ASEC REPORT

VOL.30 | 2012.07

AhnLab Monthly Security Report

AhnLab

AhnLab Security Emergency response Center

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).

CONTENTS

1. SECURITY TRENDS - JUNE 2012

01. Malicious Code Trend

a. Malicious Code Statistics

11 Million Malicious Codes Reported in June, a Decrease of 12.6%

Statistics collected by the ASEC show that 11,006,597 malicious codes were reported in June 2012. This is a decrease of 1,582,812 from the 12,589,409 reported in the previous month (See Fig. 1-1]). The most frequently reported malicious code was ASD.PREVENTION, followed by JS/Agent and Trojan/Win32.Gen. Also, a total of four malicious codes such as Java/Exploit, Backdoor/Win32.trojan, Java/Cve-2011-3544 and Downloader/Win32.opentab were newly enlisted among the top 20 (See [Table 1-1]).

[Fig. 1-1] Monthly Malicious Code Reports

Ranking	↑↓	Malicious Code	Reports	Percentage
1	▲3	ASD.PREVENTION	499,586	13.5%
2	▲5	JS/Agent	442,822	12.0%
3	▼1	Trojan/Win32.Gen	436,387	11.8%
4	▲2	Textimage/Autorun	308,594	8.3%
5	▲13	Downloader/Win32.agent	270,554	7.3%
6	▲3	Malware/Win32.generic	218,769	5.9%
7	▼4	Trojan/Win32.adh	202,204	5.5%
8	—	Adware/Win32.korad	189,221	5.1%
9	▲6	JS/Exploit	141,331	3.8%
10	▼5	Trojan/Win32.bho	133,177	3.6%
11	▼1	Trojan/Win32.sasfis	103,509	2.8%
12	NEW	Java/Exploit	94,353	2.6%
13	▲1	Als/Bursted	93,881	2.5%
14	▲6	RIPPER	88,015	2.4%
15	NEW	Backdoor/Win32.trojan	86,971	2.4%
16	NEW	Java/Cve-2011-3544	85,448	2.3%
17	—	Trojan/Win32.agent	79,946	2.2%
18	▼6	Malware/Win32.suspicious	76,612	2.1%
19	▼3	Mov/Cve-2012-0754	74,073	2.0%
20	NEW	Downloader/Win32.opentab	72,764	1.9%
			3,698,217	100.0%

[Table 1-1] June 2012 Top 20 Malicious Code Reports (By Report and Malicious Code)

Top 20 Distributed Malicious Codes

[Table 1-2] below shows the percentage breakdown of the top 20 malicious code variants reported this month. For June 2012, Trojan/Win32 (1,534,154 reports) was the most reported malicious code of the top 20 malicious code variants, followed by Adware/Win32 (566,838 reports) and Win-Adware/Korad (550,361 reports).

Ranking ↑↓		Malicious Code	Reports	Percentage
1	—	Trojan/Win32	1,534,154	21.0%
2	▲1	Adware/Win32	566,838	7.8%
3	▲7	Win-Adware/Korad	550,361	7.5%
4	▲2	Downloader/Win32	533,926	7.3%
5	▲2	ASD	499,586	6.8%
6	▼1	Win-Trojan/Agent	486,534	6.7%
7	▲1	JS/Agent	465,723	6.4%
8	▲3	Win-Trojan/Downloader	392,453	5.4%
9	▼5	Malware/Win32	325,274	4.4%
10	▼1	Textimage/Autorun	308,659	4.2%
11	▲1	Win-Trojan/Onlinegamehack	276,251	3.8%
12	▲4	Win-Trojan/Korad	230,691	3.2%
13	NEW	Backdoor/Win32	184,321	2.5%
14	—	Win32/Conficker	151,449	2.1%
15	NEW	Win-Dropper/Korad	151,225	2.1%
16	▼1	Dropper/Win32	146,058	2.0%
17	▲2	JS/Exploit	141,331	1.9%
18	▼1	Win32/Virut	133,727	1.8%
19	▲1	Win32/Kido	119,882	1.6%
20	NEW	Win32/Autorun.worm	114,198	1.5%
			7,312,641	100.0%

[Table 1-2] Top 20 Distributed Malicious Codes

'Win-Adware/KorAD.608256' – the New and Most Reported Malware in June

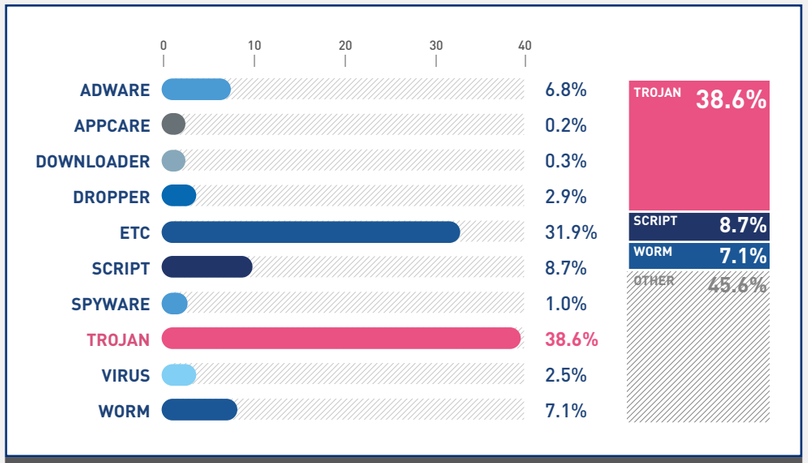
[Table 1-3] below shows the percentage breakdown of the top 20 new malicious codes reported this month. Win-Adware/KorAD.608256 was the most frequently reported new malicious code, representing 14.9% (71,935 reports) of the top 20 new malicious codes, followed by Win-Trojan/Agent.20480.BQF (34,540 reports) and Win-Spyware/KeyMatch.612344.B (34,349 reports).

Ranking ↑↓	Malicious Code	Reports	Percentage
1	Win-Adware/KorAd.608256	71,935	14.9%
2	Win-Trojan/Agent.20480.BQF	34,540	7.2%
3	Win-Spyware/KeyMatch.612344.B	34,349	7.1%
4	Win-Trojan/Agent.20480.BQE	34,239	7.1%
5	Win-Adware/KorAd.335872	32,217	6.7%
6	Win-Trojan/Downloader.91808	26,707	5.5%
7	Win-Trojan/Agent.402432.AC	25,611	5.3%
8	Win-Trojan/Korad.782848	23,103	4.8%
9	Win-Trojan/Agent.230400.AY	21,087	4.4%
10	Win-Adware/KorAd.323584.E	20,887	4.3%
11	Win-Trojan/Downloader.570296	20,221	4.2%
12	Win-Spyware/KeyMatch.612344	19,277	4.0%
13	Win-Trojan/Agent.122880.ABW	18,752	3.9%
14	Win-Spyware/SpyBot.658944	16,822	3.5%
15	Win-Trojan/Spybot.658944	15,290	3.2%
16	Win-Trojan/Graybird.462336	14,212	3.0%
17	Win-Adware/KorAd.319488.C	13,887	2.9%
18	Win-Adware/Shortcut.Zipcorn.20480	13,198	2.8%
19	Win-Adware/KorAd.763147	12,790	2.7%
20	Win-Trojan/Downloader.164016	12,239	2.5%
		481,363	100.0%

[Table 1-3] Top 20 New Malicious Code Reports

'Trojan Horse Ranked the Most Reported' Malicious Codes in June

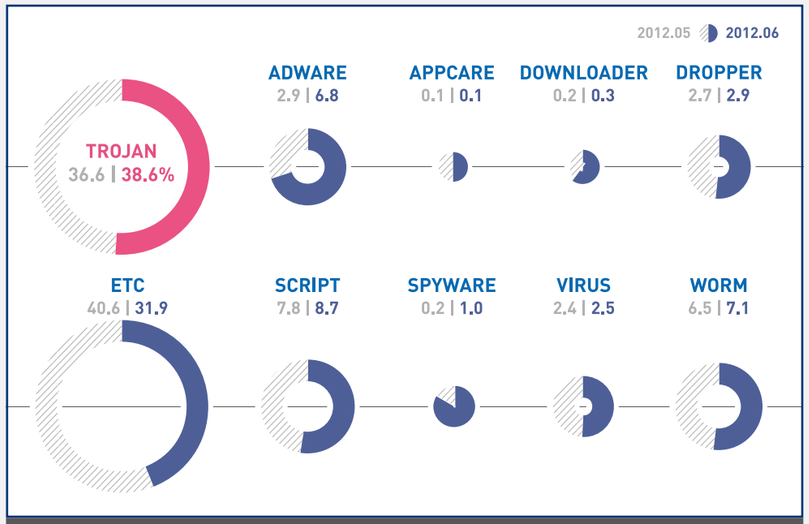
The chart below categorizes the top malicious codes reported this month. Trojan is the most reported malicious code, representing 38.6% of the top reported malicious codes, followed by script (8.7%) and worm (7.1%).



[Fig. 1-2] Primary Malicious Code Type Breakdown

Primary Malicious Code Type Breakdown for June vs May 2012

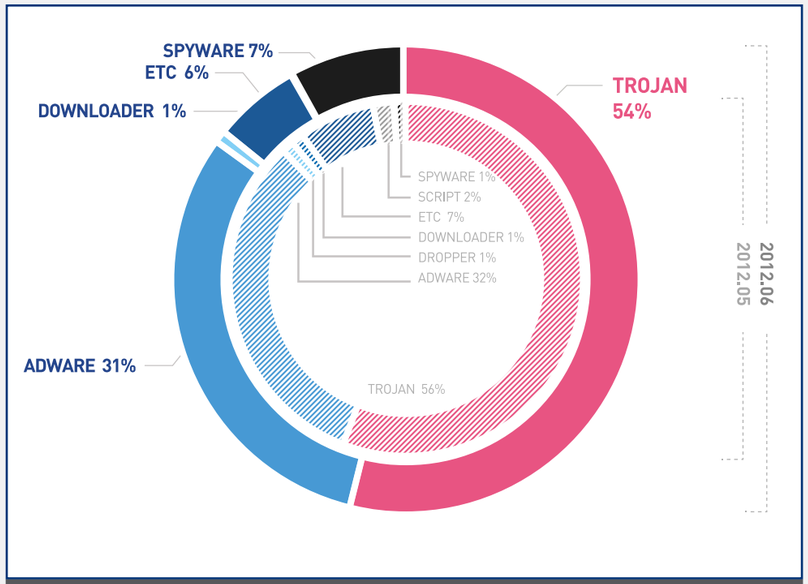
Compared to the previous month, the number of Trojan, script, worm, adware, virus, spyware and downloader reports increased, whereas the number of appcare remained the same.



[Fig. 1-3] Primary Malicious Code Type Breakdown for June vs May 2012

New Malicious Code Type Breakdown

For June 2012, Trojan was the most reported new malicious code, representing 54% of the top reported new malicious codes, followed by adware (31%) and spyware (8%).



[Fig. 1-4] New Malicious Code Type Breakdown

01. Malicious Code Trend
b. Malicious Code Issues

Malicious Codes Target your Bank Account

New form of combined phishing and malware attacks targeting online banking users are becoming ever more sophisticated. The following are the common phishing techniques designed to steal banking information in recent days.

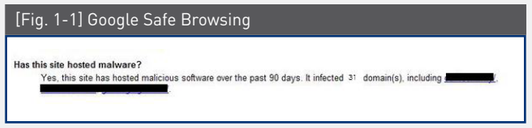
1. How do they distribute malware?

So far three types of distribution channels have been identified.

(1) Website intrusions and application vulnerability combined

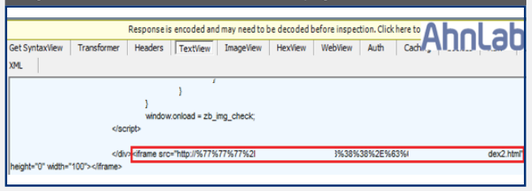
This type of malicious code for stealing online banking information was disseminated via certain URLs. This type attacked computers by taking advantage of security vulnerability in applications (Java, IE, Flash Player and Windows Media Player) running on the hacked websites (31 websites and Google Safe Browsing).

[Fig. 1-1] Google Safe Browsing



The hacked websites had a malicious script link inserted in the notice page (See [Fig. 1-2]) written with Zeroboard.

[Fig. 1-2] iframe inserted in the notice page

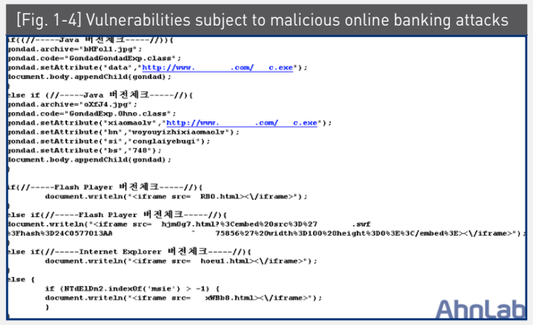


The distribution and infection of malicious codes that intercept online banking information originate from malicious HTML files. Running the infected HTML files triggers the download and execution of other HTML files of which codes are obfuscated to make their identification difficult (See [Fig. 1-3]).

[Fig. 1-3] Obfuscated malicious HTML

If you de-obfuscate them, you will see codes that seem to exploit vulnerabilities of Java, IE and Flash Player.

[Fig. 1-4] Vulnerabilities subject to malicious online banking attacks



Malicious codes targeting online banking check the version of each application (See [Table 1-4]) to identify vulnerabilities to exploit to infect as many computers as possible.

[Table 1-4] Online banking vulnerability breakdown by application

Application	Vulnerability ID
Java	CVE-2011-3544 / CVE-2012-0507
Flash Player	CVE-2011-2140 or CVE-2012-0754
Windows Media Player	MS12-004
Internet Explorer	MS10-018

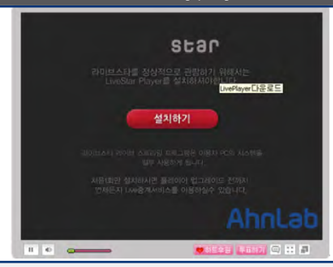
(2) Repackaged malware into legitimate application

There were reports on repackaging of certain Internet live broadcasting programs and Torrent, a P2P program with malicious codes for online banking.

1) Internet live broadcasting programs

If you click the "Install" button as shown in [Fig. 1-5], you will

[Fig. 1-5] Internet live broadcasting programs



end up downloading Install_LiveManagerPlayer.exe along with malicious codes lurking inside to steal your banking information. However, this problem is fixed now and the program is clean.

2) Torrent, a P2P program

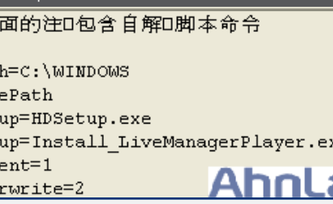
[Fig. 1-6] uTorrent, a P2P program

uTorrent is one of the most widely used P2P programs and is easy to download. With this in mind, malicious attackers repackaged the legitimate files in the uTorrent.exe with malicious codes to steal online banking information.

This disguises itself as executable with a .exe extension but is structured as a self-extracting executable file or SFX.

If you run the code, the following option will automatically be executed (See [Fig. 1-7]).

[Fig. 1-7] SFX option and a normal file when executed



Running the malicious code will cause a normal file in an SFX file . However, malicious codes are created and run in the background, making it hard for the user to spot such an attack.

2. Malicious Code Analysis

The basic format of an online banking malicious code is a self-extracting executable file or SFX but the actual attack is made by the following three files that the SFX contains.

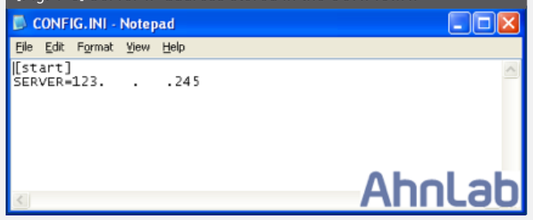
[Table 1-5] Structure of a malicious SFX

File name:	Major function
CONFIG.INI	A configuration file that stores the server IP address for the following two files to run on.
CretClient.exe	Searches for and steals certificates in a certain path.
HDSetup.exe	Modifies and deletes hosts file and changes security options of Internet Explorer.

(1) CONFIG.INI

CONFIG.INI is a configuration file that stores the server IP address for CretClient.exe and HDSetup.exe to run on.

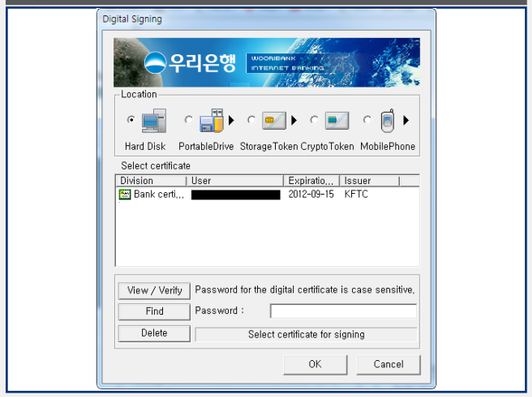
[Fig. 1-8] Server IP address stored in the CONFIG.INI



(2) CretClient.exe

CretClient.exe is a fraudulent digital certification file that runs when a user connects to the phishing websites from an infected computer. If the file is run alone, a fraudulent KB Kookmin Bank digital certification window appears as in [Fig. 1-9] below but, if it is executed from a phishing website, the window will automatically turn to the certification windows of one of the four

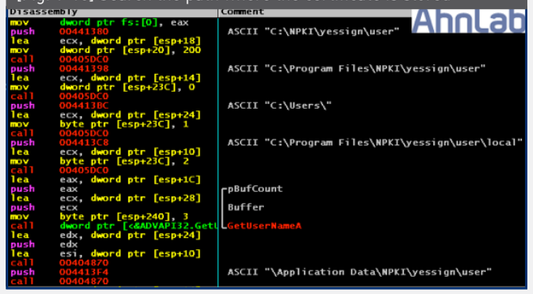
[Fig. 1-9] CretClient.exe execution screen



fake bank websites, namely Kookmin Bank, Woori Bank, NH Bank and Korea Exchange Bank.

The scam certification program extracts certificate information under use and induces the user to enter the password.

[Fig. 1-10] Search the path where the certificate is stored



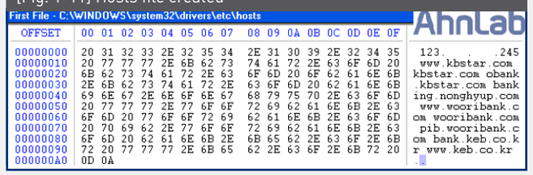
(3) HDSetup.exe

HDSetup.exe creates hosts files containing a fake IP address and a URL that redirect the user to phishing websites.

Modified Hosts File

When run, HDSetup.exe will delete the existing hosts file and replace it with a new one containing the following information as shown in [Fig. 1-11].

[Fig. 1-11] Hosts file created



The user will be redirected later to the phishing website if he/she tries to connect to one of the banks specified in [Table. 1-5].

3. Analysis of phishing websites

See [Table 1-6] below for the banks names that have been the subject of phishing scams.

[Table 1-6] List of phishing target banks

Bank Name	Phishing URL
Kookmin Bank	http://www.kbstar.com, http://kbstar.com http://obank.kbstar.com
NH Bank	http://banking.nonghyup.com
Woori Bank	http://www.wooribank.com, http://wooribank.com http://pib.wooribank.com
Korea Exchange Bank	http://bank.keb.co.kr, http://www.keb.co.kr

Although the process flow may differ slightly between each bank, the following diagram conceptualizes generally how the user's account information is stolen:to phishibg webite

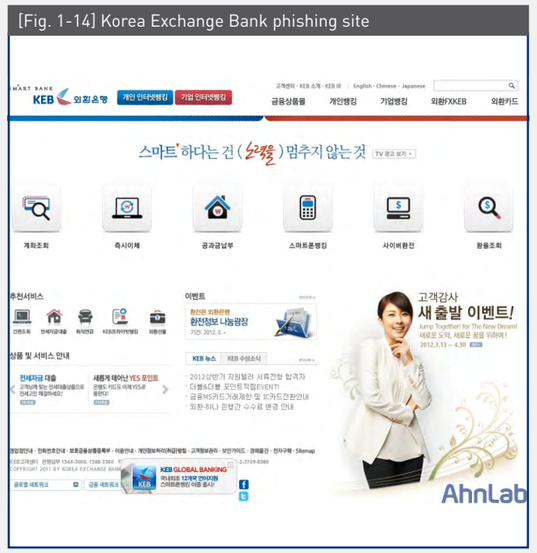
2. Fake certification login
3. Request security level upgrade
4. Type name and identification number
5. Type account number

It is hard to tell phishing websites from legitimate ones. A significant amount of time investment seems to have been made in their preparation.

[Fig. 1-12] KB Kookmin Bank phishing site

[Fig. 1-13] NH Bank phishing site

[Fig. 1-14] Korea Exchange Bank phishing site



[Fig. 1-15] Woori Bank phishing site

It is not easy to distinguish phishing sites from legitimate ones. However, if you stay alert to warnings and advisories published by banks regarding phishing, you can easily detect signs of a phishing scam.

For example, phishing websites require you to enter the number strings on your security card in their entirety, whereas legitimate sites do not. Suspicious signs can also be detected in the steps of public certification login.

V3 detects this malware as:

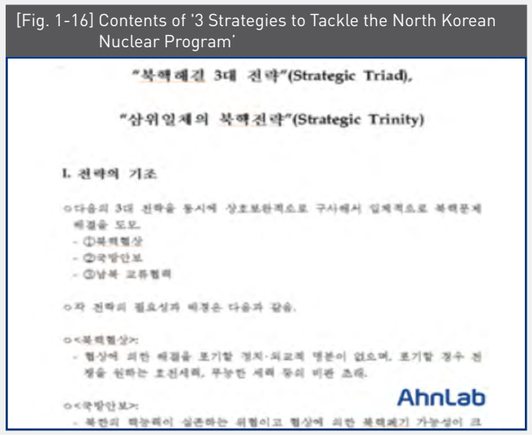
- Trojan/Win32.Banki(V3, 2012.06.11.02)
- Dropper/Banki.386832(V3, 2012.06.11.02)
- Win-Trojan/Qhost.386826(V3, 2012.06.08.03)
- Win-Trojan/Banki.525299(V3, 2012.05.25.00)
- Win-Trojan/Banki.425984.B(V3, 2012.06.11.02)
- Win-Trojan/Banki.421888(V3, 2012.06.11.02)
- Win-Trojan/Banki.643072(V3, 2012.05.25.00)
- Win-Trojan/Banki.643072.B(V3, 2012.06.11.02)
- Win-Trojan/Banki.643072.C(V3, 2012.06.11.02)

Malicious Codes Exploiting Hangul Zero-day Vulnerability – 1

Malicious codes exploiting Hangul (*.HWP files) zero-day vulnerabilities have been emerging recently, causing fear in many companies suffering APT attacks. Therefore, before security patches are released, extra caution needs to be taken not to open malformed HWP (Hangul) files.

If a victim opens the malformed file, a normal HWP document file entitled <3 Strategies to Tackle the North Korean Nuclear Program> will be opened.

[Fig. 1-16] Contents of '3 Strategies to Tackle the North Korean Nuclear Program'



Taking advantage of the application vulnerabilities, then below malicious files are created.

- %Systemroot%\hwprnt.dll
- %Systemroot%\system32\comirv.dll
- %Systemroot%\system32\rundir.dll
- %Systemroot%\hwprnt.dll

1. The hwprnt.dll file collects system information using the systeminfo command and stores it in the soric.rxc file.

2. The comirv.dll file transfers the system information file (soric.

rxc) collected through the web mail service of indiatimes.com to an email account 'kim unhong <voice????@indiatimes.com>'.

3. The rundir.dll file is registered in the service as 'Themas', named similarly to the legitimate 'Themes' service and automatically run when the system starts. Once the service starts, the file changes the setting of the Windows firewall to 'Off' and injects the comirv.dll file into the explorer.exe process for execution.

V3 detects this malware as:
- HWP/Exploit(2012.06.21.00)
- Win-Trojan/Agent.147456.QS(2012.06.21.00)
- Trojan/Win32.Infostealer(2012.06.20.03)
- Win-Trojan/Agent.45056.BOS(2012.06.21.00)

TrusGuard detects this malware as:
- Exploit/HWP.AccessViolation-DE

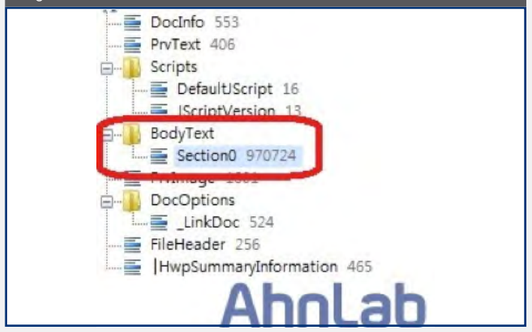
The new behavior-based MDP engine embeded in V3 Internet Security 9.0 can also detect it without a signature.

ASD 2.0 MDP engine detects this malware as:
- Dropper/MDP.Document (57)

Malicious Codes Exploiting Hangul Zero-day Vulnerability – 2

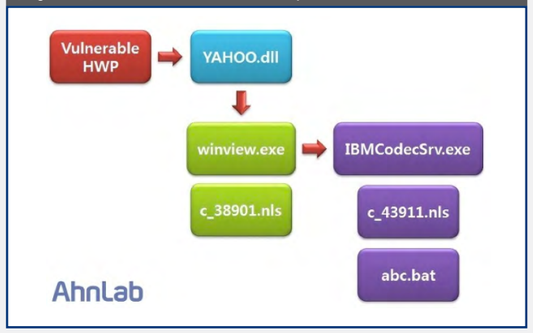
Another malicious HWP file in the form of an email attachment has been reported. The fie size is 986,624 bytes and it is structured as in [Fig. 1-17],and contain other encoded PE (portable executable) files.

[Fig. 1-17] Vulnerable HWP file structure



They shows the following infection flow ([Fig. 1-18]), and generate other malicious files and log files.

[Fig. 1-18] Malicious codes created by a vulnerable HWP file



Running this HWP file will trigger the creation of the following files in the Windows system.

- C:\WINDOWS\YAHOO.dll (135,168 bytes)
  The YAHOO.dll file then generates the following files in the Windows system folder (C:\WINDOWS\system32\).
- C:\WINDOWS\system32\winview.exe (49,152 bytes)
- C:\WINDOWS\system32\c_38901.nls (45,056 bytes)

The winview.exe file then clones itself as shown below as well as generating log files that record the information of the infected system.

- C:\WINDOWS\system32\IBMCodecSrv.exe (49,152 bytes)
- C:\WINDOWS\system32\c_43911.nls
- C:\WINDOWS\system32\abc.bat (39 bytes)

The abc.bat file then creates tmp.dat in the same Windows system folder and records the year and date of the execution of the malicious code.

- date /t > "C:\WINDOWS\system32\tmp.dat"

Log file c_43911.nls records the information on the hardware, the operating system and the processes of the programs currently running on the compromised system).

To make the malicious code automatically run again upon boot, a certain registry key will be created so that IBMCodecSrv.exe is registered as a Windows service under the name of 'Microsoft Audio Codec Services'.

Registered registry:
- HKLM\SYSTEM\ControlSet001\Services\Microsoft Audio Codec Services

- ImagePath = "C:\WINDOWS\system32\IBMCodecSrv.exe"

All created files were designed to perform different functions, making it difficult to identify the purposes of such malicious codes as a whole by analyzing a single code.

1. Winview.exe created originally from the YAHOO.dll file and its clone IBMCodecSrv.exe collect hardware and operating system information of the attacked system (See [Fig. 1-19]).

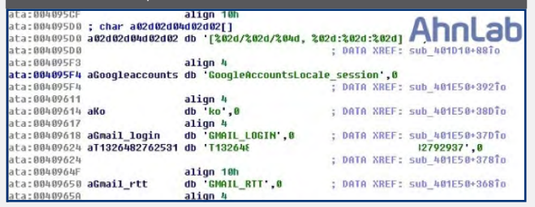
[Fig. 1-19] Malicious codes that collect web browser access information

If a user tries connection to certain web browsers such as Firefox, Internet Explorer and Chrome from a corrupted system, the codes monitor the process and collect all the website addresses accessed.

2. Winview.exe and its clone IBMCodecSrv.exe are designed to collect website addresses accessed from the system under influence and the hardware and operating system information to record in the log file c_43911.nls.

3. Other c_38901.nls files spawned by YAHOO.dll connect to the user session of Google Gmail without user permission (See [Fig. 1-20]).

[Fig. 1-20] Codes connecting to Google Gmail user session without permission



4. c_38901.nls transfers the log file c_43911.nls storing information collected from the systems infected by winview. exe and its clone IBMCodecSrv.exe to a certain email address through the Google Gmail session.

The recently detected malicious codes exploiting Hangul zero-day vulnerability are thought to be devised to collect a variety of information from the system under attack. Such information can be utilized for planning further attacks.

V3 detects this malware as:
- HWP/Exploit
- Trojan/Win32.Dllbot
- Trojan/Win32.Npkon

TrusWatcher detects this malware as:
- Exploit/HWP.AccessViolation-DE

ASD 2.0 MDP engine detects this malware as:
- Dropper/MDP.Document (57)
- service_exploit(CVE-2012-1889)

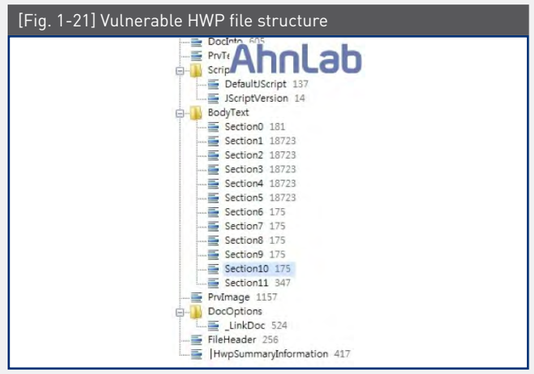
Distribution of Malwares Using Known Hangul Vulnerability

On June 15th, 2012, malwares were detected using vulnerable HWP files that allow code execution. Later, on June 22nd, 2012, Hancom Inc. released security patches to fix such vulnerability, thereby completely blocking further malware attack.

The Hangul files have been spread in the form of an email attachment.

Having the following structure ([Fig. 1-21]).

[Fig. 1-21] Vulnerable HWP file structure



This is a buffer overflow, caused when the periphery of the stack is left unchecked, one of the Hangul vulnerabilities that have been exploited since 2010. If the user opens this compromised HWP file on an also vulnerable system, the scvhost.exe (138,752 bytes) file will be created in the user account's temp folder.

- c:\documents and settings\[user account name]\local settings\

temp\scvhost.exe (138,752 bytes)
When the created scvhost.exe file is executed, wdmaud.drv (78,848 bytes) and wdmaud.dat (78,848 bytes) will be created under the Windows folder (c:\windows).

- C:\WINDOWS\wdmaud.drv (78,848 bytes)
- C:\WINDOWS\wdmaud.dat (78,848 bytes)

Decoding the wdmaud.dat (78,848 bytes) file will trigger the creation of wdmaud.drv (78,848 bytes), a PE file. The wdmaud.dat file is then deleted by scvhost.exe. Wdmaud.drv functions to collect and transfer the following information from the system, which was foiled at the time of our analysis.

[Information to be collected by malware]
- Hardware information
- Windows operating system information
- User login information
- Upload and download files
- IP and Proxy server addresses of the infected system

V3 detects this malware as:
- JS/Agent
- Win-Trojan/Dekor.32936
- Trojan/Win32.Dllbot

TrusWatcher detects this malware as:
- Exploit/HWP.AccessViolation-DE

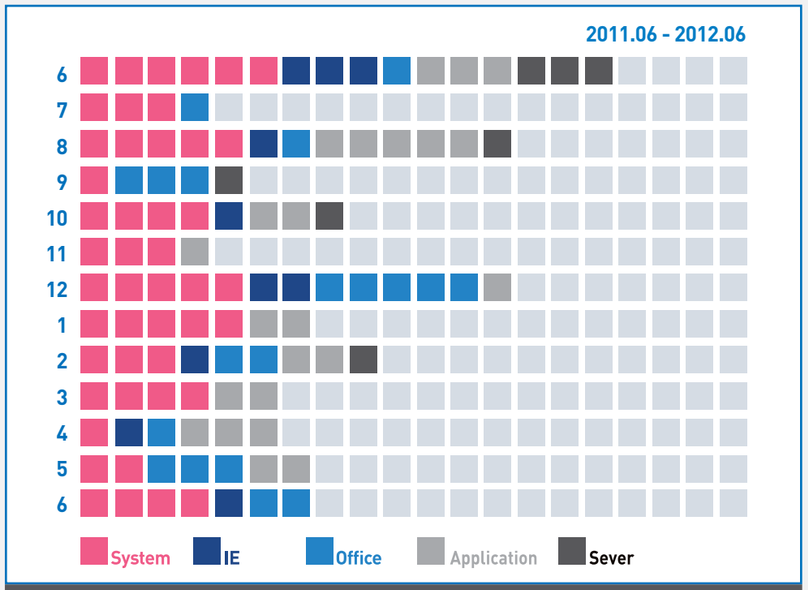
ASD 2.0 MDP engine detects this malware as:
- Dropper/MDP.Document (57)

Security patches to fix this vulnerability are already available.

02. Security Trend
a. Security Statistics

Microsoft Security Updates – June 2012

Microsoft issued 7 security updates this month (3 critical and 4 important).



[Fig. 2-1] MS Security Updates

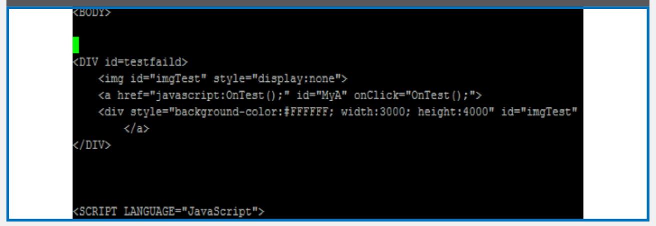
Severity	Vulnerability
Critical	MS12-036: Vulnerabilities in Remote Desktops Could Allow Remote Code Execution
Critical	MS12-037: Cumulative Security Update for Internet Explorer
Critical	MS12-038: Vulnerabilities in .NET Framework Could Allow Remote Code Execution
Important	MS12-039: Vulnerabilities in Lync that Allow Remote Code Execution
Important	MS12-040: Vulnerabilities in Microsoft Dynamics AX Enterprise Portal Could Allow Elevation of Privilege
Important	MS12-041: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege
Important	MS12-042: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege

[Table 2-1] MS Security Updates for June 2012

02. Security Trend
b. Security Issues

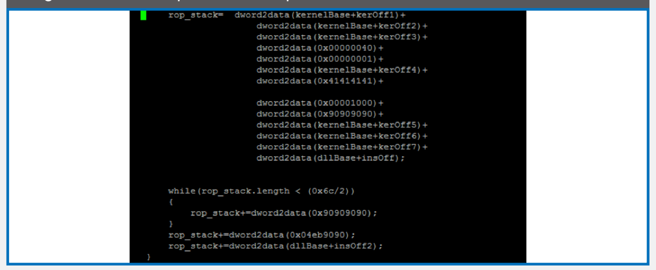
Identical IE ID Attributes Could Allow Remote Code Execution (CVE-2012-1875)

Vulnerability to remote code execution by the identical ID attributes classified as CVE-2012-1875 was disclosed. Its patch was included in MS12-037: Cumulative Security Update for Internet Explorer announced by Microsoft in June. Extra care is needed for this vulnerability, given the rising number of attacks reported. It is a memory corruption bug caused by use-after-free when you use the identical ID attributes for img tags and div tags. A use-after-free bug occurs when you try to use the same value once you used and freed heap memory.


[Fig. 2-2] Identical ID attributes vulnerability codes

CVE-2012-1875 is a vulnerability attacking Internet Explorer 8 only, requiring users of IE8 to take extra precaution.

Codes exploiting the CVE-2012-1875 vulnerability are html based and are using emails or malicious websites for infiltration. The codes adopt the ROP (return-oriented programming) technique, bypassing Windows security mechanisms such as DEP and ASLR. These codes can also attack Windows 7 in addition to Windows XP systems where IE is running.


[Fig. 2-3] ROP Exploit technique

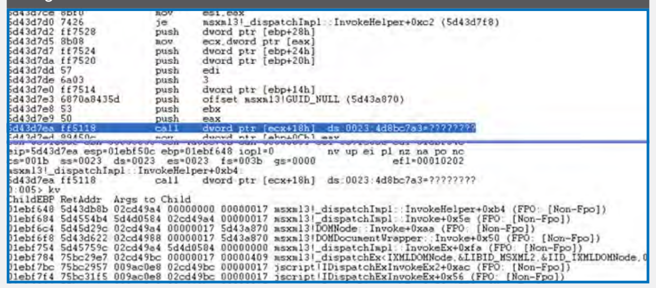
MS12-037: Cumulative Security Update for Internet Explorer includes patches for a total of 13 vulnerabilities. For safe use of the Internet, it is necessary to install these patches before use.

Vulnerability in XML Core Services Could Allow Remote Code Execution (CVE-2012-1889)

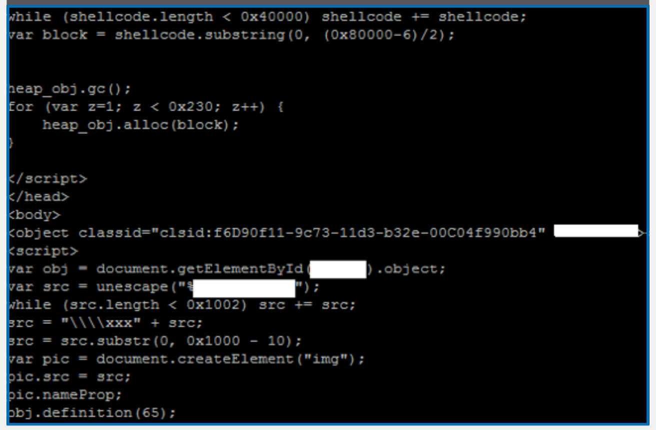
A zero-day attack on MS XML Core Services was reported immediately after the release of June security patches by MS. To tackle this vulnerability, Microsoft announced a Security Advisory.

Microsoft Fix it solutions supplied by Microsoft Security Advisory (2719615) are the only answer since the patches are not yet available. Nevertheless, there are a number of reports on attacks exploiting the vulnerability, and more complex forms of attacks that combine existing vulnerabilities such as Java CVE-2010-0886 and Flash CVE-2011-0611 have also recently been detected.

This vulnerability is exposed when the definition function of msxml makes attempts to access an uninitialized memory object. The memory is then damaged, exposing vulnerability to malicious code execution.


[Fig. 2-4] Msxml3.dll crash screen

Known exploits use F6D90F11-9C73-11D3-B32E-00C04F990BB4 as their CLASS ID value and a definition function in a Heap spray method for their attacks. There are also many variants.



[Fig. 2-5] Xml core services vulnerability attack

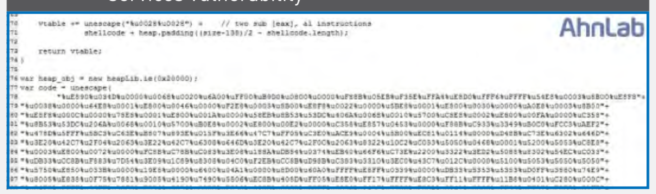
To safeguard against this type of attack, access to unknown and strange-looking websites needs to be minimized. It is also worth considering using web browsers other than IE, such as Chrome and Firefox, which provide quick, automatic security updates.

XML Core Services Vulnerability (CVE-2012-1889) Exploitation on the Rise

In its <Microsoft Security Advisory (2719615) Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution>, Microsoft made public on June 12th, 2012 that unknown zero-day vulnerability had been detected in XML Core Services.

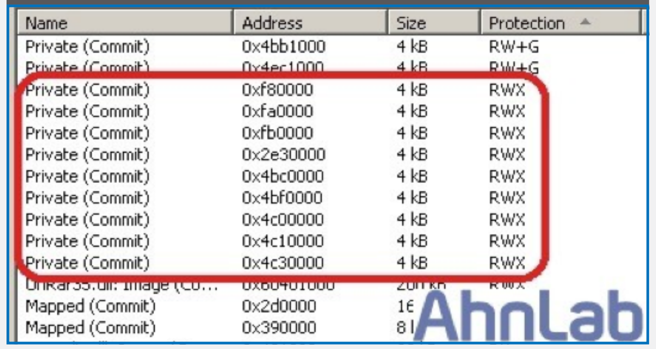
This vulnerability enables the attacker to execute designated codes. It can also be used to attack the Windows operating system and Office Ver. 2003 and 2007 using the XML Core Services. It is a zero-day vulnerability with its security patch yet to be released by Microsoft. Fix it is a temporary solution included in the Microsoft Security Advisory entitled <Microsoft Security Advisory: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution>.

Reports of malicious scripts using XML Core Services are on the rise overseas, keeping the users on the alert. Malicious scripts exploiting the newly found zero-day vulnerability contain shellcodes as shown in [Fig. 2-6].



[Fig. 2-6] Malicious scripts exploiting XML core services vulnerability

Once the shellcodes contained in the scripts are activated, a system in Hong Kong downloads and executes css.exe (32,936 bytes). The file will insert its codes in the thread of explorer.exe, the normal process running on the Windows operating system (See [Fig. 2-7]).



[Fig. 2-7] Malicious codes overwritten on the Explorer.exe process memory

After successful thread injection, queries are transmitted to Google's open DNS server to check whether the infected system can connect to the Internet without a problem. The codes then try to access a designated system in Singapore. The access was foiled at the time of our analysis. Malicious codes collect hardware and operating system information and execute command-line commands information from the compromised system.

The aforementioned XML core services vulnerability is zero-day without a security patch, so users need to be on extra alert. In the meantime, they can install the MS Fix it.

V3 detects malwares exploiting XML Core Services vulnerability as follows:

V3 detects this malware as:

- JS/Agent
- Win-Trojan/Dekor.32936

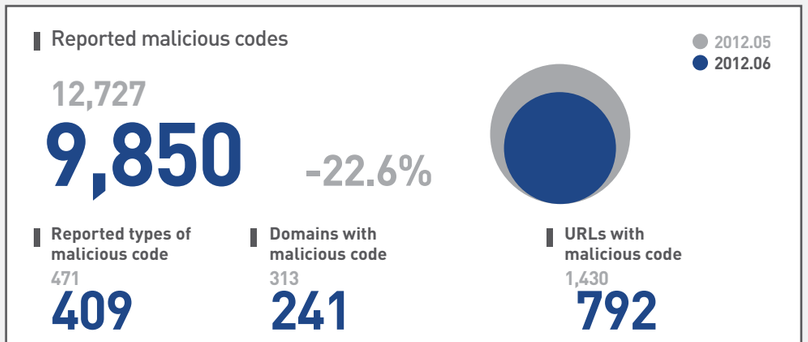
TrusGuard detects this malware as:

- http_ie_heap_spray_attack-4 (HTTP)
- ms_xml_core_

03. Web Security Trend
a. Web Security Statistics

Website Security Summary

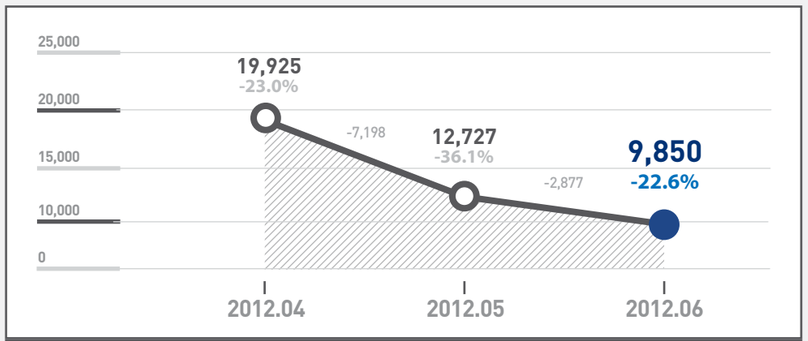
This month, SiteGuard (AhnLab's web browser security service) blocked 9,850 websites that distributed malicious codes. 409 types of malicious code, 241 domains with malicious code and 792 URLs with malicious code were found. The overall numbers decreased slightly from the previous month.



[Table 3-1] June 2012: Website Security Summary

Monthly Change in Blocked Malicious URLs

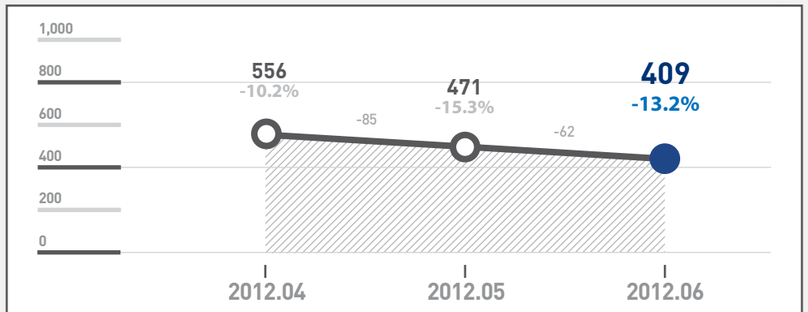
9,850 malicious URLs were blocked in June 2012, a 23% fall from the 12,727 blocked in the previous month.



[Fig. 3-1] Monthly Change in Blocked Malicious URLs

Monthly Change in the Number of Reported Malicious Code Types

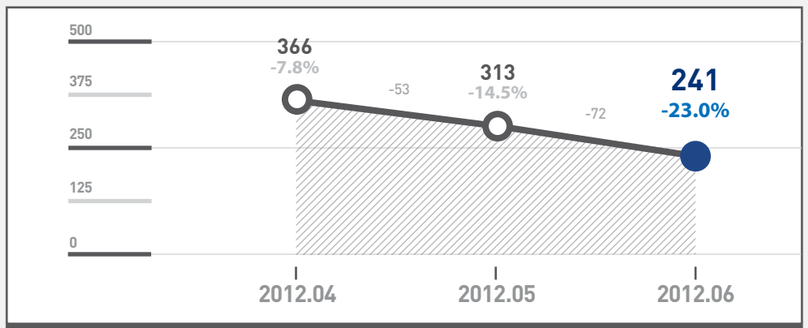
409 malicious code types were reported in June 2012, a 13% fall from the 471 reported in the previous month.



[Fig. 3-2] Monthly Change in the Number of Reported Malicious Code Types

Monthly Change in Domains with Malicious Code

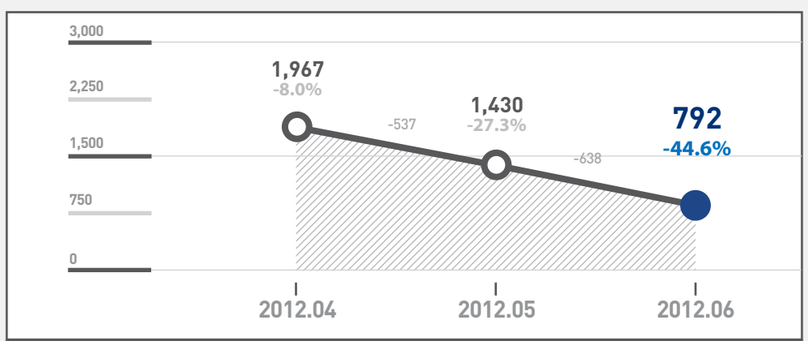
241 domains were found with malicious codes in June 2012, a 23% fall from the 313 found in the previous month.



[Fig. 3-3] Monthly Change in Domains with Malicious Code

Monthly Change in URLs with Malicious Code

792 URLs were found with malicious codes in June 2012, a 45% fall from the 1,430 found in the previous month.



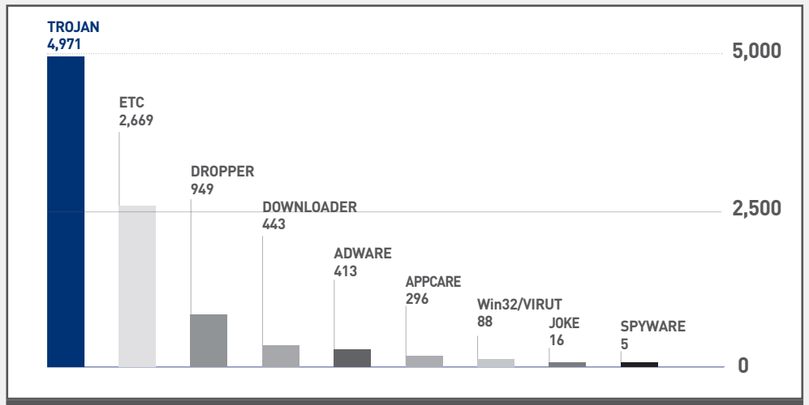
[Fig. 3-4] Monthly Change in URLs with Malicious Code

Top Distributed Types of Malicious Code

For June 2012, Trojan was the top distributed type of malicious code with 4,971 (50.5%) cases reported, followed by dropper with 949 (9.6%) cases reported.

TYPE	Reports	Percentage
TROJAN	**4,971**	**50.5%**
DROPPER	949	9.6%
DOWNLOADER	443	4.5%
ADWARE	413	4.2%
APPCARE	296	3.0%
Win32/VIRUT	88	0.9%
JOKE	16	0.2%
SPYWARE	5	0.1%
ETC	2,669	27.0%
	9,850	**100.0%**

[Table 3-2] Top Distributed Types of Malicious Code



[Fig. 3-5] Top Distributed Types of Malicious Code

Top 10 Distributed Malicious Codes

For June 2012, Win-Trojan/Adload.651264.W was the top distributed malicious code with 1,245 cases reported, followed by Trojan/Win32.BHO with 914 cases reported.

Ranking ↑↓		Malicious Code	Reports	Percentage
1	**NEW**	**Win-Trojan/Adload.651264.W**	**1,245**	**22.9%**
2	NEW	Trojan/Win32.BHO	914	16.8%
3	NEW	Win32/Parite	774	14.3%
4	-3	Trojan/Win32.HDC	489	9.0%
5	-1	ALS/Qfas	416	7.7%
6	-4	Downloader/Win32.Korad	351	6.5%
7	-4	ALS/Bursted	346	6.4%
8	NEW	Dropper/Onlinegamehack.123904.B	318	5.9%
9	-3	Trojan/Win32.SendMail	295	5.4%
10	NEW	Win-AppCare/Wlwhs.53248	281	5.1%
			5,429	**100.0%**

[Table 3-3] Top 10 Distributed Malicious Codes

2. Security Trends – Q2 2012

01. Malicious Code Trend

a. Malicious Code Statistics

Q2 2012 Top 20 Malicious Code Reports

Statistics collected by the ASEC show that 35,005,368 malicious codes were reported in Q2 2012, recording a decrease of 6,429,513 cases from 41,434,881 in Q1 2012. The most frequently reported malicious code was Mov/Cve-2011-2140, followed by Trojan/Win32.Gen and Trojan/Win32.adh, respectively. 10 new malicious codes were reported this month (See [Table 4-1]).

Ranking ↑↓		Malicious Code	Reports	Percentage
1	NEW	Mov/Cve-2011-2140	1,744,492	12.8 %
2	▼1	Trojan/Win32.adh	1,522,315	11.2 %
3	▲1	Trojan/Win32.Gen	1,347,733	9.9 %
4	▲2	Textimage/Autorun	997,257	7.3 %
5	▲11	ASD.PREVENTION	948,088	7.0 %
6	▼4	JS/Agent	926,920	6.8 %
7	▼2	Malware/Win32.generic	882,361	6.5 %
8	NEW	Trojan/Win32.bho	756,408	5.6 %
9	▼1	Adware/Win32.korad	634,390	4.7 %
10	NEW	Mov/Cve-2012-0754	609,183	4.5 %
11	▲2	Downloader/Win32.agent	495,460	3.6 %
12	▼3	Trojan/Win32.agent	392,251	2.9 %
13	NEW	Als/Bursted	350,695	2.6 %
14	NEW	Trojan/Win32.sasfis	323,877	2.4 %
15	NEW	Malware/Win32.suspicious	316,990	2.3 %
16	NEW	JS/Exploit	291,183	2.1 %
17	NEW	Downloader/Win32.opentab	286,342	2.1 %
18	NEW	Adware/Win32.winagir	259,190	2.0 %
19	NEW	RIPPER	257,582	1.9 %
20	▼5	Java/Agent	245,185	1.8 %
			13,587,902	100 %

[Table 4-1] Q2 2012 Top 20 Malicious Code Reports

Q2 2012 Top 20 Distributed Malicious Codes

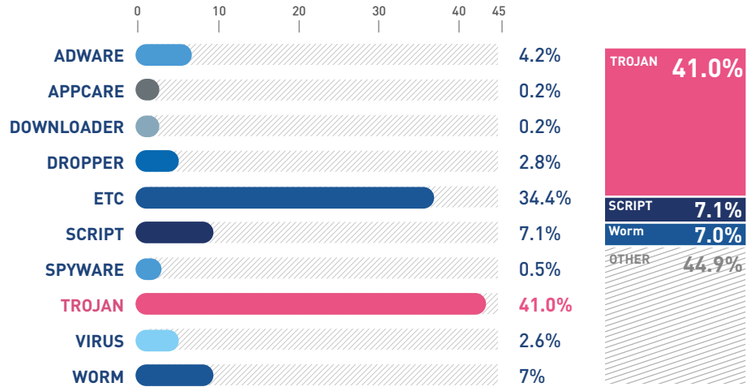
The table below shows the percentage breakdown of the top 20 malicious code variants reported this month. For Q2 2012, Trojan/Win32 was the most reported malicious code, representing 27.2% (6,398,533 reports) of the top 20 malicious code variants, followed by Adware/Win32 (1,864,466 reports) and Mov/Cve-2011-2140 (1,744,492 reports).

Ranking ↑↓		Malicious Code	Reports	Percentage
1	—	Trojan/Win32	6,398,533	27.2%
2	—	Adware/Win32	1,864,466	7.9%
3	NEW	Mov/Cve-2011-2140	1,744,492	7.4%
4	▲3	Downloader/Win32	1,323,903	5.6%
5	▼1	Win-Trojan/Agent	1,319,338	5.6%
6	—	Malware/Win32	1,284,901	5.5%
7	▲1	Win-Trojan/Downloader	1,038,556	4.4%
8	▼3	Win-Adware/Korad	1,032,315	4.4%
9	—	Textimage/Autorun	997,461	4.2%
10	▼7	JS/Agent	953,130	4.1%
11	NEW	ASD	948,088	4.0%
12	▼2	Win-Trojan/Onlinegamehack	866,391	3.7%
13	NEW	Mov/Cve-2012-0754	609,183	2.6%
14	▲2	Win-Trojan/Korad	514,827	2.2%
15	▼4	Backdoor/Win32	511,507	2.2%
16	▼3	Win32/Conficker	482,947	2.0%
17	▼5	Win32/Virut	447,707	1.9%
18	NEW	Win-Trojan/Rootkit	429,006	1.8%
19	▼1	Dropper/Win32	388,597	1.7%
20	▼5	Win32/Kido	378,262	1.6%
			23,533,610	100.0%

[Table 4-2] Q2 2012 Top 20 Distributed Malicious Codes

Primary Malicious Code Types Found in Q2 2012

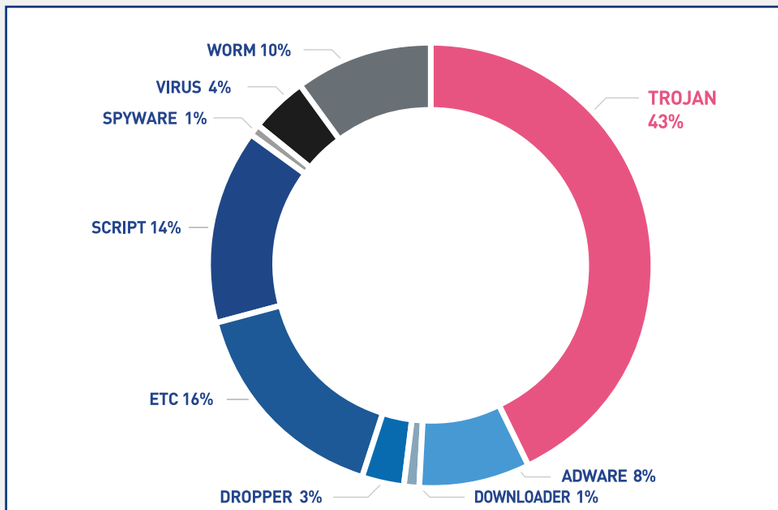
The chart below categorizes the top malicious codes reported during the second quarter of this year. For Q2 2012, Trojan was the most reported new malicious code, representing 41% of the top reported new malicious codes, followed by script (7.1%) and worm (7%).



[Fig. 4-1] Q2 2012 Primary Malicious Code Type Breakdown

Q2 2012 New Malicious Code Type Breakdown

For Q2 2012, Trojan was the most reported new malicious code type, representing 43% of the top reported new malicious code types, followed by script (14%) and worm (10%) respectively.



[Fig. 4-2] Q2 2012 New Malicious Code Type Breakdown

New Malicious Code Types Found in Q2 2012

The table below shows the percentage breakdown of the top 20 new malicious codes reported this quarter. For Q2 2012, Textimage/Autorun (995,935 reports) was the most reported new malicious code, representing 20.7% of the top reported new malicious codes, followed by JS/Agent (926,910 reports).

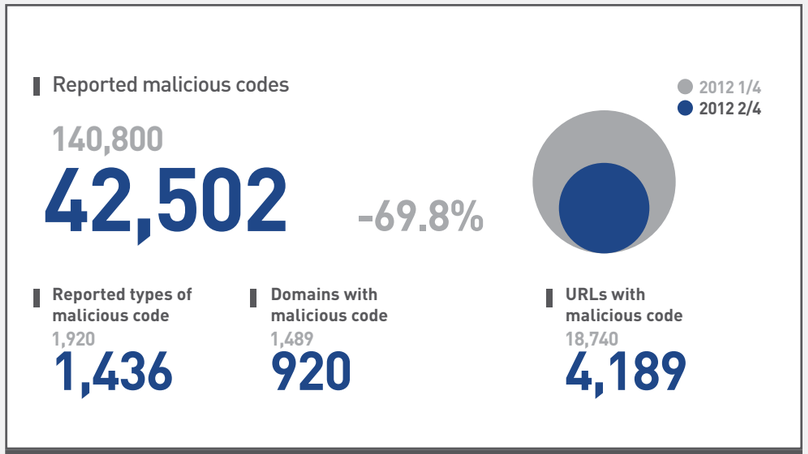
Ranking ↑↓	Malicious Code	Reports	Percentage
1	TextImage/Autorun	995,935	20.7%
2	JS/Agent	926,910	19.3%
3	ALS/Bursted	350,695	7.3%
4	JS/Exploit	291,180	6.1%
5	JAVA/Agent	238,669	5.0%
6	HTML/IFrame	190,330	4.0%
7	Win32/Olala.worm.57344	183,916	3.8%
8	Win-Trojan/Rootkit.28928.D	176,624	3.7%
9	Win32/Virut.F	164,293	3.4%
10	Win32/Induc	158,390	3.3%
11	Win-Trojan/Dllbot.132096.C	147,990	3.1%
12	Win-Trojan/Rootkit.28928.C	147,753	3.1%
13	JAVA/Cve-2011-3544	127,809	2.7%
14	Win-Trojan/Agent.465408.T	115,472	2.4%
15	Win32/Kido.worm.156691	105,998	2.2%
16	Win32/Conficker.worm.162155	100,797	2.1%
17	Win-Trojan/Korad.311296	100,328	2.1%
18	Java/Exploit	97,514	2.0%
19	Win32/Virut.E	94,464	1.9%
20	HTML/Agent	92,735	1.8%
		4,807,802	100.0%

[Table 4-3] Q1 2012 Top 20 New Malicious Code Reports

02. Web Security Trend
a. Web Security Statistics

Website Security Summary

During the second quarter of 2012, SiteGuard (AhnLab's web browser security service) blocked 42,502 websites that distributed malicious codes, a 70% fall from the 140,800 blocked in the first quarter. 1,436 malicious code types were reported, a 25% fall from the 1,920 reported in the previous quarter. The number of reported domains with malicious code decreased to 920, a 38% drop from the 1,489 of the previous quarter. The number of reported URLs with malicious code decreased 78% to 4,189 from the 18,740 of the previous quarter.



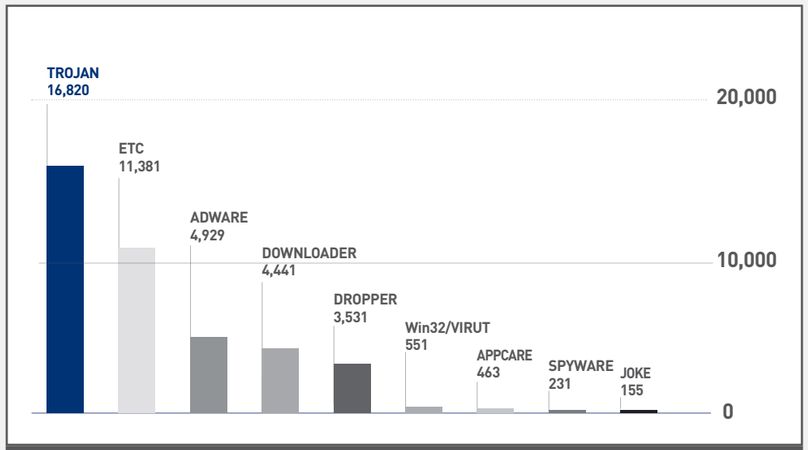
[Table 5-1] Q2 2012 Website Security Summary

TYPE	Reports	Percentage
TROJAN	**16,820**	**39.6%**
ADWARE	4,929	11.6%
DOWNLOADER	4,441	10.4%
DROPPER	3,531	8.3%
Win32/VIRUT	551	1.3%
APPCARE	463	1.1%
SPYWARE	231	0.5%
JOKE	155	0.4%
ETC	11,381	26.8%
	42,502	**100.0%**

[Table 5-2] Q2 2012 Top Distributed Types of Malicious Code

Q2 2012 Top Distributed Types of Malicious Code

For Q2 2012, Trojan was the top distributed type of malicious code with 16,820 (39.6%) cases reported, followed by adware with 4,929 (11.6%) cases reported.



[Fig. 5-1] Q2 2012 Top Distributed Types of Malicious Code

Q2 2012 Top 10 Distributed Malicious Codes

For Q2 2012, Downloader/Win32.Korad was the top distributed malicious code with 2,361 cases reported, followed by Trojan/Win32.HDC with 2,165 cases reported.

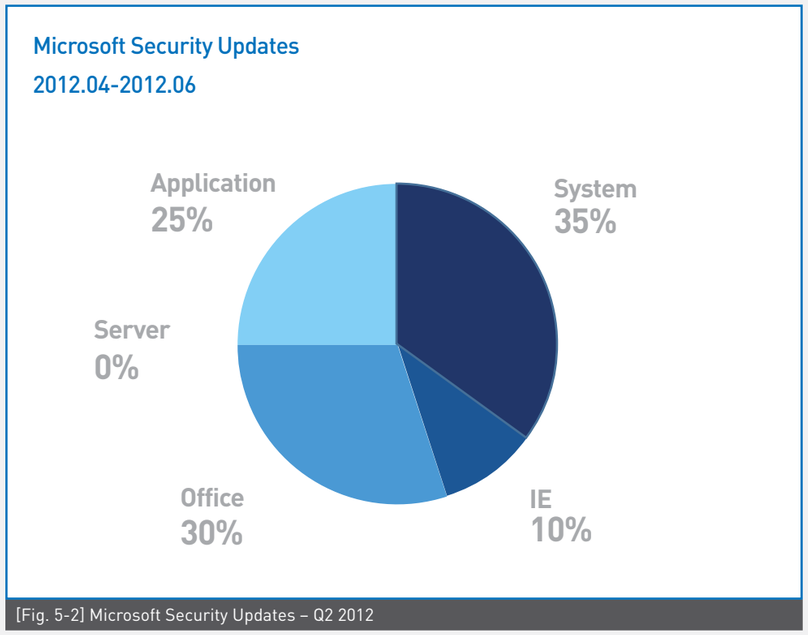
Ranking	↑↓	Malicious Code	Reports	Percentage
1	**2**	**Downloader/Win32.Korad**	**2,361**	**15.0%**
2	NEW	Trojan/Win32.HDC	2,165	13.8%
3	3	Win-Adware/ToolBar.Cashon.308224	1,848	11.8%
4	NEW	ALS/Bursted	1,651	10.5%
5	NEW	ALS/Qfas	1,360	8.7%
6	-2	Downloader/Win32.Totoran	1,353	8.6%
7	-2	Dropper/Small.Gen	1,298	8.3%
8	NEW	Win-Trojan/Adload.651264.W	1,245	7.9%
9	NEW	Trojan/Win32.ADH	1,236	7.9%
10	NEW	Unwanted/Win32.WinKeyfinder	1,181	7.5%
			15,698	**100.0%**

[Table 5-3] Q2 2012 Top 10 Distributed Malicious Codes

03. Security Trend
a. Security Statistics

Microsoft Security Updates – Q2 2012

Microsoft released 20 security updates this quarter. A reduced number of security patches were released and the vulnerability in the system area still remains on top of the list from the previous quarter, representing 35%. May and June each had 7 security updates, most of which were Critical. Cumulative Security Updates are provided in the June batch, installation of which is strongly recommended for Internet users. Given the consistent reports of MS Office vulnerabilities, the users must take precautions in opening any Office files attached to emails.



[Fig. 5-2] Microsoft Security Updates – Q2 2012

3. 2012 First Half Security Trends

The first half of 2012 went smoothly without the witnessing of huge security incidents such as large-scale DDoS attacks or disclosure of internal information reported during the same period last year. What is characteristic of this year, however, is the variety of channels through which malicious codes are distributed and the rise of APT-type attacks targeting particular groups.

1. Rise of APT (Advanced Persistent Threast) Attacks to Steal Information

An outstanding trend in the security threats reported during the first half of 2012 is the increase of APT attacks designed to steal internal information. Such APT attacks against internal systems were mostly made by using files with vulnerabilities attached to emails.

Such emails regularly contain a social issue or an interesting topic in the message, attracting the user to open the attachment. Attackers take advantage of vulnerabilities in the digital documents written in MS Word, Adobe Reader or Hangul to corrupt the system. Most of the malicious codes contaminated by vulnerable digital documents are designed to remotely control and monitor the attacked computer to steal important internal information.

2. Consistent Reports of Malware to Steal Personal Information

Online game hacking malware keeps spawning its variants, stealing personal information from vulnerable websites every weekend. Such a phenomenon has almost become a category under the domestic security threats.

Online game malwares bypass detection from security software by patching or altering Windows system files, concurrently making continued efforts to neutralize security software.

The first half of 2012 saw the emergence of malicious codes designed to steal personal financial information used for online banking. By redirecting users to fraudulent phishing websites of financial institutions, such malwares tried to steal banking information such as passwords for security cards and public certificates.

Personal information used to log in to top web portals was also exposed to malicious attacks. Attackers faked login windows to the portals or used keylogging, which snatches what the user types in to steal user accounts and passwords.

Unlike the known malwares devised to steal items of online games, the new malicious attacks

targeting personal information are designed to make direct financial profits or secure personal information to access websites later without user permission.

3. Functions of Malware Exploiting Application Vulnerabilities

Vulnerabilities in widely used applications were consistently exploited by attackers during the first half of 2012. Malwares confined to a specific area and distributed within a specific country also became prevalent.

General applications under attack are broken down into digital documents, web browsers and web applications.

Further down, among digital documents, Microsoft Word (DOC) and Adobe Reader (PDF) are primary targets. When it comes to web browsers, malwares are mostly found in Internet Explorer. Web application targets are mostly Adobe Flash Player vulnerabilities.

However, general application vulnerabilities that begun to be exploited in Korea during the first half of 2012 include MS12-004 vulnerabilities in Windows Media and CVE-2012-0507 vulnerabilities in Java. The first half also saw a number of attacks exploiting vulnerabilities in Hangul (HWP), Korean software used only domestically.

Digital document applications such as Microsoft Word, Adobe Reader and Hangul are more vulnerable to APT-type attacks.

However, web browsers and applications such as Internet Explorer, Adobe Flash Player and Java are more susceptible to malicious attacks to steal online game information of personal computer users. In particular, the XML core services vulnerability (CVE-2012-1889) of Microsoft has been persistent for more than one month since its identification of May 30th as zero-day. This also is used to steal personal information for online gaming.

4. Mobile Malware Diversifies its Distribution Channels

Android malware identified during the first half of 2012 continues to rise in numbers. Android malwares reported during the first half of 2012 are distributed through different channels from those reported in the second half of 2011, although they are consistently disguised as legitimate Android apps.

Existing Android malwares thrived on either Google's app store or 3rd party app stores operating on the Internet. However, new malwares were detected in fake app stores or well-known app distribution sites made by malicious attackers, and Twitter and other SNS sites were also used for their circulation.

This is due to the tightened security checks in Google on Android apps circulating through app stores. In view of a number of visitor comments available in the widely used 3rd party app stores, Android malware attackers found it hard to depend on existing channels. This is why Android malware attackers make continued efforts to develop new distribution channels.

[Fig. 7-4] Android malwares being distributed in a fake Android market

5. Emergence of Phishing Sites Targeting both PC and Mobile

Another trend that stood out during the last half is the prevalence of phishing websites. What made the new phishing sites distinguishable were their sophisticated designs customized for different terminals from smartphone to personal computer.

One of the most widely used attacks was to forward website addresses via SMS messages on a smartphone. Phishing websites that fit the mobile web browser were also made.

Phishing website makers are believed to have a good understanding of the Korean society and culture, taking advantage of the fact that smartphones are widely used for personal data services such as email, shopping, and online banking in Korea.

VOL. 30
ASEC REPORT Contributors

Contributors

Principal Researcher	Jeong-hyeong Lee
Senior Researcher	Chang-yong Ahn
Senior Researcher	Young-jun Jang
Assistant Researcher	Young-jo Moon
Researcher	Min-cheol Kang

Contributing Researchers

ASEC Team
SiteGuard Team

Editor in Chief

Senior Researcher	Hyung-bong Ahn

Editor	Sales Marketing Team
Design	UX Design Team

Reviewer

CTO	Si-haeng Cho

Publisher

AhnLab, Inc.
673, Sampyeong-dong,
Bundang-gu, Seongnam-si,
Gyeonggi-do, 463-400,
South Korea
T. +82-31-722-8000
F. +82-31-722-8901

AhnLab