ASEC REPORT

VOL.42 | 2013.06

AhnLab

CONTENTS

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 it focuses on the most significant security threats and the latest security technologies to guard against these threats. For further information about this report, please refer to AhnLab, Inc.'s homepage (www.ahnlab.com).

Malicious Code Trends

01. Malicious Code Statistics

The number of malicious codes reported in June decreased by 1,030,000 from May

Statistics collected by the ASEC show that 4,138,029 malicious codes were reported in June 2013. The number of reports decreased by 1,032,964 from the 5,170,993 reported in the previous month. (See [Figure 1-1]) The most frequently reported malicious code was ASD.PREVENTION, followed by Win-Trojan/Wgames.Gen and Textimage/Autorun. A total of 3 malicious codes were added to the "Top 20" list. (See [Table 1-1].)

Figure 1-1 | Monthly Malicious Code Report Changes

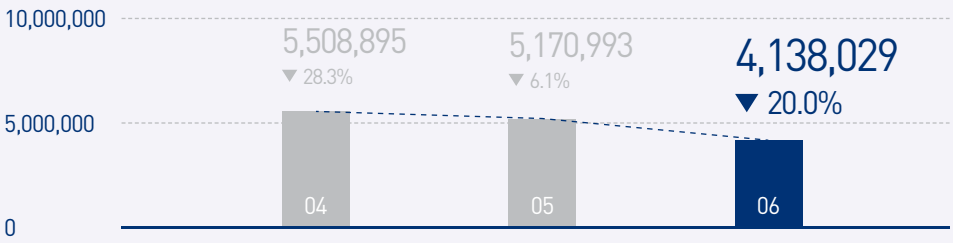


Table 1-1 | June 2013 Top 20 Malicious Code Reports (By Report and Malicious Code)

Ranking	↑↓	Malicious Code	Reports	Percentage
1	▲1	ASD.PREVENTION	249,187	16.1%
2	▼1	Win-Trojan/Wgames.Gen	149,197	9.6%
3	▲1	Textimage/Autorun	132,316	8.6%
4	▲3	Win-Trojan/Onlinegamehack140.Gen	101,122	6.5%
5	▲1	Trojan/Win32.onlinegamehack	95,433	6.2%
6	▲2	Trojan/Win32.urelas	87,625	5.7%
7	NEW	Win-Trojan/Agent.206512	83,179	5.4%
8	▲1	Trojan/Win32.agent	82,965	5.4%
9	▲2	Als/Bursted	64,939	4.2%
10	▲2	RIPPER	64,909	4.2%
11	▲3	BinImage/Host	59,255	3.8%
12	▼9	Win-Trojan/Asd.variant	52,682	3.4%
13	▼8	Malware/Win32.generic	52,508	3.4%
14	NEW	Win-Trojan/Malpacked5.Gen	47,869	3.1%
15	—	Malware/Win32.suspicious	43,744	2.8%
16	▲1	Win32/Autorun.worm.307200.F	41,664	2.7%
17	▼1	Win-Trojan/Avkiller4.Gen	41,408	2.7%
18	▲2	Win32/Virut.f	33,279	2.2%
19	NEW	Trojan/Win32.adh	33,042	2.1%
20	▼2	Trojan/Win32.Gen	30,883	1.9%
		TOTAL	1,547,206	100.0 %

Top 20 Malicious Code Reports

[Table 1-2] shows the percentage breakdown of the Top 20 malicious code variants reported this month. In June 2013, Trojan/Win32 (579,543 reports) was the most frequently reported malicious code among the Top 20 malicious code variants, followed by Win-Trojan/Agent (279,946 reports) and ASD (249,187 reports).

Table 1-2 | Top 20 Malicious Codes

Ranking	↑↓	Malicious Code	Reports	Percentage
1	—	Trojan/Win32	579,543	22.2%
2	—	Win-Trojan/Agent	279,946	10.7%
3	▲3	ASD	249,187	9.5%
4	▼1	Win-Trojan/Onlinegamehack	165,574	6.3%
5	▼1	Win-Trojan/Wgames	149,197	5.7%
6	▲4	Textimage/Autorun	132,346	5.1%
7	▲2	Malware/Win32	105,638	4.0%
8	▼3	Win-Trojan/Downloader	103,737	4.0%
9	▲2	Win-Trojan/Onlinegamehack140	101,122	3.9%
10	▼2	Adware/Win32	97,341	3.7%
11	▲1	Win32/Virut	82,498	3.2%
12	▲1	Win32/Conficker	79,639	3.1%
13	▲1	Win32/Autorun.worm	78,834	3.0%
14	▲1	Als/Bursted	64,939	2.5%
15	▲1	RIPPER	64,909	2.5%
16	▲2	Win32/Kido	60,015	2.3%
17	▲3	BinImage/Host	59,255	2.3%
18	▼1	Downloader/Win32	55,557	2.1%
19	▼12	Win-Trojan/Asd	52,682	2.0%
20	NEW	Win-Trojan/Malpacked5	47,869	1.9%
		TOTAL	2,609,828	100.0 %

Trojan Horse – The most frequently reported new malicious code in June

[Table 1-3] shows the percentage breakdown of the Top 20 new malicious codes reported in June. Win-Trojan/Agent.206512 was the most frequently reported new malicious code, representing 68.3% (83,179 reports) of the Top 20 new malicious codes in June, followed by Win-Trojan/Urelas.451584 (11,576 reports).

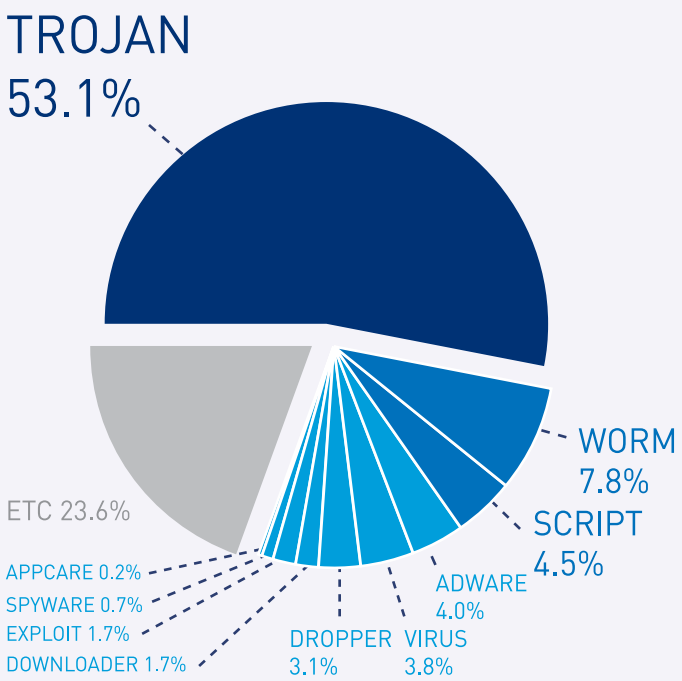
Table 1-3 | Top 20 New Malicious Code Reports

Ranking	Malicious Code	Reports	Percentage
1	Win-Trojan/Agent.206512	83,179	68.3%
2	Win-Trojan/Urelas.451584	11,576	9.5%
3	Win-Trojan/Agent.540672.NH	8,387	6.9%
4	Win-Adware/KorAd.98304.F	1,912	1.6%
5	Win-Trojan/Agent.907811	1,837	1.5%
6	Win-Trojan/Qhost.83072	1,804	1.5%
7	Win-Trojan/Agent.846330	1,648	1.4%
8	Java/Gondad	1,258	1.0%
9	Win-Trojan/Small.550912	1,177	1.0%
10	Win-Trojan/Agent.1155072.P	1,059	0.9%
11	Win-Spyware/OnlineGameHack.348160	1,034	0.8%
12	JS/Expoit	987	0.8%
13	Win-Adware/KorAd.187075	944	0.8%
14	S/Exploit	919	0.8%
15	Win-Trojan/Agent.596480.P	879	0.7%
16	Win-Trojan/Downloader.911872.B	784	0.6%
17	JAVA/Cve-2011-2544	730	0.6%
18	Win-Trojan/Agent.675840.BX	642	0.5%
19	Win-Trojan/Qhost.22016.V	611	0.5%
20	Dropper/Expjava	498	0.3%
	TOTAL	121,865	100.0 %

Trojan Horse Ranked as the Most Reported Malicious Code in June

[Figure 1-2] categorizes the top malicious code types reported by AhnLab customers in June 2013. Trojan was the most reported malicious code type, representing 53.1% of the top reported malicious code types, followed by Worm (7.8%) and Script (4.5%).

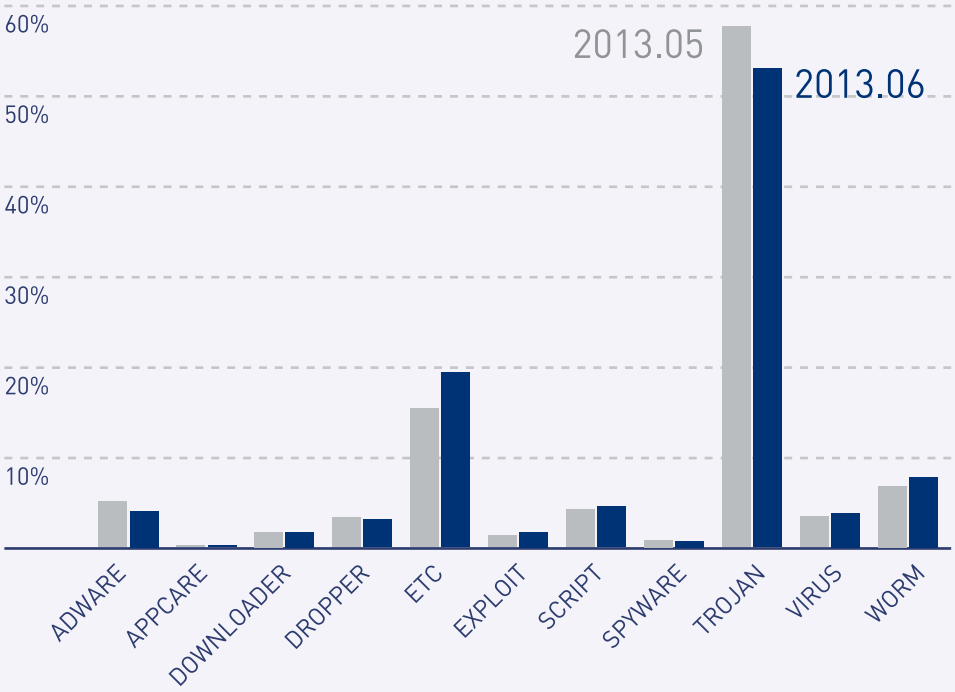
Figure 1-2 | Malicious Code Type Breakdown



Comparison of Malicious Codes with Previous Month

[Figure 1-3] shows the malicious code breakdown compared to the previous month. Compared to the last month, the number of Worms, Scripts, Viruses, and Exploits increased, whereas the number of Trojan horses, Adware, Droppers, and Spyware decreased. The numbers for Downloaders and Appcare was similar to that of the previous month.

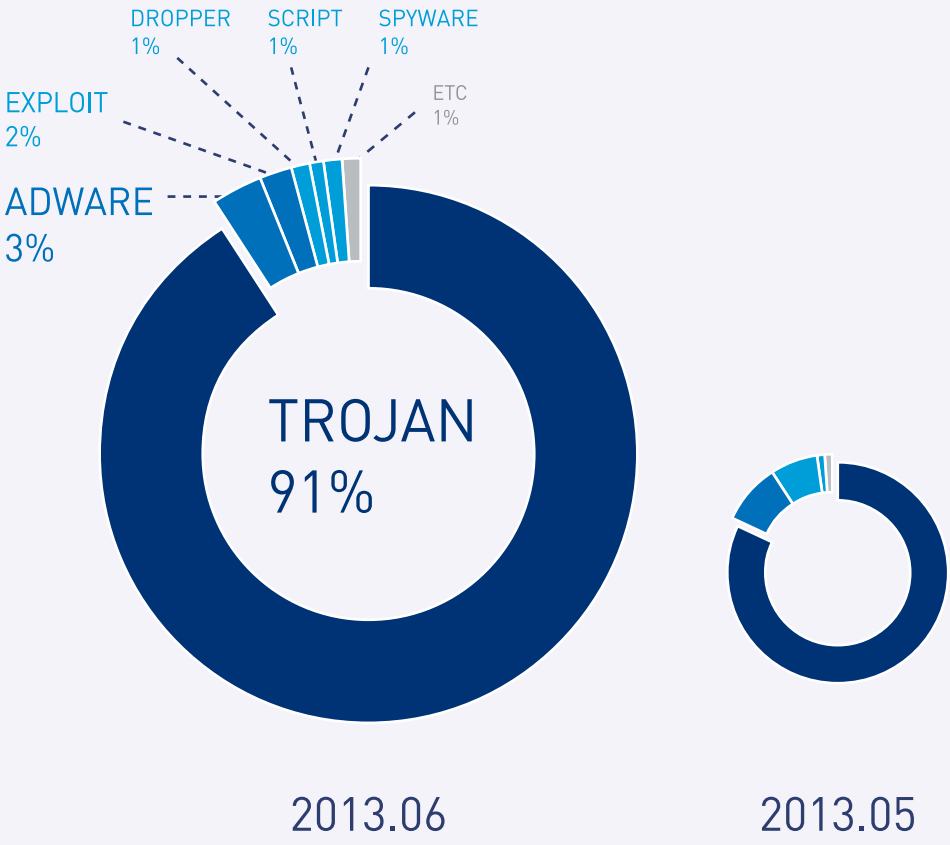
Figure 1-3 | Primary Malicious Code Type Breakdown for June VS. May



Breakdown of New Malicious Code Types

Trojan Horse was the most frequently reported new malicious code type in June, representing 91% of the new malicious code types, followed by Adware (3%) and Exploit (2%).

Figure 1-4 | Breakdown of New Malicious Code Types



Malicious Code Trends

02. Malicious Code Issues

Malicious codes spread from the shipment status checking page of a postal and logistics site

Malicious codes have been continuously distributed through various websites such as file sharing sites (P2P), news sites, game item exchange sites, and torrents. Malicious codesdistributed from the shipment status checking page of a frequently-visited postal and logistics sitehave recently been reported. Currently, the inserted malicious script has been removed.

When you visit the shipment status page to check your shipment process details, the iframe is loaded to infect the system through a vulnerability exploitation.

Figure 1-10 | iframe inserted to the bottom of the Java script

The internal codes of the page are obfuscated with the Gongda pack toolkit.

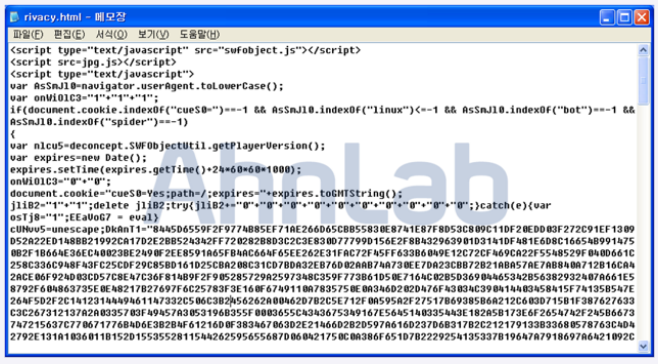


Figure 1-11 | Malicious HTML file (rivacy.html)

The de-obfuscated script reveals the Java vulnerability (CVE-2011-3544) file and malicious code distribution URL.

The system infected with the malicious code (nate.exe) attempts to connect to a specific server (118.***.***.36), and the following information can be verified in the internal strings.

Figure 1-12 | Decoding the obfuscated script (rivacy.html)

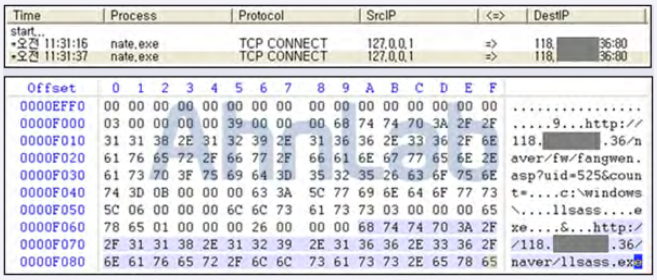


Figure 1-13 | Internal strings of the nate.exe

The downloaded malicious code (llsass.exe) is registered as a scheduled job to execute automatically every hour.

This malicious code (llsass.exe) works as a backdoor in attempts to connect to a specific server (126.**.**.40:1000).

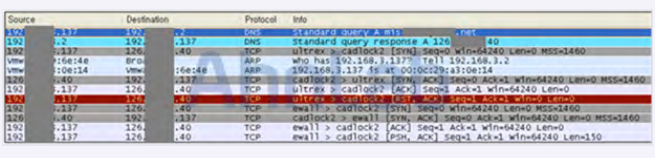


Figure 1-15 | llsass.exe network connection information

This malicious code can be found and repaired with a V3 product.

<Malware name in V3 products>

-Java/Cve-2011-3544 (2013.05.30.00)

-Downloader/Win32.Agent (2013.05.30.00)

-Trojan/Win32.Agent (2013.05.30.00)

Malicious code distributed via a torrent site creates a hosts.ics file

Recently, the malicious code that creates hosts.ics files is distributed via a torrent file sharing site. As large numbers of users frequently visit this site, users are advised to take extra caution.

This pharming malware, which is designed to steal banking information, modifies the hosts file or creates a hosts.ics file to connect to the fake scam site – even if users enter normal site addresses.

When users visit the malicious website, the iframe that is inserted in the common.js file is loaded to infect the system through a vulnerability exploitation.

Figure 1-17 | iframe inserted in the Java script file

The internal codes of the page are obfuscated with the Gongda pack toolkit.

Figure 1-18 | Malicious HTML file

The de-obfuscated codes show the Java vulnerability-related codes and malicious code distribution URLs.

Figure 1-19 | De-obfuscation

If the system is infected with the malware (server.exe), the hosts.ics file is created as shown in [Figure 1-20].

Figure 1-20 | hosts.ics file

The malware assigns the hostis.ics file with the highest priority to direct users to a fake pharming site, even if users enter the legitimate online banking site addresses.

Figure 1-21 | hosts.ics file information

V3 can detect this malware as follows.

<Malware name in V3 products>
-Worm/Win32.Allaple (2013.06.17.05)
-Trojan/Win32.Hosts (2013.06.17.00)
-Trojan/Win32.Jorik (2013.06.19.00)
-JS/Agent (2013.06.25.00)

Malware spread via latest movie sharing files

Currently many people share and download movies, games and utility programs via file sharing sites (P2P) or torrent programs. Sharing files in this way might encourage unintentional copyright violations. These files sometimes contain malicious codes from uncertain file sources. Therefore, users need to exercise extra special caution.

Malicious code disguised as a torrent file of the latest movie has been reported. The malicious file appears to have a movie torrent file (.torrent) icon, but the malicious code is actually hidden inside the file.

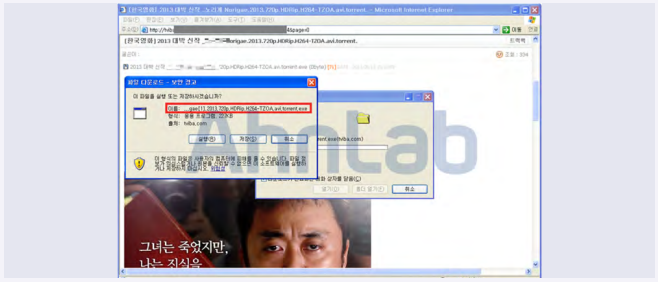


Figure 1-12 | Torrent site

This malware is designed with Nullsoft, containing a torrent sharing file and a malicious code (Activex.exe).

Similar malicious codes disguised as various movie torrent files continue spreading via file sharing sites. When the system is infected, the following files are created.

C:\Activex.exe
C:\Program Files\Microsoft Window Update\lsass.exe

The created file (lsass.exe) is registered in the system start registry to be executed.

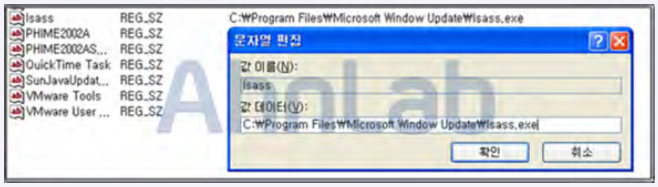


Figure 1-25 | Register in the system start registry

After malware infection, the functioning lsass.exe process continuously attempts to connect to a specific server (121.***.***.146:4183) as shown in [Figure 1-26]. At the time of ASEC analysis, we could not connect to the server.

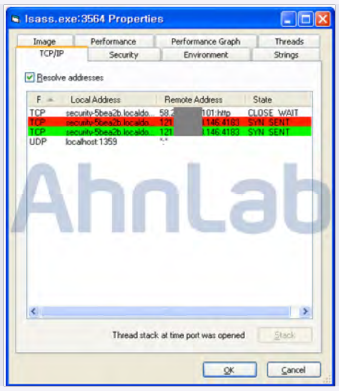


Figure 1-26 | lsass.exe process

Since user systems can be infected with illegally downloaded movies, broadcasted materials, paid programs from file sharing sites (P2P), or malware disguised as torrent files, users need to exercise special caution.

V3 can detect this malware as follows.

<Malware name in V3 products>
-Trojan/Win32.Scar (2013.05.29.03)

Malware with various DDoS attack functions

Recently, it was reported that a DDoS attacker overloaded a victim's computer by constantly sending ICMP packets to the specific IP bandwidth. The ICMP Flood attack was executed through the victim's computer to target the Amazon IP bandwidth located in the U.S. According to ASEC analysis results on several victims' computers that created excessive ICMP packets, these computers were commonly running the P2P download program from Company A as shown in [Figure 1-27].

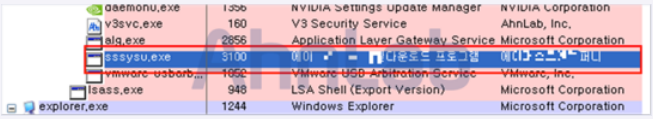


Figure 1-27 | P2P download program in the running process

As the properties of the sssysu.exe file in [Figure 1-27] are the same as the properties of the actual P2P download program, users can be easily tricked into believing it to be a normal file. The P2P download program files with the same properties under different random names are executed in several systems that were attacked with the excessive ICMP packet flooding.

At the time of ASEC analysis, we cannot verify whether the P2P download program from Company A actually downloads DDoS attack-related malware because the P2P program was already modified. The malicious P2P download program, however, attempts to connect to the same domain (death***.hopto.org) as the one to which the DDoS attack malware connects. As a result, it is assumed that the modified version of Company A's P2P download program is related to the DDoS attack malware.

No file is linked to the "File distribution" link, but the attackers can distribute malicious codes through similar methods in the future. Users need to pay extra caution. The link attempts to connect to hopto.org which provides a free Dynamic DNS service and we assume that the malware creator uses this domain to change C&C server IP more easily. The death***.hopto.org domain uses the IP (211.***.**.242) located in Korea.

The modified P2P download program file periodically connects to the following server (presumably a C&C server) upon execution. It snatches the computer name, OS, memory, CPU and other information from the victim's computers.

hxxps://deat****.hopto.org
http://DDoS.j*****.in:2222
http://DDoS.j*****.in:1111

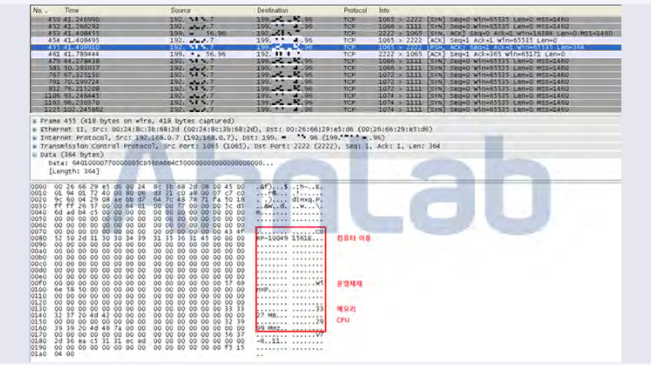


Figure 1-29 | Packet contents of stolen system information

The DDoS attack malware is downloaded from hxxp://roc*****.com/u.exe. The following files are created in the compromised system and register themselves in the system registry to be automatically executed upon system restart.

[File creation]
%Systemroot%\System32\nrvunrqfey.exe
└%Systemroot%\System32\yxurqreekf.exe
└%Temp%\svchest.exe

[Registry Registration]
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aspnet_states
"ImagePath"="%Temp%\svchest.exe"

The DDoS traffic is not verified because the last installed svchest.exe file cannot be connected to the hxxps://death***.hopto.org

domain. After analyzing the memory dump of the processes, we verified that the strings in [Figure 1-30] are included. It is assumed that various DDoS attacks are carried out through C&C server commands.

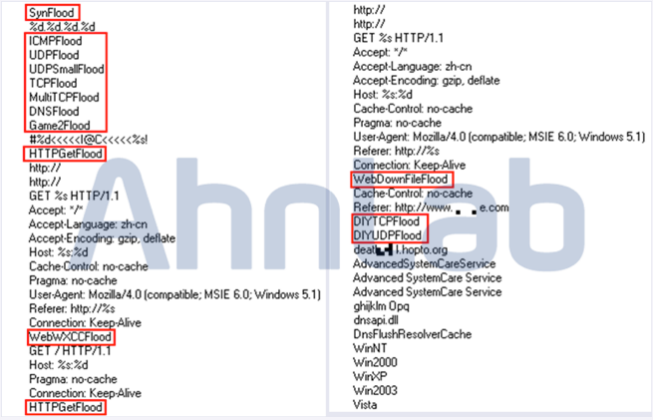


Figure 1-30 | svchest.exe process memory dump

V3 can detect this malware as follows.

<Malware name in V3 products>

-Packed/Win32.Morphine (2013.06.13.01)

-Trojan/Win32.Symmi (2013.06.13.00)

-Packed/Win32.Morphine (2013.06.12.03)

Fraudulent spam e-mails disguised as electronic account statements

Various spam e-mails that claim to be from legitimate banks have been circulated. Although these spam e-mails are not legitimate bank e-mails, the subject and body messages of the spam e-mails are exactly the same as those sent from specific bank e-mails, except for the bank's name. Spam e-mails, claiming to be from the Royal Bank of Scotland (RBS) bank in the United Kingdom or the City Bank in U.S. have been also circulated. Apart from the spam e-mails mentioned above, we assume many kinds of spam e-mails might be circulated by disguising themselves as legitimate bank e-mails.

• Sender
XXXXXXvaluation@citi.com
rbsXXX@rbs.com
Mail subject
(SECURE) Electronic Account Statement (Random number)_(Random number)
Mail body
You have received a Secure PDF message from the CitiSecure (the RBS Bankline) Messaging Server. Open the PDF file attached to this notification.
...[Leave out details] ...
Help is available 24 hours a day by calling 1-866-535-2504 or 1-904-954-6181 or by e-mail at secure.emailhelp@citi.com (secure.emailhelp@rbs.com)
Please note: Adobe Reader version 7 or above is required to view all SecurePDF messages.
• The attachment
Secure.pdf.zip

The fraudulent e-mails lure users into clicking the attached electronic account statement, which is actually a malicious execution file disguised as a normal PDF file. When the attachment is executed, the malicious code is registered in the system registry to be automatically run upon system restart to attempt to connect to a remote system in Seattle (U.S.).

[Created files]
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\3857906.exe
C:\Documents and Settings\Administrator\Application Data\Jife\muziaq.exe

[Registered registry]:
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Muziaq""C:\Documents and Settings\Administrator\Application Data\Jife\muziaq.exe""

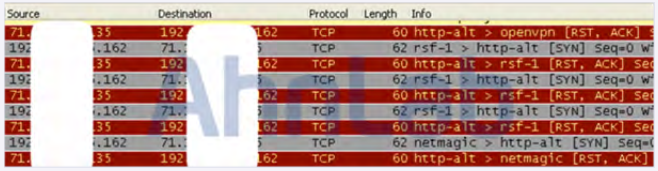


Figure 1-40 | Attempts to connect to remote sites

It tries to connect to the following URLs to download additional malware. At the time of ASEC analysis, some URLs were not connected, but others were successfully connected.

Figure 1-41 | Malicious code download

V3 can detect this malware as follows.

<Malware name in V3 products>

-Trojan/Win32.Tepfer (2013.06.14.02)

Text messages received in e-mail format

The smartphone has become an essential device for information communication in this era of mobile phone communication. Mobile service providers have usually provided customers with a service that sends out text messages in e-mail format so they can be saved in user PCs. Recently, cyber criminals have exploited this service to distribute malicious codes.

The newly discovered spam e-mails disguise themselves as e-mails with text messages as shown in [Figure 1-42]. These spam e-mails pretend to contain text messages from mobile phones to lure users into clicking the attachments.

Figure 1-42 | Fake e-mail pretends to contain text messages

As these fraudulent e-mails have usually been sent from abroad, we expect no Korean users will open the attachment. There might, however, be possibilities of circulating similar spam e-mails, claiming to be from Korea mobile service providers, so users need to pay extra attention.

Generally, the fraudulent spam e-mails lure user into clicking attached files which mostly contain malicious codes. Decompressing the attached file reveals the execution file as shown in [Figure 1-43]. If the Windows Explorer option, "Hide extensions for known file types' is set as default, then the malware is displayed as _7654865S9876Y_.jpeg. Users may mistake this file as a normal image file and open it.

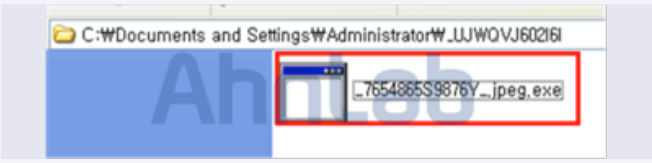


Figure 1-43 | Malicious execution file included in the attachment

When the system is infected, the malware behaves as detailed below.

[File creation]
C:\Documents and Settings\All Users\svchost.exe

[Start program registration]
SunJavaUpdateSched – C:\Documents and Settings\All Users\svchost.exe

In addition, the malware modifies registry values to change firewall policies for the _7654865S9876Y_.jpeg.exe file and registers itself in the authorized program list. As shown in [Figure 1-44], it opens the 3208 port and waits for external connection requests. At the time of ASEC analysis, the IP addresses of the remote site could not be verified.

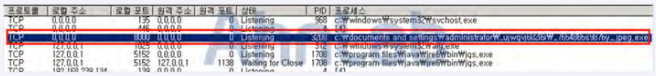


Figure 1-44 | Malware that opens specific ports and waits for connection requests

Clicking the manipulated spam e-mail attachments without verification might cause backdoor malware infection, resulting in serious system infection. Users are advised to exercise increased caution before opening links or attachments in spam e-mails. Before opening attached files, it is wise to scan files with anti-virus programs such as the V3 engine to ensure the safety of the files.

V3 can detect this malware as follows.

<Malware name in V3 products>
-Trojan/Win32.Blocker (2013.06.18.00)

Malicious Code Trends

03. Mobile Malicious Code Issues

Be aware of phishing applications disguised as banking applications

Recently, the number of malicious applications targeting Korean smartphone users has steadily increased, and phishing applications allegedly from legitimate banks have been reported more often. Malicious SMishing applications are designed to make money through mobile phone micropayments, while phishing applications disguised as banking applications are designed to steal both security card numbers and personal banking information, resulting in more severe damage, so extra caution is required.

This newly discovered phishing application is assumed to be distributed through banking-related phishing sites. The malware icon is manipulated to look like a Google Play Store icon at the time of installation.

Figure 1-45 | Application installation icon

During installation, the malware does not request any permissions. As shown in [Figure 1-46], it does not request any user permission to verify the AndroidManifest.xml file.

Figure 1-46 | AndroidManifest.xml file contents

When the Apk file is decompressed, 8 separate apk files exist in the assets folder as shown in [Figure 1-47].

Figure 1-47 | Assets folder upon file decompression

The package structure of the decompressed classes.dex file is shown in [Figure 1-48].

Figure 1-48 | Package information

It is verified that a total of 6 functions are contained in the MainActivity class of the com.google.bankun package designed by the application developers. The rest of the functions except onCreate are designed by application developers, and the behaviors for each function are listed in [Table 1-4].

Function Name	Behavior
onCreate	Initial startup EntryPoint function
installZxingApk	Apk installation function
isAvilible	Banking application installation checking function
chmodApk	Permission change function
getRootAhth	Root permission verification function
uninstallApk	Apk uninstallation function

Table 1-4 | Functions designed by application developers and related behaviors

The above functions check banking application installation and rooting before installing the 1.apk through 8.apk files in the asset folder according to each condition. Based on the analysis result of the 8.apk file, it is verified to be a phishing application disguised as a banking application to lure users into entering user names and account information.

Apart from the 8.apk file, other additionally discovered applications have different bank names but work in the same way. Each application disguises itself as the following bank.

APK	Bank name
1.apk	00 Bank
2.apk	00 Bank
3.apk	00 Bank
4.apk	00 Bank
5.apk	00 Bank
6.apk	0000 Bank
7.apk	00 Bank
8.apk	00000 Bank

Table 1-5 | Applications disguised as banking applications

In addition to the above phishing application, various malicious applications are distributed via SMishing messages in Korea. It is advised that users regularly scan their systems with anti-virus programs like V3 Mobile.

This malicious code can be detected and repaired with V3 Mobile products.

<Malware name in V3 products>

-Android-Trojan/Bankun

Alert! Malicious applications infringing on privacy by collecting text messages

There have been continuous reports about "Malicious applications infringing on privacy" stealing text messages or phone numbers saved in smartphones. The newly discovered malicious application is disguised as a legitimate Google Market application. The package name and resource files are also made to appear like specific Korea anti-virus applications for mobile phones.

Figure 1-51 | Application installation screen

Figure 1-52 | Application package names and resource files

When you run the malicious application, a black screen appears for 10 seconds. During this process, the malicious application collects user information and sends it to a specific server (211.***.***.184) in Taiwan, luring users into adding this application in the device manager.

The following personal information is collected:

- Incoming text message contents and sender information
- User mobile phone number
- User device ID

The malicious application works in the background to send personal information to a specific server whenever text messages are received.

Figure 1-53 | Part of malicious application sources

The V3 Mobile can detect this malicious code as follows.

<Malware name in V3 products>

-Android-Trojan/SMSstealer.8134D

Be aware of Android ransomware

Fake anti-virus programs trick users into paying bills to remove the malware found in mobile devices as well as user PCs. Recently, a ransomware application that requests payment to remove non-existing malicious codes in the fake detection screen has been discovered.

Figure 1-59 | Android ransomware

The malicious applications restricts access to the smartphone by continuously displaying pop-up images (See [Figure 1-59]), and coaxes users into paying for the restriction to be removed, causing huge inconvenience.

This type of malware is called Ransomware because it threatens the user, usually for money or data by taking important user assets hostage.

From last March until recently, the newly discovered Android ransomware disguised as icons in [Figure 1-60] has been distributed. It uses familiar icons for Opera, Firefox, Chrome, Facebook, or operating systems to trick users without arousing suspicion.

Figure 1-60 | Android ransomware icons

By analyzing the malicious application's permissions, we can assume the main behaviors. Presumably, it terminates SMS, network, background processes, and accesses user contact information, which is designed to be automatically executed upon system restart.

Figure 1-61 | Malicious application permission information

As shown in [Figure 1-62], the permission information can be verified during application installation.

Regardless of user selections (cancel or activation), the application installation is already completed. The malicious application displays fake malware infection information screens (see [Figure 1-64]) to lure users into paying the ransom.

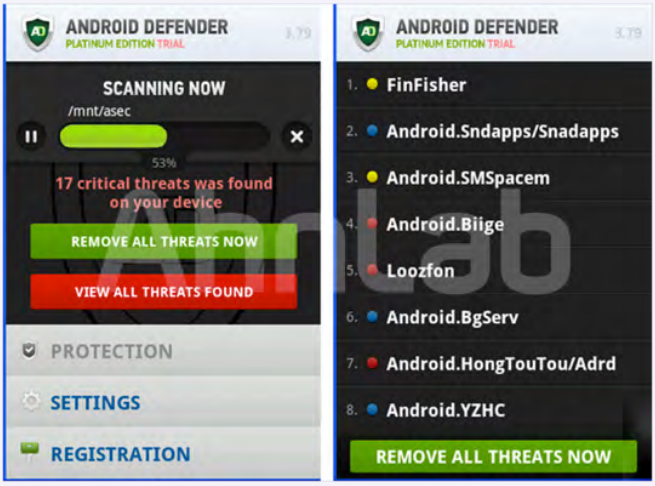


Figure 1-64 | Fake scan screen (Left) / Fake diagnosis screen (Right)

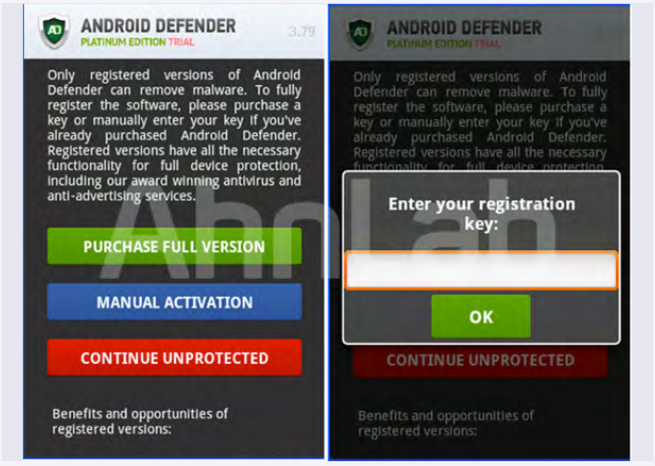


Figure 1-65 | Purchase coaxing screen (Left) / Authorization key input screen (Right)

Even if users move from the application execution screen to the Home screen, all functions are restricted. Performing basic mobile phone functions such as texting and making phone calls are not possible.

As shown in [Figure 1-66], the ransomware displays pop-up messages that recommend removal of malicious codes to lift restriction of user activities. Note the poor grammar of the last sentence. This should also raise a red flag that this may not be legit.

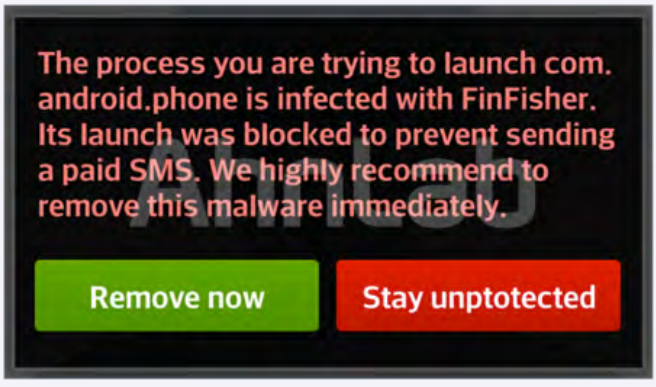


Figure 1-66 | Pop-up message with recommendation to remove fake malicious codes

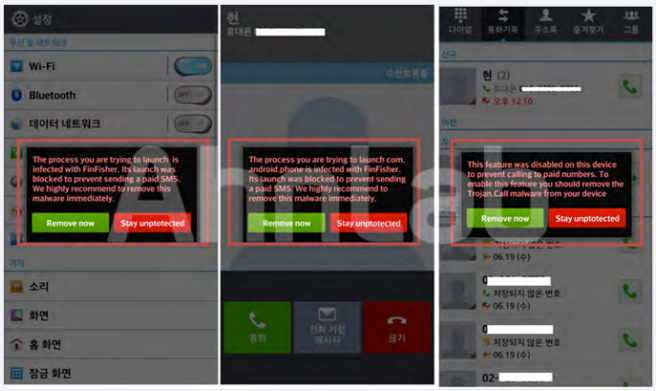


Figure 1-67 | Pop-up message on the recommendation of removing malicious codes

All these malicious activities prevent the user from manually removing the malicious application and performing all other activities.

According to the source code analysis results, the malicious application is designed to stop the device in the event of the following processes.

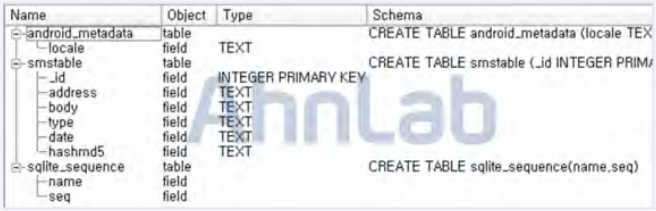
Figure 1-68 | Process termination command code parts

[Process list]
"com.rechild.advancedtaskkiller",
"com.estrongs.android.pop",
"com.metago.astro",
"com.avast.android.mobilesecurity",
"com.estrongs.android.taskmanager",
"com.gau.go.launcherex.gowidget.taskmanagerex",
"com.gau.go.launcherex",
"com.rechild.advancedtaskkillerpro",
"mobi.infolife.taskmanager",
"com.rechild.advancedtaskkillerfroyo",
"com.netqin.aotkiller",
"com.arron.taskManagerFree",
"com.rhythm.hexise.task"

The codes read SMS saved in the smartphone devices and save the stolen SMS in the droidbackup.db.

Figure 1-69 | Code parts reading saved SMS

The droidbackup.db is configured as detailed below.



Name	Object	Type	Schema
android_metadata	table		CREATE TABLE android_metadata (locale TEX
locale	field	TEXT	
smstable	table		CREATE TABLE smstable (_id INTEGER PRIM
_id	field	INTEGER PRIMARY KEY	
address	field	TEXT	
body	field	TEXT	
type	field	TEXT	
date	field	TEXT	
hashmd5	field	TEXT	
sqlite_sequence	table		CREATE TABLE sqlite_sequence(name,seq)
name	field		
seq	field		

Figure 1-70 | droidbackup.db

It might be difficult for general users to remove the installed "ANDROID DEFENDER" ransomware. Consequently, mobile anti-virus products like the V3 mobile program are to be installed immediately to prevent ransomware infection.

This malicious code can be detected and repaired with V3 Mobile products.

<Malware name in V3 products>
-Android-Trojan/FkDefend

Security Trend

01. Security Statistics

Microsoft Security Updates – June 2013

Microsoft issued 5 security updates (1 critical, 4 important) in June 2013. Especially in the case of a critical Microsoft Explorer vulnerability, the attack code is publicly exposed and most likely to be abused, so immediate updates are needed.

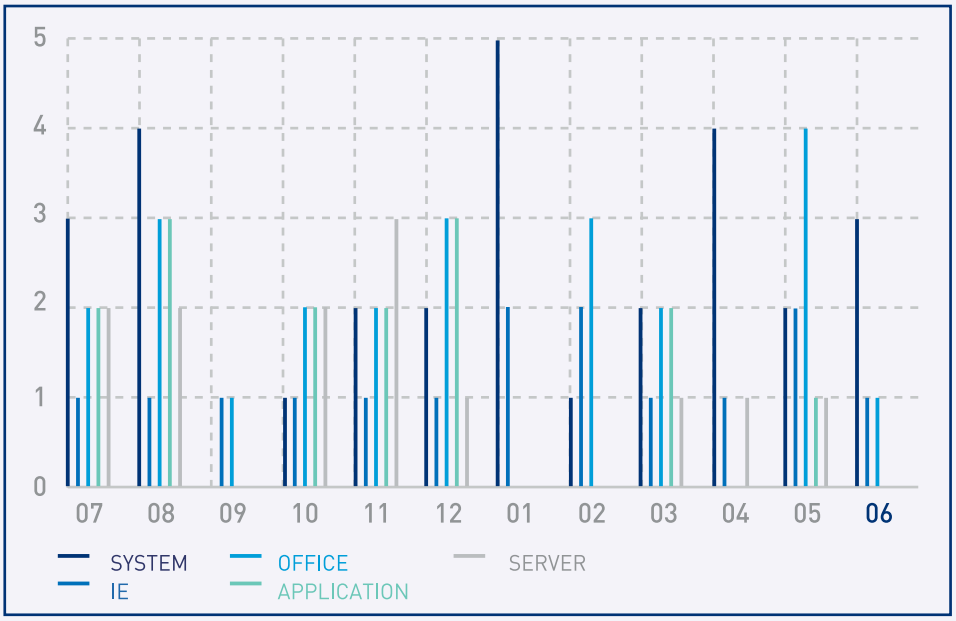


Figure 2-1 | MS Security Updates for each attack target

Critical	
MS13-047	Internet Explorer cumulative security update

Important	
MS13-048	Vulnerability in the Windows kernel could allow information disclosure
MS13-049	Vulnerability in the kernel mode driver could allow denial of service
MS13-050	Vulnerability in Windows print spooler could allow elevation of privilege
MS13-051	Vulnerability in Microsoft Office could allow remote code execution

Table 2-1 | MS Security Updates for June 2013

Security Trend

02. Security Issues

DDoS attacks specifically targeting major government agency DNS servers

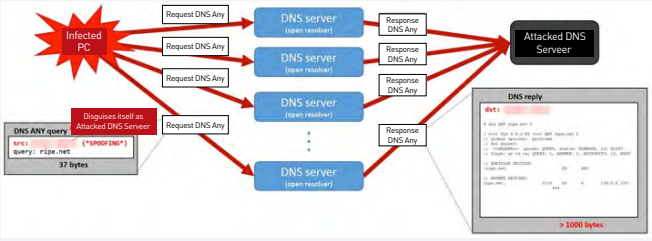


Figure 2-2 | Basic diagram for DNS-Amplification – DDoS attacks

Samples for DNS Amplification DDoS Attacks have been discovered in the anonymous 6.25 hacking event. The primary technique of DNS Amplification DDoS Attack is sending a DNS ANY Query with an IP spoofed to be the target's IP to the publically accessible Open Resolver (Reflector, a king of mediating DNS server) to flood a target system with DNS response traffic. The queries result in much larger response, up to several dozen times the size of the original queries, overwhelming the system and causing a DDoS attack situation.

In an amplification scenario, the attack infects several PCs to make them into zombie PCs. The IP addresses of zombie PCs are forged as the target's IP address to send domain address verification requests to the other DNS servers. The DNS servers that received these requests send responses to the forged IP address, flooding a target system with DNS response traffic.

When sending IP address verification requests to other DNS servers through forged IP addresses, the attacker also requests a response whose size is a dozen times larger than the size of the original query. With this,, the target DNS server is flooded with amplified response traffic.

To verify the attack process, ASEC simultaneously sends specific domain verification requests to 20,000 different DNS servers to attack the target with more than 1,000-byte response traffic.

As shown in [Figure 2-3], the results of ANY records of the ripe.net are more than 1,000 bytes. Many PCs requests domain verifications at the same time, so the bandwidths and name server resources are completely consumed.

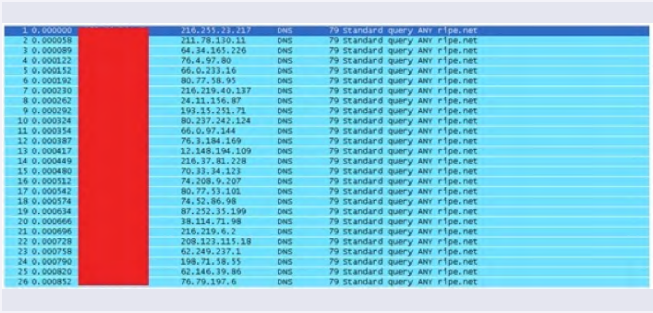


Figure 2-3 | DNS Query using a forged IP address

These malicious codes can be detected and repaired with the latest V3 products.

-Trojan/Win32.Ddkr

-Trojan/Win32.XwDoor

Edward Snowden effect causing ripple effects around the world

Edward Joseph Snowden, a former CIA employee, leaked details of several top NSA secrets including PRISM, a mass electronic surveillance program and the interception of the United States telephone audit data to the Guardian press, causing a deep impact around the world.

Snowden warned that the extent of mass data collection and the surveillance range of PRISM were far greater than the public knew and included what he characterized as "dangerous" and "criminal" activities. PRISM is one of the mass electronic surveillance programs operated by the United States National Security Agency (NSA). PRISM began in the wake of the passage of the Protect America act under the Bush administration after the 9.11 terror attacks.

According to The Guardian, the electronic system, a major tool to collect information for PRISM, basically collects and analyzes all electronic communication in the U.S. and abroad. With this tool, phone numbers, call duration, caller locations, and telephone conversations can be recorded. Snowden leaked to the press that PRISM had collected 97 billion pieces of data from each nation's government agencies as well as general American citizens.

Based on the disclosures about the National Security Agency (NSA) and CIA data-gathering operations around the world, the European Union requested the U.S. government to give an explanation. Since Snowden's story became one of the hottest topics, the secretary general of the International Telecommunication Union (ITU), a United Nations agency said in his interview, "The international society has an opportunity to reach a cease-fire agreement to stop cyber wars." By cooperating with the United Nations Office on Drugs and Crime, the ITU has cracked down various cyber crimes. In fact, all nations keep watch over each other in cyber space and are waging fierce cyber wars.

Snowden also revealed that U.S. agencies have hacked into computers in Hong Kong and mainland China hundreds of times since 2009. He added that the U.S. has a powerful boundless informant system to view cyber communication without hacking into individual computers and has hacked into universities, schools, and companies located in China as well as Hong Kong. The U.S. has launched more than 60,000 hacking operations against the world.

The most interesting fact is that Snowden's leaks of classified information has boosted some of the Chinese Internet security stocks. The investors eagerly buy Internet security stocks as the United States government surveillance program reaches into computers in mainland China and Hong Kong. Chinese stock market calls this phenomenon the "Snowden Effect".

Snowden's disclosures about the U.S. NSA data-gathering operations, cyber surveillance, and hacking operations around the world have aided to boost the Internet security stock price, launch cyber wars across nations, and cause various ripple effects.

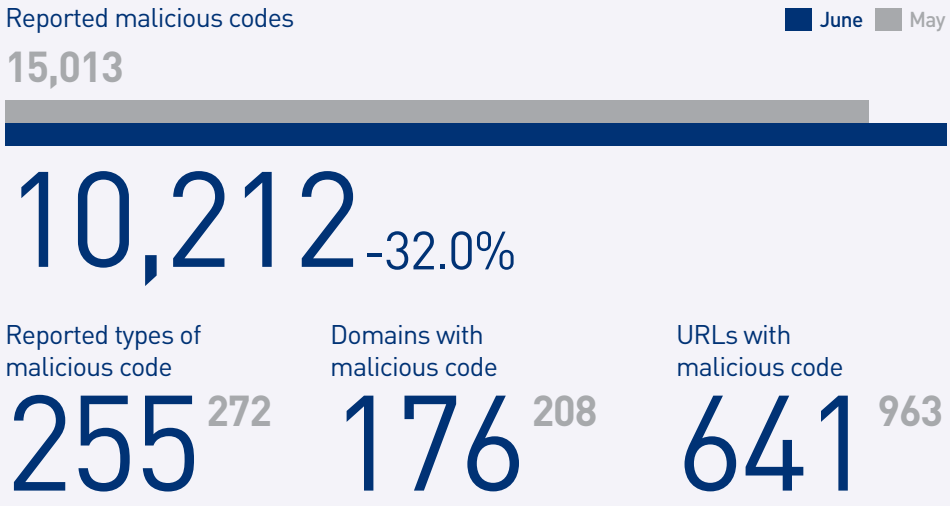
Web Security Trends

01. Web Security Statistics

Website malicious code trends

This month, SiteGuard (AhnLab's web browser security service) blocked 10,212 malware from websites that distributed malicious codes. 255 types of malicious code, 176 domains with malicious code, and 641 URLs with malicious code were found. Compared to the previous month, the number of malicious code reports increased, whereas the number of malicious code types, malicious URLs, and malicious domains decreased.

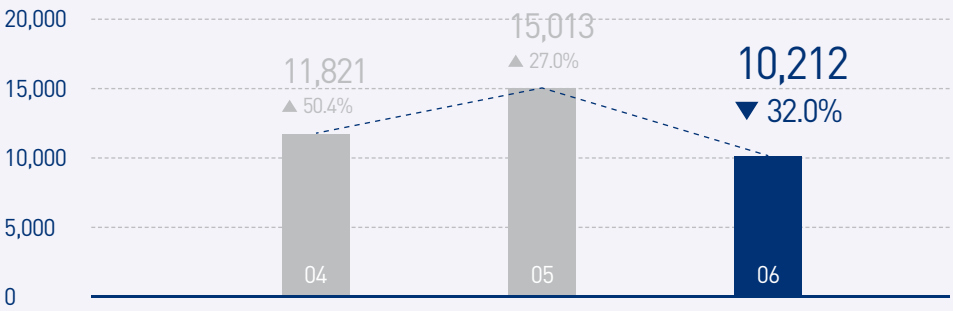
Table 3-1 | Website security trends for June 2013



Monthly Change in Malicious Code Reports

As of June 2013, the number of malicious code reports decreased to 10,212, a 32% drop from the 15,013 reported in the previous month.

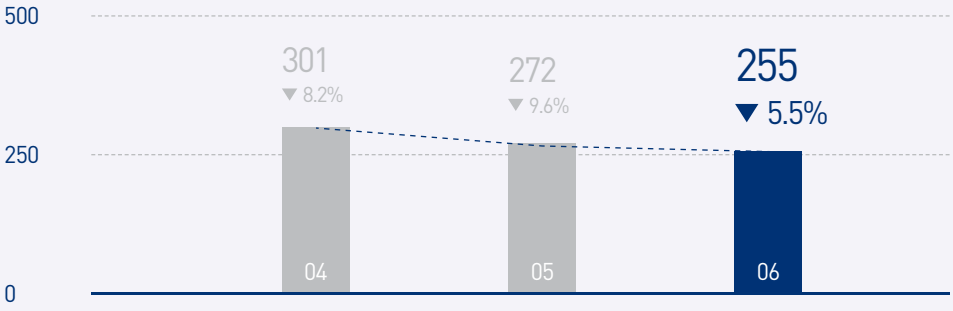
Figure 3-1 | Monthly Change in Malicious Code Reports



Monthly Change in the Number of Reported Malicious Code Types

As of June 2013, 255 malicious code types were reported, a 5.5% decrease from 272 reported in the previous month.

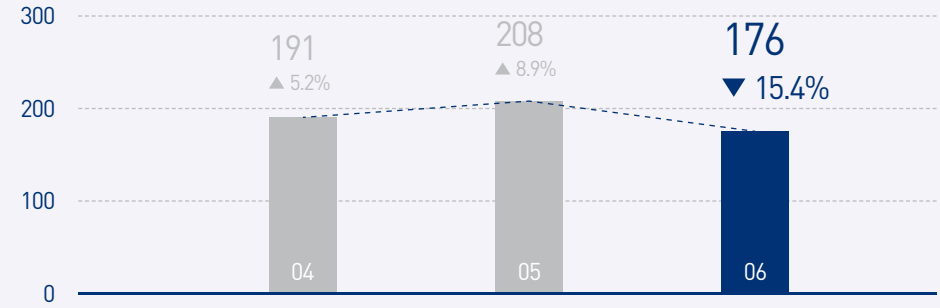
Figure 3-2 | Monthly Change in the Number of Reported Malicious Code Types



Monthly Change in Domains with Malicious Code

As of June 2013, 176 domains with malicious code were reported, which is a decrease from 208 reported in the previous month.

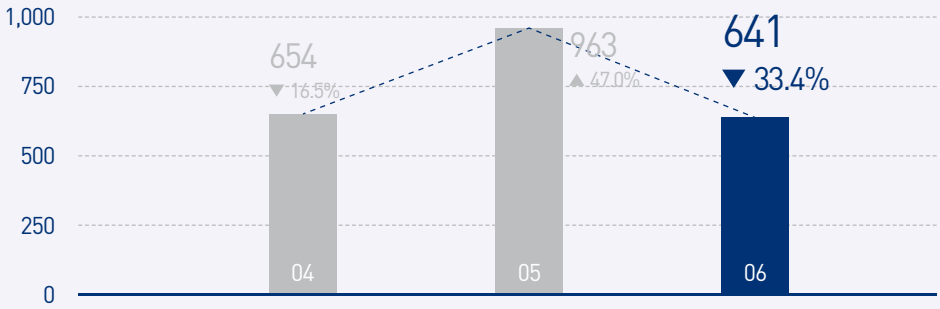
Figure 3-3 | Monthly Change in Domains with Malicious Code



Monthly Change in URLs with Malicious Code

As of June 2013, 641 URLs with malicious code were reported, a 66% decrease from 963 reported in the previous month.

Figure 3-4 | Monthly Change in URLs with Malicious Code



Top Distributed Types of Malicious Code

Type	Report	Percentage
TROJAN	4,759	31.7 %
SPYWARE	4,038	26.9 %
ADWARE	3,548	23.6 %
DOWNLOADER	277	1.8 %
DROPPER	89	0.6 %
Win32/VIRUT	41	0.3 %
APPCARE	11	0.1 %
JOKE	2	0.0 %
ETC	2,248	15.0 %
	15,013	100.0 %

Table 3-2 | Top Distributed Types of Malicious Code

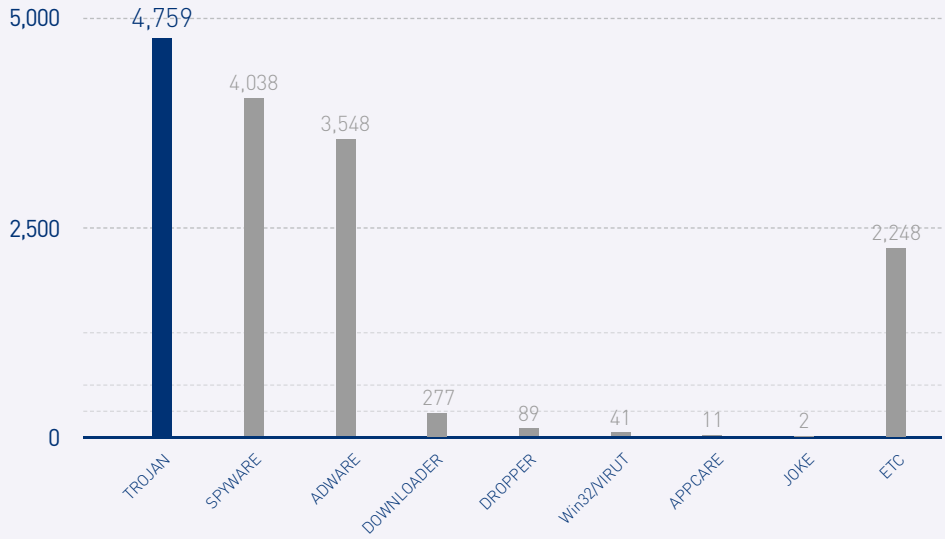


Figure 3-5 | Top Distributed Types of Malicious Code

II. Security Trends for the First Half of 2013

01. Security threat trends for the first half of 2013

Large-scale security events at government agencies, news press, and financial companies

During the first half of 2013, large-scale security events targeting government agencies, news press, and financial companies occurred on March 20 and June 25. Two large-scale security events through the first half of 2013 were similar in that social infrastructure such as government agencies, news press, and financial companies were the main targets. The detailed attack methods, however, were different.

The main purpose of the security event on March 20 was to spread malicious codes that overwrote disk Master Boot Records (MBRs) and Volume Boot Records (VBRs) with specific strings to prevent normal operation of the infected systems and destroy data, which was similar to previously reported large-scale security events.

The security event took place on June 25 to spread malware for data destruction and system malfunction as well as to launch large DDoS (Distributed Denial of Service) attacks against the websites of Korean government agencies including Blue House. In addition, new DDoS attack methods such as a DNS Amplification DDoS Attack method and a script-based DDoS attack method were introduced in these security events.

Internet banking malware using memory patching functions

Online game hacking malware for stealing game user information reported in June 2013 used a new information stealing function for Korea Internet banking sites. The online game hacking malware, which originally was used to steal online game user information, has been used to target other websites since August 2012. Around that time, this malware snatched server administrator page information from news press companies and government agencies. It modified hosts files that the Banki malware used to hijack users' browsers, directing them to banking websites.

The newly discovered Internet baking attack method in 2013 steals user information by performing memory patching for unique security modules. Usually, this type of attack method steals user information during normal Internet banking processes, so it is difficult for users to recognize this malware infection.

Korean software Zero-day vulnerability attacks are on the rise

Increase in malware exploiting Korean software vulnerabilities started several years ago and continues to rapidly accelerate year after year.. This malware poses a great challenge in that it exploits widely-used general products. For example, Internet banking software vulnerabilities and other security software vulnerabilities were discovered in early June. The latest updates are also recommended for newly discovered movie player vulnerabilities.

The attack method for inserting malicious codes into document files by exploiting document software vulnerabilities is also on the rise.

Malware exploiting vulnerabilities of both MS Office products and Adobe Reader (PDF) has been continuously reported with thenumber of reports on Korean software vulnerability exploitation steadily increasing. ASEC reports of malicious codes that exploit vulnerabilities in Hangul files have increased, and a similar attack first took place in June against "Hancell" (a spreadsheet program).

The increase of vulnerability attacks that target specific Korean software means that cyber attackers want to steal internal confidential information from specific organizations. Since many

government agencies are widely using Korean documentation software products, they have become hot targets for cyber attackers. The newly discovered Korean software vulnerabilities in the first half of 2013 are prevalent in Korea. It is no doubt that the cyber criminals can steal data and perform malicious activities more easily through zero-day vulnerabilities if a large number of users widely use those programs.

As the number of zero-day vulnerability attacks against Korean software products is expected to steadily increase, users need to exercise more caution.

Malware evolution – online game hacking malware combined with pharming malware

One of the peculiar features of security threats reported during the first half of 2013 is that the number of cyber attacks that stole personal information drastically increased. The most frequently reported personal information-stealing malware types in H1/2013 are internet banking information-stealing malware and online game account information-stealing malware.

Internet banking information-stealing malware and online game account information-stealing malware have been reported for a long time, and more refined and improved variants are constantly emerging.

Online game account information-stealing malware in particular has been distributed by modifying or dispatching Windows system files to evade detection. Most online game hacking malicious codes use this method. To avoid detection by anti-virus software, attackers have endlessly distributed many variants and developed various security software incapacitation methods.

Internet banking information-stealing malware uses various advanced methods such as: using fraudulent phishing websites that are almost the same as legitimate bank sites, modifying hosts.ics files as well as hosts files, and preventing IP blocking by communicating with C&C servers to update new pharming site addresses. This latest attack method has evolved to perform malicious activities based on monitored security module activities.

If PC users enter the desired website addresses in their web browsers, then the system verifies the website IP addresses through the DNS (Domain Name Service) based on the entered information. The priority of the verification processes is described in the table below. If one of processes is forged or modified, then users are directed to the fraudulent websites instead of the legitimate websites that they want to visit.

1. DNS Cache information of the local system
2. hosts.ics
3. hosts
4. DNS

Malicious codes that steal important personal information are evolving rapidly, and new variants are constantly emerging. Recently, we found new malware using both the internet banking information-stealing method and the online game account information-stealing method to maximize financial gains.

JAVA and Internet Explorer vulnerabilities continuously exploited

The special feature of vulnerability threats of the H1/2013 is that most malicious codes exploit various application vulnerabilities (MS Internet Explorer, Adobe Flash Player, Acrobat Reader, Oracle Java) instead of system vulnerabilities. Vulnerability exploitations have been reported much more frequently for Internet Explorer and Java applications than other applications in H1/2013.

In particular, two Java zero-day vulnerabilities became the hottest issues in the first half of 2013. Like other previous Java vulnerabilities, the first CVE-2013-0422 vulnerability can allow the sandbox bypass by exploiting the fact that Java does not have security check functions. The second CVE-2013-1493 vulnerability that was also used by the Cool Exploit Toolkit can allow malicious activities through memory corruption errors.

According to ASEC analysis results on Internet Explorer vulnerabilities (including CVE-2013-1347) during H1/2013, the use-after-free vulnerabilities was the most frequently reported vulnerability. These are Heap Memory vulnerabilities on browsers that have been reported since the end of 2012.

Since these vulnerabilities are actively exploited by Web Exploit Toolkits to attack user PCs that are accessing websites, it is recommended to update security patches and install the latest security solutions.

Internet cyber intelligence wars trigger fears of wider conflict across nations

During the first half of 2013, as internet cyber intelligence activities arousing rumors and suspicions for a long time have slowly been disclosed to the public, tension and conflict are increasing around the world.

On January 30, The New York Times announced that its system had been continuously attacked by Chinese hackers for 4 months

after the report on the Chinese Wen Jiabao family-owned property was published in October 2012. In addition, The New York Times reported on February 19 that the Chinese People's Liberation Army 61398 was secretly involved in the United States information disclosure incident by quoting security reports created by Mandiant, the United States security provider. The Department of Defense insisted that the Chinese government and the People's Liberation Army were deeply involved in cyber intelligence activities. As a consequence, imposing strong import restrictions against Chinese network devices and equipment was publicly discussed.

In early June, the Guardian exposed Prism, a clandestine mass data-gathering program to detect terrorists and prevent terrorism. On June 10, the Foreign Policy reported that the NSA has a dedicated internal organization responsible for hacking Chinese computers and systems. In addition, the Guardian revealed that the United Kingdom Intelligence agency hacked each delegation during the 2009 G20 summit.

The Syrian Electronic Army hacked the BBC Weather, Guardian, and Onion Twitter accounts. Especially on April 23, the stock price temporally soared as the Syrian Electronic Army hacked the AP news twitter account to send out false messages about the White House's explosion.

It is suspected that the North Korea People's army might be maneuvering behind the scenes of the March 20 and June 25 network failures in South Korea.

Currently, the government agencies of each nation are strengthening their systems and organizations to quickly respond to ever-increasing cyber threats. There is a high possibility that diplomatic conflicts triggered by cyber intelligence activities might be exacerbated in the future.

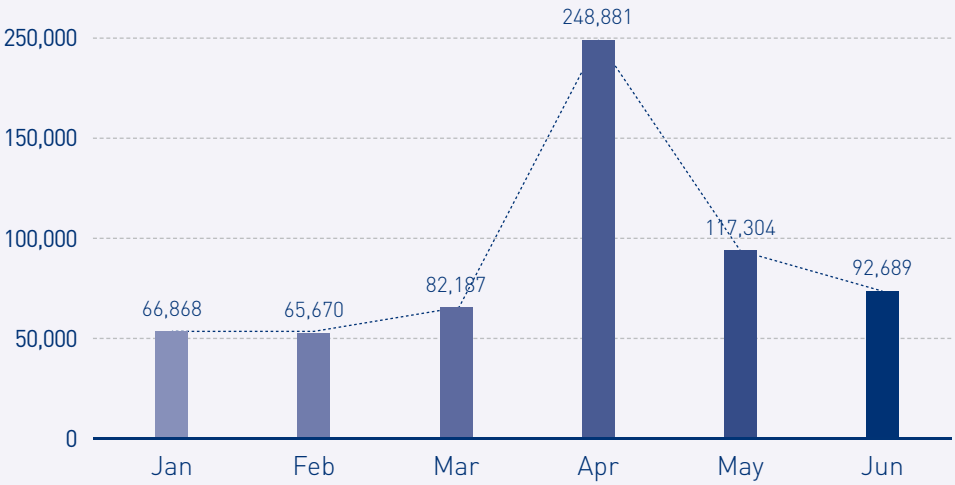
II. Security Trends for the First Half of 2013

02. Malicious code trends for the first half of 2013

The number of mobile malware reports is soaring in H1/2013

[Figure 5-1] shows monthly mobile malicious code reports that are categorized and detected as malicious codes with V3 Mobile. Through H1/2013, V3 Mobile had detected 673,599 malicious code reports, which is much higher than the malicious code reports (262,718) for last year.

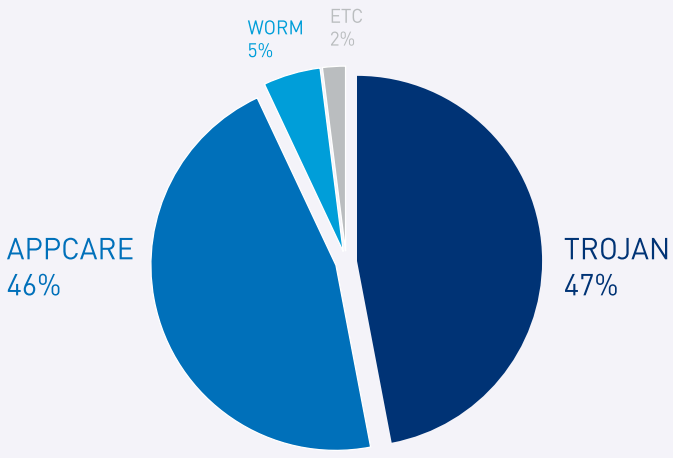
Figure 5-1 | Monthly malicious code reports



Trojan horse on the rise – stealing information and luring users into paying money

The malicious code types reported during the first half of 2013 are listed in [Figure 5-2]. Last year, the PUP malware that exposes unwanted advertisements without executing the specific application was the most frequently reported malware. In the first half of this year, the Trojan Horse malware that steals user information or racks up hefty bills was the most frequently reported malware.

Figure 5-2 | Malicious code type breakdown



Malicious application racking up hefty charges ranked as the most frequently reported malicious code

[Table 5-1] categorizes the Top 10 mobile malicious code types reported by AhnLab customers in the first half of 2013. Android-Trojan/FakeInst that lures users into installing paid applications for free to rack up hefty charges was the most reported malicious code type, and 6 types of PUP malicious codes that display unwanted advertisements without executing specific applications were ranked among Top 10 malicious code types.

Table 5-1 | Top 10 malicious code type reports

Number	Threat	Reports	Percentage
1	Android-Trojan/FakeInst	158,663	24%
2	Android-PUP/Airpush	90,218	13%
3	Android-Trojan/Opfake	49,309	7%
4	Android-PUP/Kuguo	33,730	5%
5	Android-PUP/Wapsx	32,890	5%
6	Android-Exploit/Rootor	28,000	4%
7	Android-PUP/Plankton	23,329	3%
8	Android-PUP/Leadbolt	22,028	3%
9	Android-PUP/Admogo	18,842	3%
10	Android-Trojan/GinMaster	18,214	3%

ASEC REPORT CONTRIBUTORS

Contributors	ASEC Researchers SiteGuard Researchers
Editor	Sales Marketing Team
Design	UX Design Team
Publisher	AhnLab, Inc.

US:
info@ahnlab.com

Other Regions:
global.sales@ahnlab.com

AhnLab