 | A file created for stealing the user's PC information

"Vag.tbl" with its extension "tbl" is actually a system driver file as its PE (Portable Executable) header indicates. The file type (driver / GUI / CUI) can be confirmed with the subsystem value in the optional header.

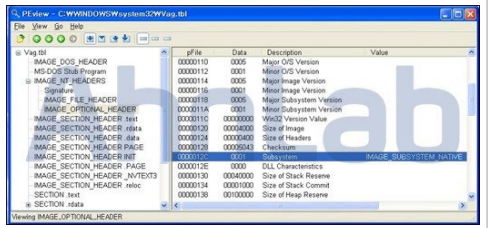


Figure 2-7 | File type of "Vag.tbl"

As shown in Figure 2-8, Vag.tbl is registered in Services, and executes for "hooking" information on the infected PC. "Hooking" refers to commands, methods, technologies, and actions that switch or steal function calls, messages, and events generated between software components of various PC programs (operating systems, applications, etc). It is also used to steal PC memory information and keyboard input information from target PCs.

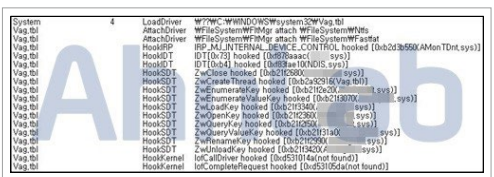


Figure 2-8 | Hooking progress

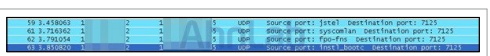


Figure 2-9 | Sending the collected information via UDP

Information stolen from an infected PC is sent to a statistical website via UDP (User Datagram Protocol) as shown in Figure

2-9. The stolen information is likely to be used for additional attacks such as distributing malware.

V3, AhnLab's anti-malware product, detects the relevant malware as follows.

<Malicious code name in V3 products>

Trojan/Win32.OnlineGameHack (2014.08.12.00)
Backdoor/Win32.Trojan (2014.08.14.00)
Trojan/Win32.Hooker (2014.08.02.01)
Trojan/Win32.Agent (2014.08.13.00)

SECURITY ISSUE

02

Normal System Files Tampered by Online Game Hack

Online Game Hacks are designed to steal online game user accounts for financial gain. Most online game providers have a security module or anti-virus program in place to prevent theft of their user accounts. Malware creators, however, continuously develop various techniques to render specific security related services ineffective or to evade detection by an anti-virus program.

The online game hack discovered in August also interferes with anti-virus programs and disguises itself as normal file by altering a Windows system file.

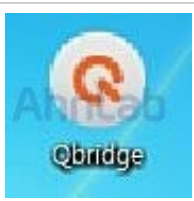


Figure 2-10 | Icon of disguised file

When the malware is executed, it creates additional malware as shown in Figure 2-11; this malware is used to steal user accounts and interfere with anti-virus programs.

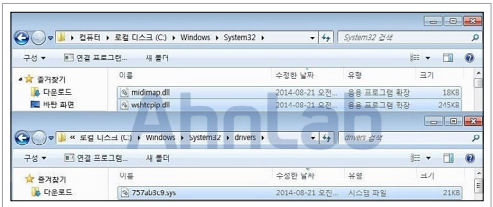


Figure 2-11 | Additionally generated malware

Figure 2-12 shows [random string].sys, generated in C:\Windows\System32\drivers and registered in the registry, to be executed automatically as a service when booting. At the same time, it interferes with the driver loading to disable the anti-virus program. Preventing the anti-virus program from being disabled requires deleting the corresponding malware manually

or repairing the infected PC with the relevant virus removal program.

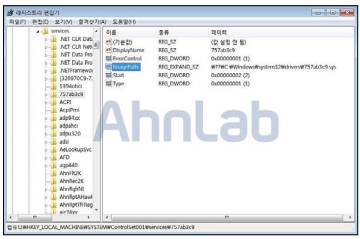


Figure 2-12 | Malware registered in Services

"wshtcpip.dll", which is generated by malware, appears to be a normal Windows system file, but it is a malicious file which is altered by patching the normal system file. The Properties information of those files is different from each other. The malicious file gets loaded during a normal process and attempts to steal online game user accounts as shown in Figure 2-13.

Figure 2-13 | Stolen user account information

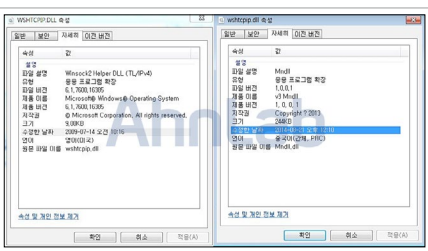


Figure 2-14 | Normal "wshtcpip.dll" (left) and altered "wshtcpip.dll" (right)

However, the malicious file is still a Windows system file. When deleting the file, therefore, it may make internet access unavailable or result in the Blue Screen of Death (BSOD). In order to alter "wshtcpip.dll," "Qbridge.exe" duplicates "wshtcpip.dll" into C:\Windows\System32 as "ws2tcpip.dll". "ws2tcpip.dll" is then used to generate "wshtcpip.dll," which is the malicious file by patching a normal file. The patched malicious file duplicates the normal file's functions to prevent errors caused by system file altering.

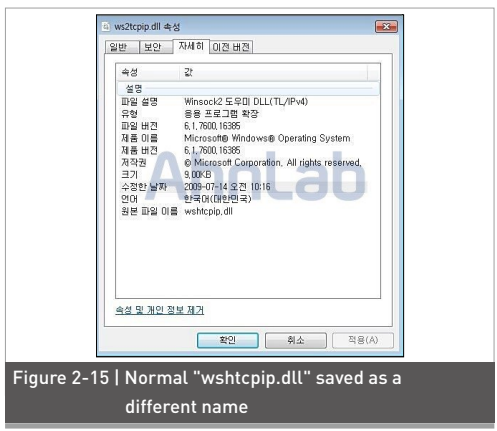


Figure 2-15 | Normal "wshtcpip.dll" saved as a different name

AhnLab provides an exclusive virus removal program via its website for relevant online game hacks that protects and prevents users from being infected by the relevant malware and its variants. When the relevant virus removal program is not available, you

can remove the malware manually by changing the malicious file with a normal file. The information detail of the DLL files required by applications are saved in the C:\Windows\winsxs folder as another file, and applications select and use a necessary DLL file from the folder. There are multiple versions of the DLL file, and different programs require different versions. Thus, the folder includes these different DLL file versions for compatibility. In order to manage the DLL files manually, you need to copy "wshtcpip.dll" and "midmap.dll" from "winsxs" folder and paste them into their original path (C:\Windows\System32).

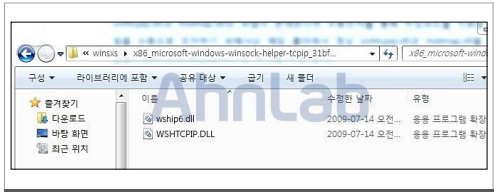


Figure 2-16 | "wshtcpip.dll" located in "winsxs" folder

The stolen online game user accounts can cause monetary loss, so it is recommended that users be more cautious.

V3 detects the relevant malware as follows.

<Malicious code name in V3 products>

Win-Trojan/Onlinegamehack (2014.08.20.00)
Win-Trojan/Onlinegames (2014.08.20.00)
Win-Trojan/Onlinegamehack (2014.08.22.00)
Trojan/Win32.Agent (2014.08.17.00)

3

ANALYSIS IN-DEPTH

Distribution of Malware through Altering PUPs

ANALYSIS IN-DEPTH

Distribution of Malware through Altering PUPs

In order to launch attacks successfully, attackers keeps developing new tactics. Altering normal applications is one of the most prevalent tactics. This report presents a case that uses the altering application method with PUP (Potentially Unwanted Programs).

PUP (Potentially Unwanted Program)

PUP (Potentially Unwanted Program), or PUA (Potentially Unwanted Application), refers to applications that would be considered unwanted despite often having been downloaded by the user, possibly after failing to read a download agreement. PUPs include spyware, adware, fraudulent dialers. Many virus checkers classify unauthorized key generators as grayware, although they frequently carry true malware in addition to their ostensible purpose.

* Source: Wikipedia

A PUP is often disguised as a normal program and distributed via blogs and online user communities as open-source program bundles. One method to use PUPs to distribute malware has been used widely and for a long period of time: attacking a PUP update server and altering the PUP update file into a malicious file to infect PCs when a PUP installed on a PC downloads and executes the PUP update file. The notorious memory-hacking malware that targeted the financial sector in South Korea in 2013 also spread to PCs via altered PUPs, and caused severe monetary losses and financial information leakage.

It is effective to use PUP for distribution of malware because most users tend not to check the Terms of Use associated with the download and installation of programs via various paths. Therefore, multiple PUPs are installed on a PC and cause malware infection when one of the installed PUPs download its update file.

The case discovered in August occurred in this manner. A large number of PCs in South Korea were infected by a single malware. The malware analysts at ASEC collected the relevant data and discovered that the same PUP was installed and executed in all the infected PCs.

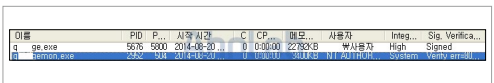


Figure 3-1 | Process information of the corresponding PUP

When "q****ge.exe" was executed, it communicated with the update server regularly and acquired version information as shown in Figure 3-2. If the PUP installed on the user PC was not the latest version, it downloaded the latest version from the update server.

Figure 3-2 | Communication record of PUP

This downloaded version included malicious codes. As you can see the file structure of the corresponding PUP as shown in Figure 3-3, PUP and malicious codes are combined in one file. The part of PUP and malicious codes are marked as Figure 3-3.

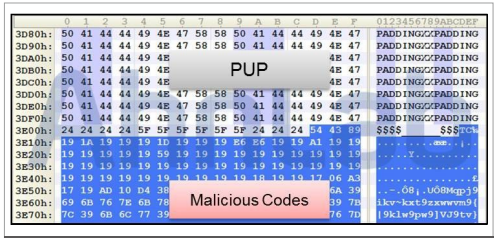


Figure 3-3 | Bundled PUP file and malicious codes

The part containing malicious codes is encrypted. The encrypted part, which consists of malicious codes, is converted into an executable file by decryption code as shown in Figure 3-4. When "q****ge.exe", the relevant PUP, is executed, it generates and executes malware in %TEMP% through decryption.

Figure 3-4 | Decrypted codes

The malware generated in %TEMP% deletes internet access history and registry records in order to hide the infection/distribution path.

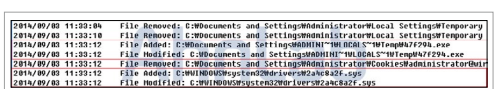


Figure 3-5 | Deleted records

In addition, the malware has a function to delete its traces when executing, and it is difficult to collect download records of the malware.

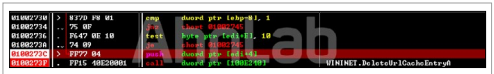


Figure 3-6 | Delete function of the malware

Figure 3-7 shows the strings contained in other malware that are generated when the malware in %TEMP% is executed. This pattern is very similar with the memory hacking attack that used JavaScript to steal the financial information of online banking users in South Korea last year. The difference between those cases is that the purpose of previous attacks was to steal users' financial information. However, since most banks in South Korea have enhanced their security measures, it has become difficult to steal financial information. In this perspective, the attackers seem to have switched their target to online game users to steal account information with a similar method.

Figure 3-7 | JavaScript extracting account information

Also, the malware attempts to connect to specific websites whenever Internet Explorer starts, and to download variants as shown in Figure 3-8 and Figure 3-9.

Figure 3-8 | Downloading variants

c****t.q*****e.c*.*r : 2**.1*1.3.*6

n**.ou***b.c*m : 2**.1**.2*.1*0

Figure 3-9 | Network connection information

V3 detects the relevant malware as follows:

<Malicious code name in V3 products>

Trojan/Win32.Agent (2014.08.17.00)

Trojan/Win32.Banki (2014.08.18.03)

AhnLab

ASEC REPORT

VOL.56
August, 2014

Contributors	**ASEC Researchers**	Publisher	**AhnLab, Inc.**
Editor	**Content Creatives Team**	Website	**www.ahnlab.com**
Design	**UX Design Team**	Email	**global.info@ahnlab.com**

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

©AhnLab, Inc. All rights reserved.