ASEC REPORT

VOL.26 | 2012.03

AhnLab Monthly Security Report

1. Malicious Code Trend
2. Security Trend
3. Web Security Trend

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 TREND – FEB. 2012

01. Malicious Code Trend

a. Malicious Code Statistics

Top 20 Malicious Code Reports

Statistics collected by the ASEC show that 13,663,774 malicious codes were reported in February 2012. This is a decrease of 287,127 from the 13,950,901 reported in the previous month (Fig. 1-1). As with the previous month, JS/Agent was again the most reported malicious code this month, followed by Malware/Win32.generic and Trojan/Win32.adh, respectively. In addition, 5 new malicious codes were reported this month ([Table 1-1]).

[Fig. 1-1] Monthly Malicious Code Reports

Ranking	↑↓	Malicious Code	Reports	Percentage
1	—	JS/Agent	634,569	12.1%
2	▲4	Malware/Win32.generic	605,987	11.6%
3	—	Trojan/Win32.adh	515,485	9.8%
4	—	Trojan/Win32.Gen	476,930	9.1%
5	▲2	Trojan/Win32.fakeav	399,725	7.6%
6	▼1	Textimage/Autorun	373,495	7.1%
7	▼5	Trojan/Win32.hdc	372,184	7.1%
8	NEW	VBS/Agent	184,235	3.5%
9	NEW	Html/Downloader	176,299	3.4%
10	▼2	Adware/Win32.korad	173,314	3.3%
11	—	Win-Trojan/Agent.465408.T	162,671	3.1%
12	▼2	Trojan/Win32.agent	159,320	3.0%
13	NEW	Downloader/Win32.agent	151,895	2.9%
14	▼2	Trojan/Win32.genome	148,405	2.8%
15	NEW	Win-Adware/Korad.1038848	144,429	2.8%
16	—	Html/Iframe	120,890	2.4%
17	▲3	Backdoor/Win32.asper	116,878	2.3%
18	▲1	Packed/Win32.morphine	108,609	2.1%
19	NEW	Html/Agent	107,304	2.0%
20	▼5	ASD.PREVENTION	105,767	2.0%
			5,238,391	100.0%

[Table 1-1] Top 20 Malicious Code Reports

Top 20 Distributed Malicious Codes

The table below shows the percentage breakdown of the top 20 malicious code variants reported this month. For February 2012, Trojan/Win32 is the most reported malicious code, representing 29.1% (2,615,181 reports) of the top 20 malicious code variants, followed by Win-Trojan/Agent (786,315 reports) and Malware/Win32 (678,114 reports).

Ranking	↑↓	Malicious Code	Reports	Percentage
1	—	Trojan/Win32	2,615,181	29.1%
2	▲2	Win-Trojan/Agent	786,315	8.8%
3	▲3	Malware/Win32	678,114	7.5%
4	▲4	Win-Adware/Korad	653,582	7.3%
5	▼3	JS/Agent	635,895	7.1%
6	▼3	Adware/Win32	481,296	5.4%
7	▼2	Downloader/Win32	442,207	4.9%
8	▼1	Textimage/Autorun	373,568	4.2%
9	—	Win-Trojan/Downloader	336,090	3.7%
10	—	Win-Trojan/Onlinegamehack	308,737	3.4%
11	NEW	Win-Trojan/Korad	212,842	2.4%
12	▼1	Backdoor/Win32	209,213	2.3%
13	▼1	Win32/Virut	186,558	2.1%
14	NEW	VBS/Agent	184,236	2.1%
15	NEW	Html/Downloader	176,299	2.0%
16	▼3	Win32/Conficker	175,937	2.0%
17	▼2	Win32/Autorun.worm	135,790	1.5%
18	▼1	Win32/Kido	135,597	1.5%
19	▼1	Packed/Win32	134,559	1.4%
20	—	Html/Iframe	120,890	1.3%
			8,982,906	100.0%

[Table 1-2] Top 20 Distributed Malicious Codes

Top 20 New Malicious Code Reports

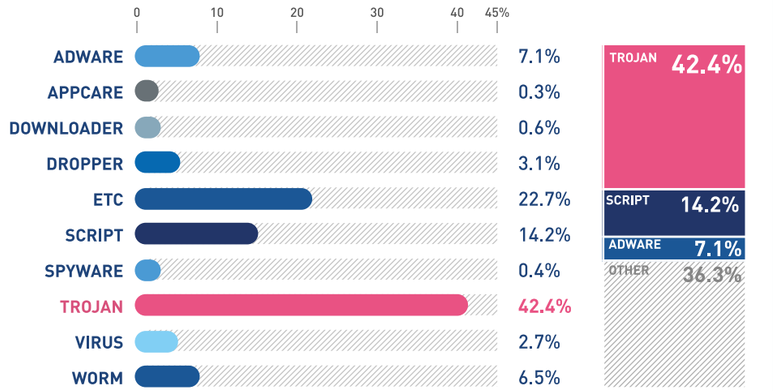
The table below shows the percentage breakdown of the top 20 new malicious codes reported this month. For February 2012, Win-Adware/KorAd.1038848 is the most reported new malicious code, representing 20% (144,429 reports) of the top 20 new malicious codes, followed by Win-Trojan/Korad.450560.C (54,806 reports).

Ranking	↑↓	Malicious Code	Reports	Percentage
1		Win-Adware/KorAd.1038848	144,429	20.0%
2		Win-Trojan/Korad.450560.C	54,806	7.6%
3		Win-Adware/KorAd.1491456	50,617	7.0%
4		Win-Adware/KorAd.1277440	41,880	5.8%
5		Win-Adware/Pop2Click.591872	39,984	5.5%
6		Win-Trojan/Agent.959536	37,382	5.2%
7		Win-Trojan/Korad.796160	35,776	5.0%
8		Win-Adware/KorAd.229376.E	33,735	4.7%
9		Win-Trojan/Korad.446464.B	33,320	4.6%
10		Win-Trojan/Agent.1738240.J	30,964	4.3%
11		Win-Trojan/Fakeav.797696.B	27,146	3.8%
12		Win-Adware/Shortcut.316928	26,772	3.7%
13		Win-Adware/KorAd.454656.J	24,315	3.4%
14		Win-Trojan/Agent.416880	22,681	3.1%
15		Win-Adware/KorAd.417280	20,823	2.9%
16		Win-Trojan/Startpage.871016	20,761	2.9%
17		Win-Trojan/Agent.2008340.B	20,467	2.8%
18		Win-Trojan/Agent.946256	20,388	2.8%
19		Win-Adware/KorAd.61440	18,167	2.5%
20		Win-Trojan/Korad.458752.C	17,851	2.4%
			722,264	100.0%

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

Breakdown of Primary Malicious Code Types

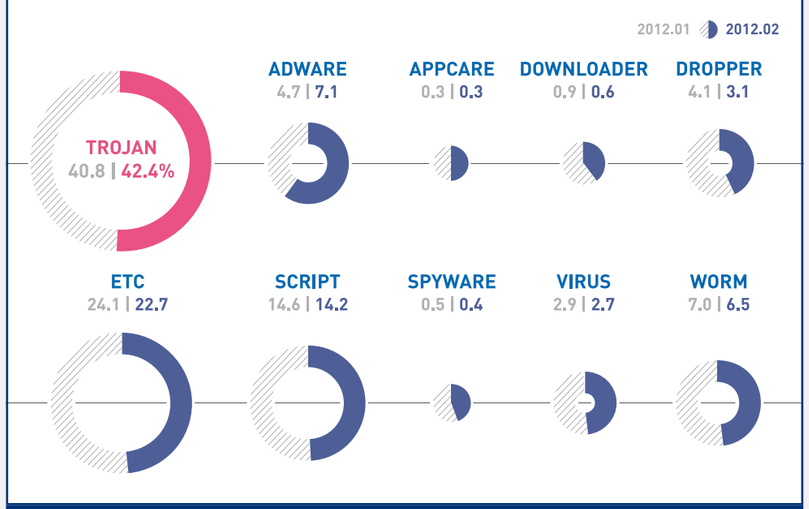
The chart below categorizes the top malicious codes reported this month. For February 2012, Trojan is the most reported malicious code, representing 42.4% of the top reported malicious codes, followed by script (14.2%) and adware (7.1%).



[Fig. 1-2] Breakdown of Primary Malicious Code Types

Monthly Breakdown of Primary Malicious Code Types

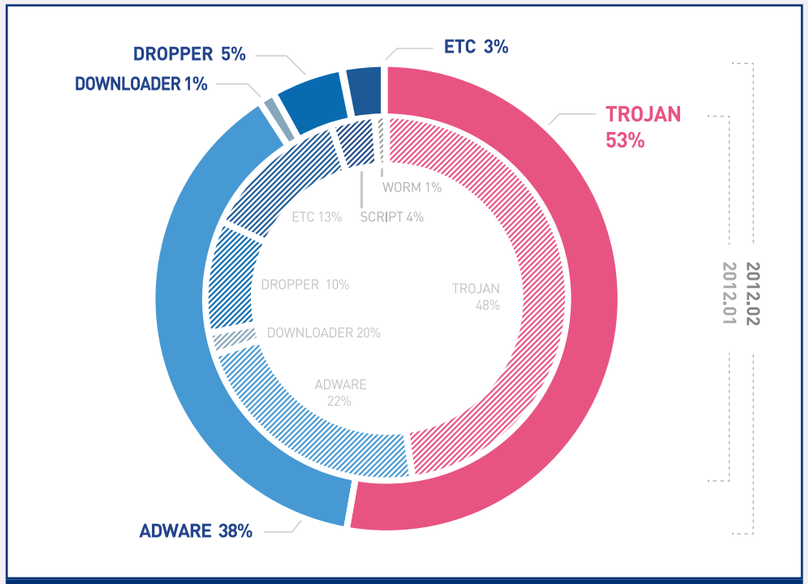
Fig. 1-3 represents the comparison of this month's malicious codes with those of last month. Compared to last month, the number of Trojan and adware increased, whereas the number of script, worm, dropper, virus, downloader and spyware decreased. The number of appcare is similar to that of the previous month.



[Fig. 1-3] Monthly Breakdown of Primary Malicious Code Types (Feb. 2012 vs. Jan. 2012)

Breakdown of New Malicious Code Types

For February 2011, Trojan is the most reported new malicious code, representing 53% of the top reported new malicious codes, followed by adware (38%) and dropper (5%).



[Fig. 1-4] Breakdown of New Malicious Code Types

01. Malicious Code Trend
b. Malicious Code Issues

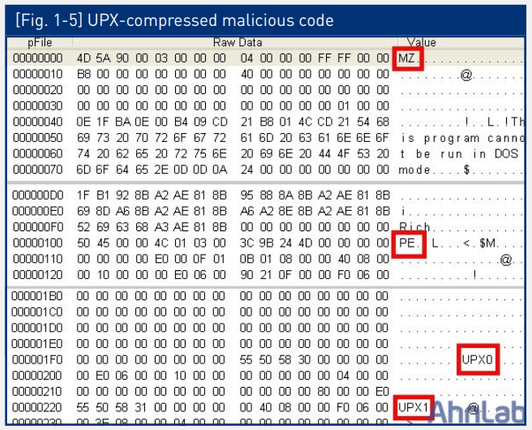
A malicious code that steals all document files on a PC

A malicious code disguised as a FedEx invoice e-mail that steals all MS Word files (doc, docx) and MS Excel files (xls, xlsx) on a victim's PC has been reported. The e-mail is sent with the subject "Your package is available for pickup.NO#8248." While home users in Korea are not at great risk from this malicious code as e-mail written in foreign languages is identified as spam, users who send and receive high volumes of e-mail in English at work and those who frequently use FedEx international freight service should exercise caution.

There have been other cases of malicious codes distributed via a fake logistics service e-mail in the past. The names of well-known global logistics service providers such as DHL, UPS and FedEx have been used to distribute rogue anti-viruses.

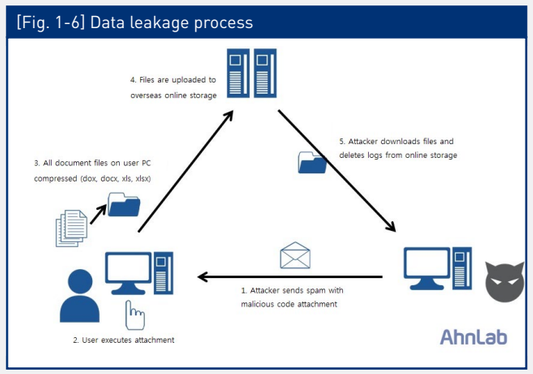
The name of the malicious code attached to the fake FedEx e-mail is FedEx_Invoice.exe. If the file is executed, a malicious executable file with a "txt" extension deceives the user into thinking that it is a safe and legitimate file. As seen in Fig. 1-5, it has been compressed more than 2 times using UPX to make analysis difficult.

[Fig. 1-5] UPX-compressed malicious code



When the user executes the attached file, all MS Word and Excel files on the PC are compressed and uploaded to online storage overseas. The online storage is run by a company called Sen****ce, a legitimate online storage service provider.

[Fig. 1-6] Data leakage process



When the malicious code is executed, it searches the entire computer to find document files. The document files found are then saved as a .zip file with a random name in c:\Documents and Settings\Administrator\Local Settings\Temp. Fig. 1-7 shows the .zip file of the stolen document files generated when the malicious code is executed.

[Fig. 1-7] Randomly named .zip file of stolen document files

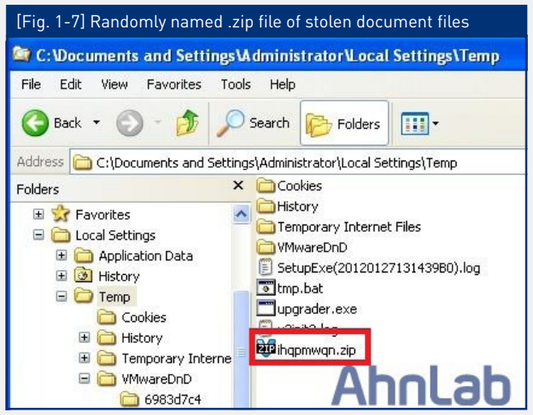
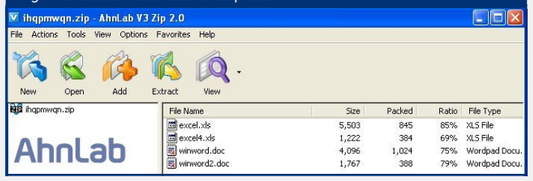


Fig. 1-8 shows a list of the folders and files in the .zip file. Note that document files in divided disks' partitions and additional disk drives (including external disk drives) are also included.

Fig. 1-8 Document files in .zip file



Once the document files are compressed, a transmission log is left on a server as shown in Fig. 1-9 before the compressed document files are sent to the online storage. It is speculated that a transmission log is created to notify the attacker that the user's PC has been attacked and to collect statistics.

[Fig. 1-9] A packet to leave a transmission log on a server

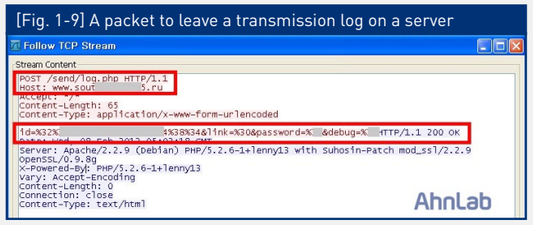
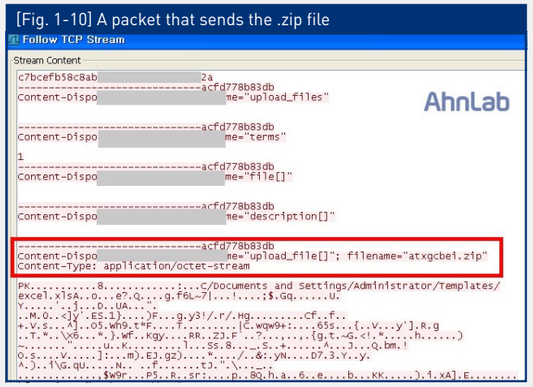


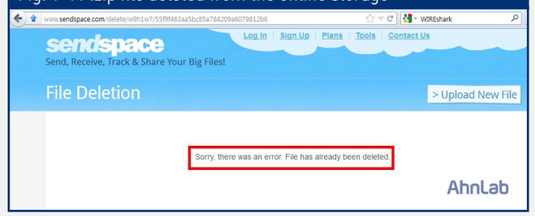
Fig. 1-10 shows a packet that sends the .zip file. This malicious code performs searching, compressing and sending of document files. The malicious code creator can be assumed to have a good understanding of the file upload/download structure of the online storage provider used in this attack.

[Fig. 1-10] A packet that sends the .zip file



When connection to the upload address identified through analyzing the transmission packet is attempted, a message saying that the file has been deleted and cannot be found is displayed as shown in Fig. 1-11. It is speculated that this is due to the stolen file's deletion from the online storage after being downloaded by the attacker.

Fig. 1-11 .zip file deleted from the online storage



The majority of computer users store most document files on their work PCs. Also, many users do not password-lock document files, so they are vulnerable to data leakage attack via junk mail, messaging, social engineering, and malicious code infection.

This malicious code is different from the form of APT (Advanced Persistent Threat) attack which has increasingly become an issue for many organizations. APT attacks are focused on specific targets and APT attackers patiently coordinate the efforts of identifying and exploiting existing vulnerabilities to penetrate the target organization's network. Conversely, this newly discovered malicious code is sent to random people, and steals all document files on victims' PCs.

V3 detects this malicious code as:
- Spyware/Win32.Zbot (2012.02.07.03)
- Trojan/Win32.Gen (2012.02.14.00)

8 ways to keep your computer free from malicious codes

1. Use a trustworthy anti-spam program to filter out spam /junk mail.
2. Don't open an e-mail from an unknown sender or with a suspicious subject; delete it.
3. Update anti-virus programs to the latest version and use real-time protection.
4. Don't execute files attached to incoming e-mail immediately. Execute them after scanning with an anti-virus program.
5. Don't click on suspicious website links included in e-mail.
6. Install all latest security updates for Windows, IE and MS Office.
7. Don't store important document files on PCs.
8. Develop a habit of password-locking important document files.

Someone could be watching you. Webcam-activating malicious code

What if you were being watched and you didn't know about it? Indeed, it is an alarming thought. A malicious code that spies on the user of an infected PC through a connected webcam has been discovered. Unlike malicious codes that steal data or interfere with system operation, this malicious code poses a grievous threat to the privacy of victims.

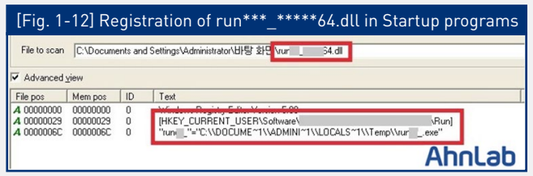
The malicious code then tries to connect to a server located in Russia; it seems to have originated from Russia. No reports of this malicious code have been made in Korea as of yet. However, users of foreign websites are advised to take precautions.

When infected, it creates additional files in the following location:

C:\Documents and Settings\Administrator\Local Settings\Temp\
Run***_*****64.dll, run***_.exe, run***_.log, run***_dll.sid, run***_.bat

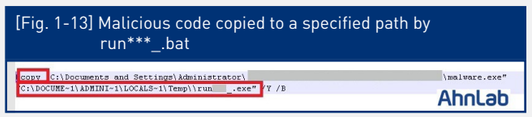
"run***_64.dll" has a command in the registry for adding itself to Startup programs. While its extension is dll, it is actually a .txt file. Once registered in startup, the malicious code will be executed every time Windows starts up.

[Fig. 1-12] Registration of run***_*****64.dll in Startup programs



"run***_.bat" copies the initially executed malicious code to the path C:\Documents and Settings\Administrator\Local Settings\Temp\. Fig. 1-13 shows the malicious code copied into the file.

[Fig. 1-13] Malicious code copied to a specified path by run***_.bat

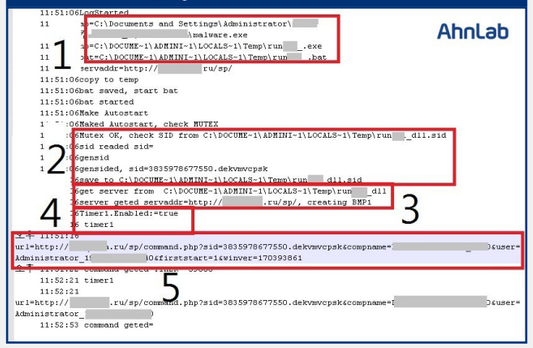


The "run***_dll.sid" file saves a randomly generated character string to identify an infected PC.

[Fig. 1-14] Identifier saved by run***_dll.sid for identification of attacked PCs

The run***_.log file generates log files recording the activities of the malware.

[Fig. 1-15] Malicious code functioning process recorded by run***_.log

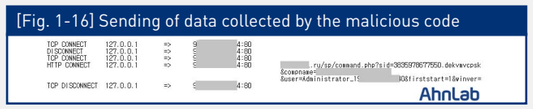


The following is the functioning process recorded in the log file.

- Malicious code is copied to C:\Documents and Settings\Administrator\Temp\
- Identifier of infected PC is generated and saved as a file
- Target server (for sending captured images to) is specified and captured images are saved as BMP files
- Timer set (59000ms = 1 minute)
- Infected PC's OS version, user name, PC name and SID data are sent to a designated server
- Stay undetected and get the next command from the server

Fig. 1-15 shows the server URL with the domain .ru, which represents Russia. The network is connected to the malicious code server and data is sent at 1-minute intervals.

[Fig. 1-16] Sending of data collected by the malicious code



In summary, this malicious code takes a photograph every 1 minute using a webcam connected to the user's PC, saves it as a BMP file and then sends it to the code writer along with the PC data.

The activity of malicious codes is no longer limited to user account data stealing (online game hacking) or bank account information stealing (phishing). Malicious codes are continuing to evolve and now there are Trojan horses that can literally peek into your private life. Users must guard against malicious codes to prevent their privacy from becoming seriously jeopardized. To guard against such malicious codes:

1. Update anti-virus programs to the latest version.
2. If you're a Windows XP user, install the latest service pack and all security updates.
3. Use IE 8.0 or a higher version or another browser.
4. Regularly scan PCs for malicious codes.
5. Disable laptop webcams in System Settings when not used.
6. Disconnect webcams from PCs when not used.

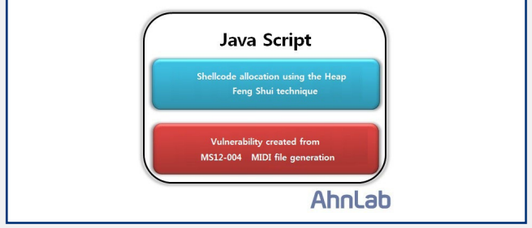
V3 detects this malicious code as:
- Win-Trojan/Backdoor.762880 (2012.02.21.00)

Malicious script preying on vulnerabilities of modified MS12-004 discovered

The ASEC discovered the distribution of a malicious code that takes advantage of MS12-004 Windows media vulnerability (CVE-2012-0003) on January 27, 2012. In turn, Microsoft announced that the vulnerability can be removed by the security patch distributed on January 11, 2012. It is speculated that this malicious code has been distributed in Far East Asia, including Korea and China, with online gaming data as the target.

On February 2, 2012, a variant of malicious script that takes advantage of MS12-004 vulnerability by using a technique called "Heap Feng Shui" was discovered on a Korean website. This malicious script is estimated to have been distributed on January 30, 2012. Its structure is shown in Fig. 1-17.

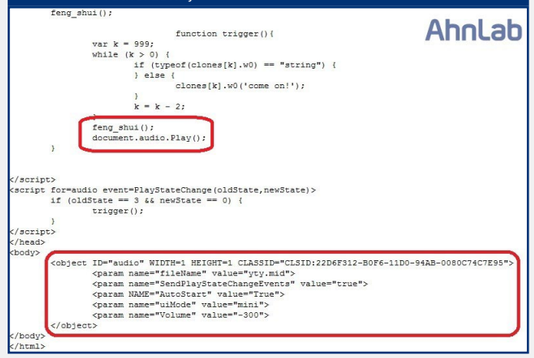
[Fig. 1-17] Structure of the malicious script variant to exploit MS12-004 vulnerability



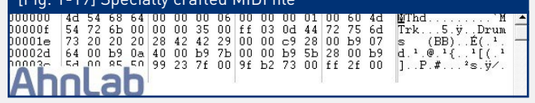
Heap Feng Shui is a technique first announced by Black Hat Europe in 2007. It manipulates the heap space on the browser through sequential Java Script allocation.

The script is designed to call file yty.mid, but the actual attacks would not have been successful as the MIDI file is damaged as shown in Fig. 1-19.

[Fig. 1-18] Part of the malicious script variant to exploit MS12-004 vulnerability



[Fig. 1-19] Specially crafted MIDI file



The shellcode of this malicious code downloads and executes i.exe (20,480 bytes) from a system located in Korea. The i.exe was created using Visual Basic and steals user data of certain online games made in Korea and reads certain ASP files.

72 variants of malicious scripts exploiting MS12-004 vulnerability were detected by V3 over the weekend. As such, distribution of this malicious code is expected to continue along with other online game-related malicious codes. Users must install the latest Windows security patch to guard against such malicious codes.

V3 detects this malicious code as:
- Downloader/Win32.Small
- HTML/Ms12-004
- Exploit/Ms12-004
- JS/Redirector
- SWF/Cve-2011-2140
- JS/Cve-2010-0806

Online game hacking codes targeted at Windows Vista and Windows 7 discovered

An online game hacking code targeted at Windows Vista and Windows 7 users has been discovered. Up until now, most online game hacking codes were targeted at Windows XP users, but this newly discovered online game hacking code identifies the OS of a target PC and attacks in a way specifically designed for a particular OS.

1. Windows XP

With Windows XP, C:\Windows\System32\ws2help.dll continues to be changed to a malicious file. Once the malicious code functions, the original file name under the path C:\Windows\System32 is changed to ws2helpXP.dll or ws2help.dll.[random].tmp and malicious file ws2help.dll is created.

[Fig. 1-20] Malicious file ws2help.dll generated on Windows XP

ws2help.dll	63 KB	Application Extension	2/27/2012 4:11 PM
ws2help.dll.pcg.tmp	20 KB	TMP File	4/14/2008 9:00 PM

2. Windows Vista or Windows 7

This malicious code generates himym.dll under C:\Windows\System32\ on Windows Vista or Windows 7. However, system file modification or deletion identified on Windows XP was not found.

This malicious code can be detected and treated using the following removal provided by AhnLab.

<Download V3 GameHack Kill Removal>
http://www.ahnlab.com/kr/site/download/vacc/vaccView.do?seq=105

As this malicious code is distributed through websites, security updates are to be installed immediately upon release to prevent infection.

Adobe Flash Player Update: http://asec.ahnlab.com/728
Windows Security Update: http://asec.ahnlab.com/221
Java Update: http://asec.ahnlab.com/758

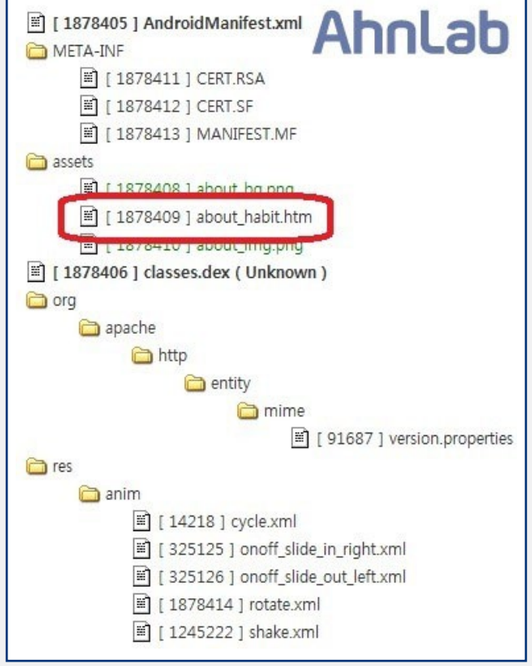
V3 detects this malicious code as:
- Win-Trojan/Patched.64000.B (2012.02.26.00)
- Win-Trojan/Patcher.135680 (2012.02.26.00)
- Win-Trojan/Patcher.133632 (2012.02.27.00)

01. Malicious Code Trend
c. Mobile Malicious Code Issues

A Windows malicious code included in Android applications

On February 3, 2012, the ASEC discovered a Windows malicious code in certain Android applications. These Android apps have the structure shown in Fig. 1-21. Script file about_habit.htm (123,196 bytes), marked in red, was found inside.

[Fig. 1-21] Visual basic script found inside an Android application



This about_habit.htm is not a general HTML file, but a visual basic script with the following structure.

This visual basic script file is named svchost.exe (61,357 bytes) and generates and executes malicious codes that function on Windows OS. However, it cannot function on Android OS and none of the application's internal codes have been designed to use the script in external memory.

[Fig. 1-22] Visual basic script for generating malicious codes

```
<SCRIPT Language=VBScript><!--
DropFileName = "svchost.exe"
WriteData = "4D5A900003000000040000000FFFF0000B800000000000000040
3CAFF03DA8D1C0809C364A13000000002F88BD0FECF8D1C088D1E1BDA8B422
96E64436C6F736500000043726561746550726F6365737357000000476574
53A3B444D4A3600400000324E00360003639433A0038004B003B46003E473
A36314                                                  31004C360
432000                                                  313232303
000000                                                  000000000
000000                                                  280008001
94E475                                                  3745004B0
6D1223                                                  393F02634
200008                                                  A864A21DC
C727B4                                                  A2C27F471
A00FEE                                                  573188345
D6EAC2                                                  CEE149FD9
7FD512                                                  C467520514
2A912F                                                  9E5662AD7
239295                                                  5DE95A62F
D3E4FB                                                  97DEDEBD9
879FC9                                                  7DB4816251
751703                                                  181C14C725
82B62A                                                  4E3DDC40A
A88CDA                                                  0237781DA
446FDC                                                  29933B2D9
1107B0                                                  F60C3C71D
7C8675.                                                 40440F4F3
4BB344                                                  B0302F42D
9D0E60                                                  78C1E9DD8
62236A2F06930BE18F6002159FED059653E85B25B190C146F488BDE7C770311
EADFACB0EC011FF7520024FE65B44D01EADFACB0EC011FF01DB30A14827C84
1427B597A26224F6573617103122228734B79557362204E6D6C2D3D000C362
Set FSO = CreateObject("Scripting.FileSystemObject")
DropPath = FSO.GetSpecialFolder(2) & "\" & DropFileName
If FSO.FileExists(DropPath)=False Then
Set FileObj = FSO.CreateTextFile(DropPath, True)
```

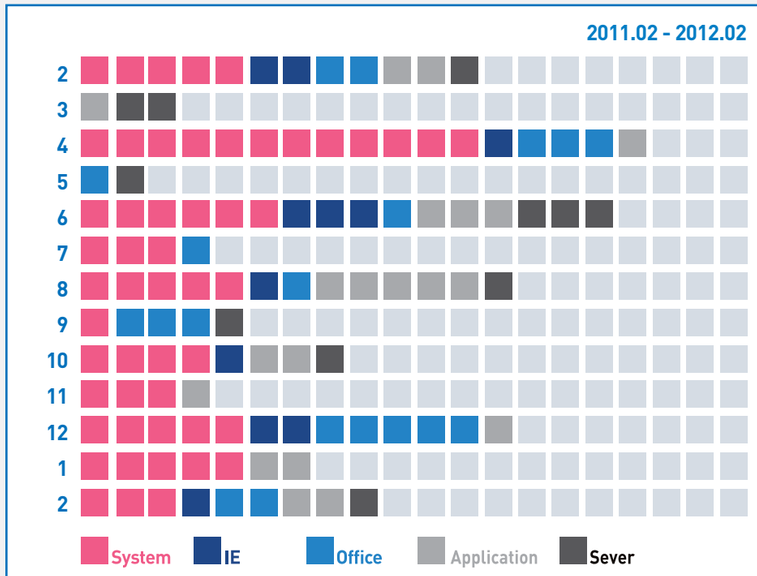
As such, it is speculated that this visual basic script file was accidentally included during application development.

V3 detects this malicious code as:
- VBS/Agent
- Win-Trojan/Krap.61357

02. Security Trend
a. Security Statistics

Microsoft Security Updates – February 2012

Microsoft issued 9 security updates this month (4 critical and 5 important). The security update released this month comprehensively addresses the vulnerabilities of Internet Explorer and Windows. Also included is MS12-013, a patch for vulnerabilities in C Runtime Library.



[Fig. 2-1] MS Security Updates

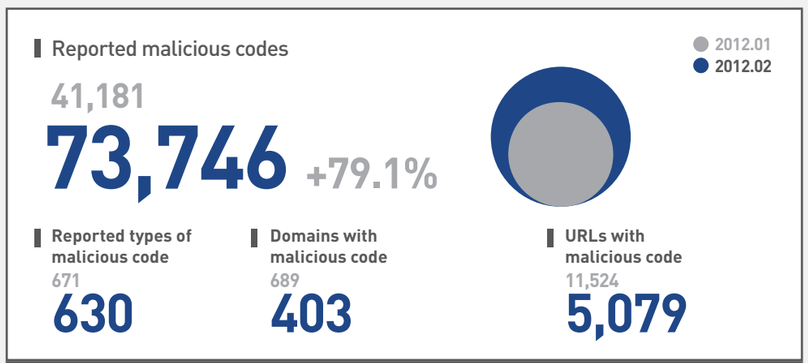
Severity	Vulnerability
Critical	Vulnerability in Windows kernel-mode drivers could allow remote code execution (2660465)
Critical	Cumulative Security Update for Internet Explorer (2647516)
Critical	Vulnerability in C Runtime Library could allow remote code execution (2654428)
Important	Vulnerability in Ancillary Function Driver could allow elevation of privilege (2645640)
Important	Vulnerability in Indeo Codec could allow remote code execution (2661637)
Critical	Vulnerability in .NET Framework and Microsoft Silverlight could allow remote code execution (2651026)
Important	Vulnerability in Color control panel could allow remote code execution (2643719)

[Table 2-1] MS Security Updates for Feb, 2012

03. Web Security Trend
a. Web Security Statistics

Website Security Summary

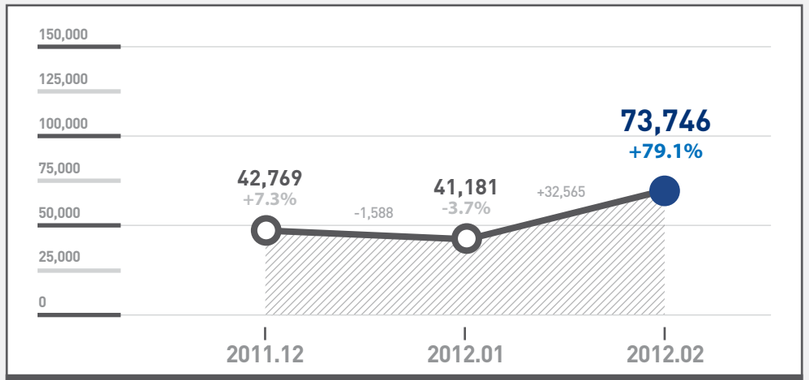
This month, SiteGuard (AhnLab's web browser security service) blocked 73,746 websites that distributed malicious codes. 630 types of malicious code, 403 domains with malicious code and 5,079 URLs with malicious code were found. The numbers of reported types of malicious code and domains and URLs with malicious code decreased from last month, but the number of reported malicious codes increased.



[Table 3-1] Website Security Summary

Monthly Change in Blocked Malicious URLs

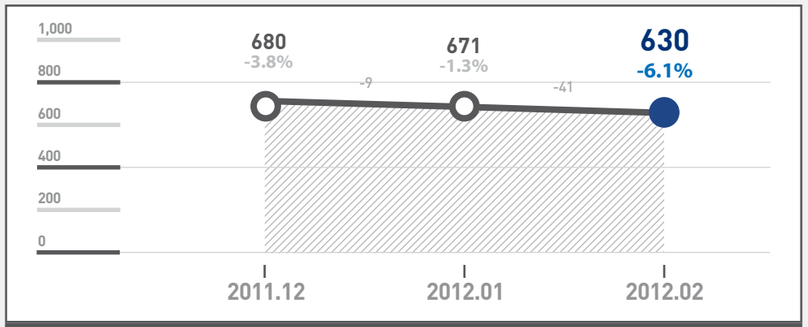
For February 2012, the number of reported blocked malicious URLs increased 79% from 41,181 the previous month to 73,746.



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

Monthly Change in the Number of Reported Malicious Code Types

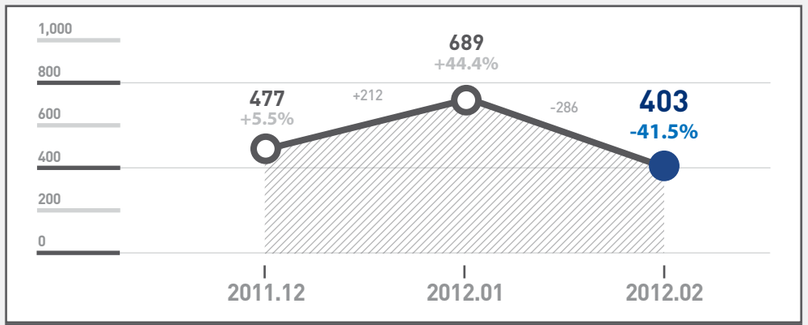
For February 2012, the number of reported types of malicious code decreased 6% from 671 the previous month to 630.



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

Monthly Change in Domains with Malicious Code

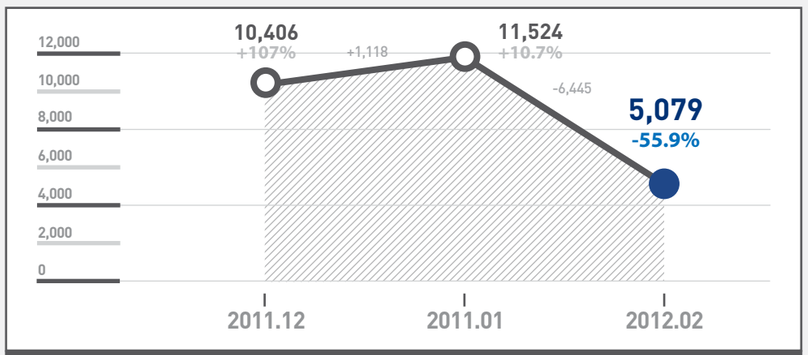
403 domains were found with malicious codes in February 2012, a 42% fall from the 689 found in the previous month.



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

Monthly Change in URLs with Malicious Code

For February 2012, the number of reported URLs with malicious code decreased 56% from 11,524 the previous month to 5,079.



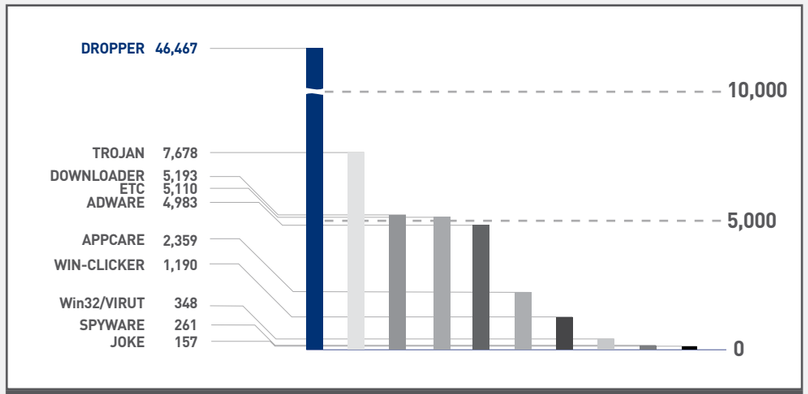
[Fig. 3-4] Monthly Change in URLs with Malicious Code

Top Distributed Types of Malicious Code

For February 2012, dropper is the top distributed type of malicious code, with 46,467 (63%) cases reported, followed by Trojan, with 7,678 (10.4%) cases reported.

TYPE	Reports	Percentage
DROPPER	**46,467**	**63.0%**
TROJAN	7,678	10.4%
DOWNLOADER	5,193	7.0%
ADWARE	4,983	6.8%
APPCARE	2,359	3.2%
WIN-CLICKER	1,190	1.6%
Win32/VIRUT	348	0.5%
SPYWARE	261	0.4%
JOKE	157	0.2%
ETC	5,110	6.9%
	73,746	**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

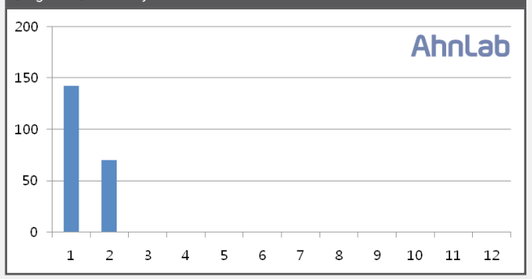
Ranking	↑↓	Malicious Code	Reports	Percentage
1	**NEW**	**Win-Dropper/KorAd.2008816**	**44,877**	**77.8%**
2	▲1	Downloader/Win32.Korad	2,403	4.2%
3	▲2	Win-AppCare/WinKeyfinder.973512	2,143	3.7%
4	▲2	Adware/Win32.KorAd	2,141	3.7%
5	▼1	Downloader/Win32.Totoran	1,592	2.8%
6	NEW	Win-Clicker/Agent.22528.B	1,190	2.1%
7	NEW	Trojan/Win32.HDC	980	1.7%
8	NEW	Win-Adware/ToolBar.Cashon.308224	924	1.6%
9	▼7	Downloader/Win32.Genome	839	1.5%
10	▼2	Win-Trojan/Buzus.430080.J	594	0.9%
			57,683	**100.0%**

[Table 3-3] Top 10 Distributed Malicious Codes

03. Web Security Trend
b. Web Security Issues

Feb. 2012 Malicious Code Intrusion: Website

[Fig. 3-6] Monthly malicious code intrusion: website



The chart above shows the number of websites intruded to distribute malicious codes. It is speculated that a reduction in external attacks, with a national holiday having fallen over a weekend, is the reason for the number falling by one half.

Top 10 malicious codes distributed via websites

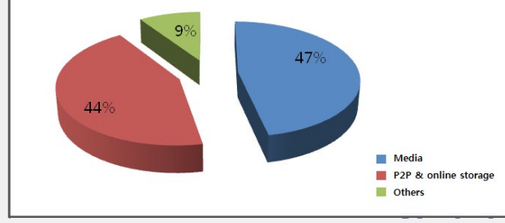
[Table 3-4] Top 10 malicious codes distributed via websites

Ranking	Threat	URL
1	**Win-Trojan/Patched.64000.B**	**32**
2	Win-Trojan/Onlinegamehack.61440.DI	25
3	Win-Trojan/Onlinegamehack.61440.DH	24
4	Win-Trojan/Patcher.135680	24
5	Dropper/Onlinegamehack.85360	16
6	Win-Trojan/Onlinegamehack.51244	15
7	Win-Trojan/Onlinegamehack.35672.B	15
8	Dropper/Onlinegamehack.86056	15
9	Win-Trojan/Patched.64512.B	13
10	Win-Trojan/Onlinegamehack.139264.CV	11

The table above shows the top 10 malicious codes distributed via websites this month. As with the previous month, online game hacking Trojan horses were the most prevalent. Win-Trojan/Patched.64000.B is the most reported malicious code, distributed via 32 compromised websites.

As for the types of site, distribution via media websites is the most reported, followed by distribution via P2P, online storage and others, as shown below.

[Fig. 3-7] Distribution of Win-Trojan/Patched.64000.B



VOL. 26
ASEC REPORT Contributors

Contributors

Principal Researcher	Seung-won Lee
Principal Researcher	Jung-hyung Lee
Senior Researcher	Dong-hyun Kang
Senior Researcher	Chang-yong Ahn
Senior Researcher	Young-jun Chang
Senior Researcher	Seol-woo Joo
Assistant Researcher	Young-goo Kim
Researcher	Sang-woo Shim

Key Sources — ASEC Team, SiteGuard Team

Executive Editor
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