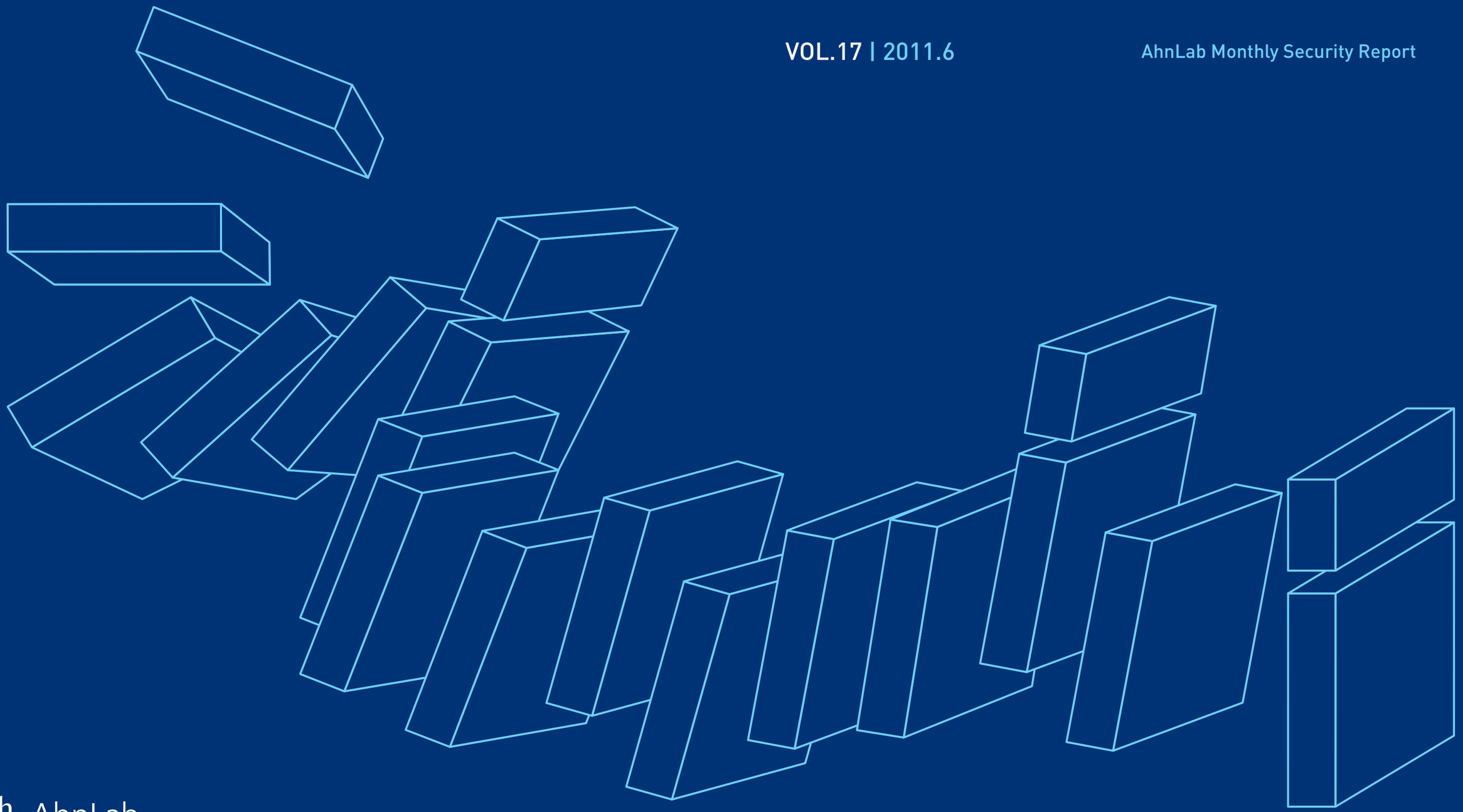
ASEC REPORT

VOL.17 | 2011.6

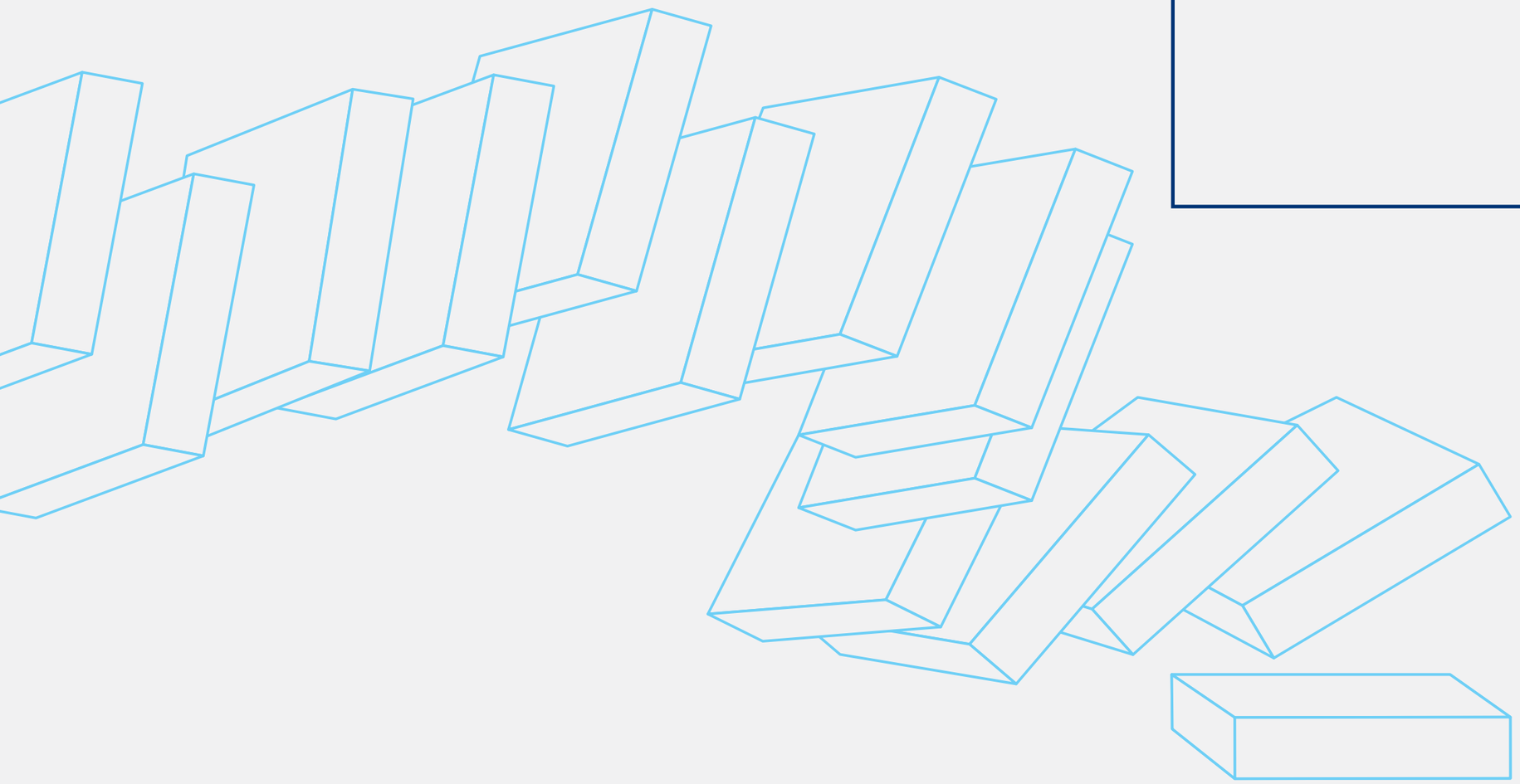
AhnLab Monthly Security Report



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

01. Malicious Code Trend

a. Malicious Code Statistics

Top 20 Malicious Code Reports

The table below shows the percentage breakdown of the top 20 malicious codes reported in May 2011. As of May 2011, TextImage/Autorun is the most reported malicious code, followed by Swf/Downloader and JS/Redirect, respectively. 8 new malicious codes were reported this month.

Ranking	↑↓	Malicious Code	Reports	Percentage
1	—	Textimage/Autorun	830,412	21.3 %
2	NEW	Swf/Downloader	458,353	11.7 %
3	—	JS/Redirect	360,137	9.2 %
4	▲4	Win-Trojan/Winsoft.78981.CIB	274,935	7.1 %
5	NEW	JS/Downloader	217,226	5.6 %
6	▲10	JS/Exploit	202,567	5.2 %
7	▼2	Win32/Induc	188,157	4.8 %
8	▼6	Win-Trojan/Overtls27.Gen	141,984	3.6 %
9	NEW	Win-Trojan/Downloader.156565	136,846	3.5 %
10	▼3	Win32/Palevo1.worm.Gen	128,923	3.3 %
11	NEW	JS/Cve-2010-0806	111,631	2.9 %
12	▼3	Win32/Conficker.worm.Gen	111,255	2.9 %
13	NEW	JS/Exploit-down	106,908	2.7 %
14	▼10	JS/Agent	101,503	2.6 %
15	▼5	Win32/Olala.worm	98,690	2.5 %
16	▼3	Win32/Virut.f	91,371	2.3 %
17	NEW	Als/Pasdoc	88,609	2.3 %
18	▼7	Win32/Parite	86,112	2.2 %
19	NEW	JS/Exploit-download	85,272	2.2 %
20	NEW	Dropper/Onlinegamehack5.Gen	80,547	2.1 %
			3,901,438	100 %

[Table 1–1] Top 20 Malicious Code Reports

Top 20 Malicious Code Variant Reports

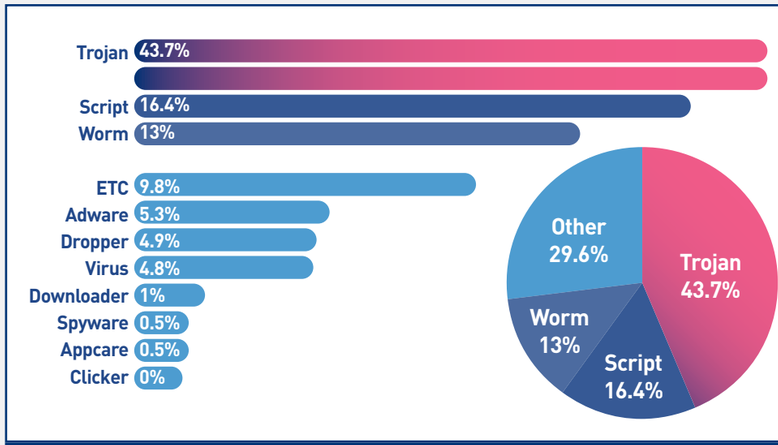
The table below shows the percentage breakdown of the top 20 malicious code variants reported this month, and identifies the malicious code trend of this month.

Ranking	↑↓	Malicious Code	Reports	Percentage
1	—	Win-Trojan/Onlinegamehack	1,224,743	15.7 %
2	▲1	Textimage/Autorun	830,553	10.7 %
3	▲1	Win-Trojan/Downloader	723,193	9.3 %
4	▲2	Win-Trojan/Winsoft	700,729	9.0 %
5	—	Win-Trojan/Agent	636,745	8.2 %
6	NEW	Swf/Downloader	458,354	5.9 %
7	▲3	Win32/Conficker	367,268	4.7 %
8	▲1	JS/Redirect	360,137	4.6 %
9	▲2	Win32/Autorun.worm	355,162	4.6 %
10	▲2	Win32/Virut	286,039	3.7 %
11	▲3	Dropper/Malware	234,709	3.0 %
12	▲2	Win32/Kido	233,226	3.0 %
13	NEW	JS/Downloader	217,226	2.8 %
14	NEW	JS/Exploit	202,567	2.6 %
15	—	Win-Adware/Koradware	192,606	2.5 %
16	—	Win32/Induc	188,275	2.4 %
17	▲1	VBS/Solow	155,686	2.0 %
18	▲1	Win32/Palevo	154,147	2.0 %
19	▲13	Win-Trojan/Overtls27	141,984	1.7 %
20	—	Win32/Palevo1	128,923	1.6 %
			7,792,272	100 %

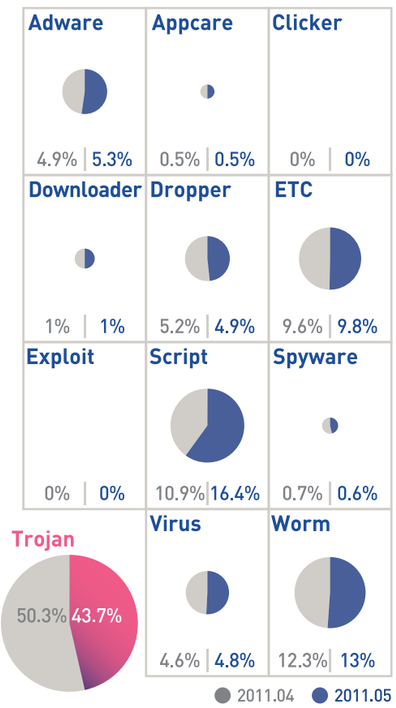
[Table 1-2] Top 20 Malicious Code Variant Reports

Breakdown of Primary Malicious Code Type

The chart below categorizes the top malicious codes reported this month. As of May 2011, Trojan is the most reported malicious code, representing 43.7% of the top reported malicious codes, followed by script (16.4%) and worm (13%).



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



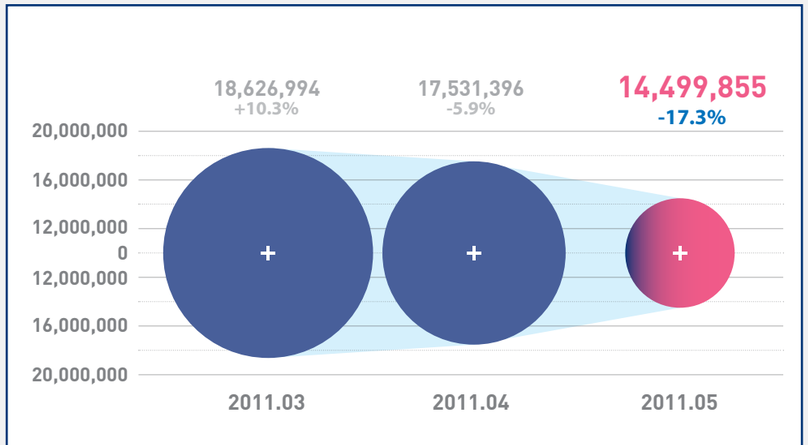
[Fig. 1-2] Comparison of Malicious Codes with Previous Month

Comparison of Malicious Codes with Previous Month

Compared to last month, the number of script, worm, adware and virus increased, whereas, the number of Trojan, dropper and spyware dropped. The number of downloader and Appcare was similar to the previous month.

Monthly Malicious Code Reports

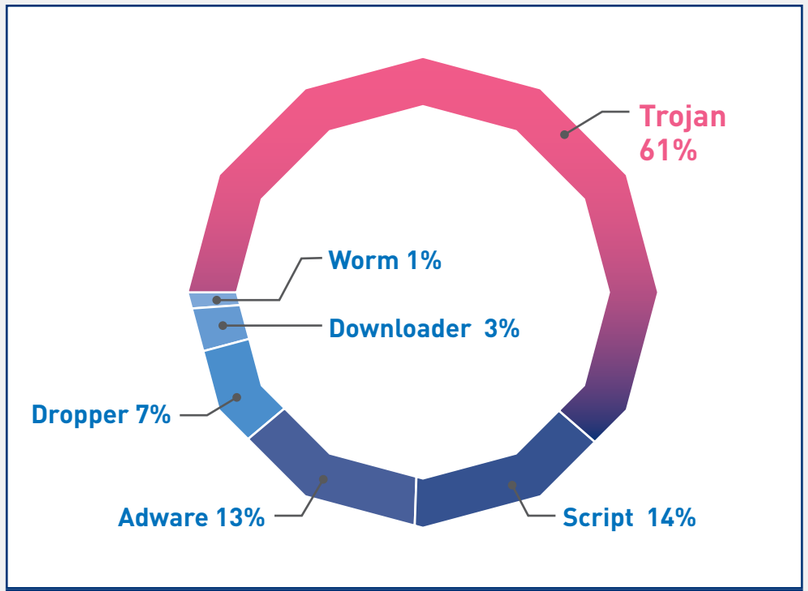
There has been a decrease in malicious code reports in May, which dropped 3,031,541 to 14,499,855 from 17,531,396 in April.



[Fig. 1-3] Monthly Malicious Code Reports

Breakdown of New Malicious Code Type

As of May 2011, Trojan is the most reported new malicious code, representing 61% of the top reported new malicious codes. It is followed by script (14%) and adware (13%).



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

Top 20 New Malicious Code Reports

The table below shows the percentage breakdown of the top 20 new malicious codes reported in May 2011. As of May 2011, JS/Exploit-down is the most reported new malicious code, representing 15% (106,908 reports) of the top 20 reported new malicious codes, followed by JS/Exploit-download (85,272 reports).

Ranking	Malicious Code	Reports	Percentage
1	JS/Exploit-down	106,908	15.0 %
2	JS/Exploit-download	85,272	12.0 %
3	Win-Trojan/Downloader.237568.Z	69,139	9.7 %
4	HTML/Exploit-down	63,019	8.9 %
5	Win-Adware/WindowSmart.77824	45,188	6.4 %
6	Win-Trojan/Agent.389120.BY	35,202	5.0 %
7	Win-Trojan/Exploit-swf	34,806	4.9 %
8	Win-Trojan/Onlinegamehack.98304.HA	31,621	4.4 %
9	Win-Trojan/Onlinegamehack.39058.B	24,402	3.4 %
10	Win-Trojan/Onlinegamehack.89088.AJ	24,138	3.4 %
11	Dropper/Agent.224248	23,628	3.3 %
12	Win-Adware/WindowSmart.53248	22,278	3.1 %
13	Win-Trojan/Adload.1197056.B	20,747	2.9 %
14	Win-Adware/Shortcut.SayPoint.434659	20,640	2.9 %
15	Win-Trojan/Downloader.1423360.B	19,641	2.8 %
16	Win-Trojan/Downloader.328635	18,282	2.6 %
17	Win-Adware/KorAdware.389120	17,805	2.5 %
18	Win-Trojan/Downloader.320000.C	17,051	2.4 %
19	Win-Trojan/Onlinegamehack.23690.B	15,886	2.2 %
20	Win-Downloader/Totoran.1698304	15,226	2.1 %
		710,879	100 %

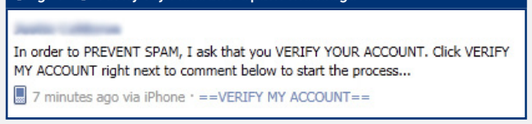
[Table 1-3] Top 20 New Malicious Code Reports

01. Malicious Code Trend
b. Malicious Code Issues

'Dislike' Button Scam

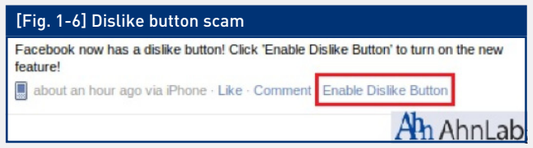
Facebook is an enormous social networking service with hundreds of millions of users all over the world and more than 3 million users in Korea alone. Facebook spam is on the increase, and on May 12, a new Facebook spam, 'Verify My Account' begun spreading on Facebook .

[Fig. 1-5] 'Verify My Account' spam message



The message is disguised as Facebook alert and asks you to verify your account in order to prevent spam. When you click on "VERIFY MY ACCOUNT", it will automatically post the same message on all of your friends' wall. Facebook deleted the spam message within a few hours and managed to stop it from spreading further, but with hundreds of millions of Facebook users, it may resurface anytime. A few days later, spammers were at it again. This time, they claimed Facebook is adding a "Dislike" button to user's pages. The message was just like the 'Verify My Account' spam, but was not an issue in Korea.

[Fig. 1-6] Dislike button scam

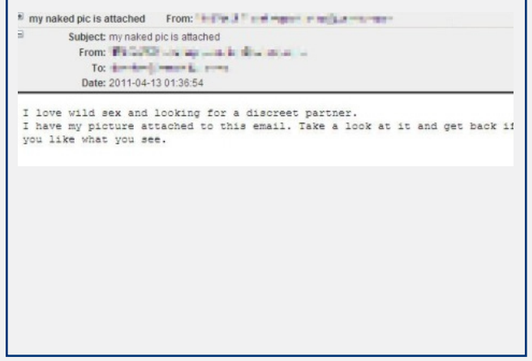


Most Facebook spam campaigns today circulate rogue codes in the procedure of their execution, but may contain malicious codes in the future. Users must always be careful of the messages and alerts posted on their walls.

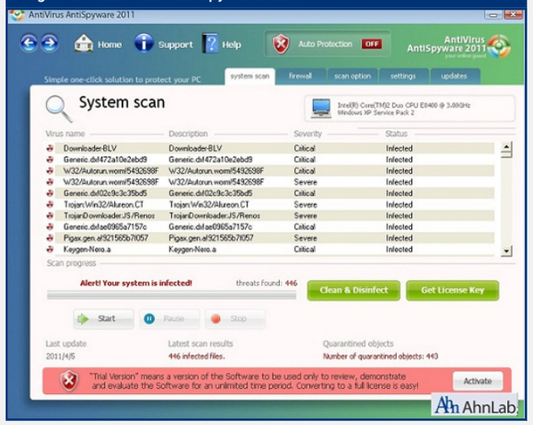
AntiVirus AntiSpyware 2011 Scam

The bait for this scam is an email with the subject line "My naked pic is attached". AntiVirus AntiSpyware is a fake antivirus application that has been around for several years. The following spam was sent out from last month:

[Fig. 1-7] Spam with 'mypicture.scr' malware attachment

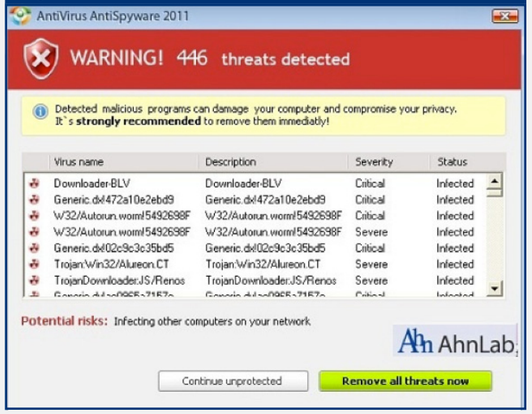


[Fig. 1-8] AntiVirus AntiSpyware 2011



Opening the file will download AntiVirus AntiSpyware 2011 onto your system. It will show false scan results claiming your PC has multiple security issues and infections that need to be removed with payment. It will continue displaying the fake results, and restrict execution of other applications while it is running.

[Fig. 1-9] False scan result



V3 detects this Trojan horse as Win-Trojan/Fakeav. With the increase in rogue antivirus, you must be careful when downloading files from websites and email attachments.

Scam Emails From Bobijou Inc.

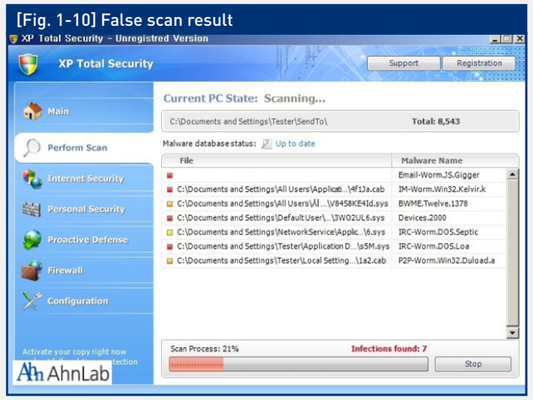
A spam claiming to be from Bobijou started circulating on April 26. The spam contains a zip file attachment containing an .exe file. Below is a sample of the spam:

[Table 1-4] Spam mail posing as an order confirmation

Subject	Successful Order [random 6-digit number]
Message	Thank you for ordering from Bobijou Inc. This message is to inform you that your order has been received and is currently being processed. Your order reference is [random 6-digit number]. You will need this in all correspondence. This receipt is NOT proof of purchase. We will send a printed invoice by mail to your billing address. You have chosen to pay by credit card. Your card will be charged for the amount of 106.00 USD and Bobijou Inc. will appear next to the charge on your statement. You will receive a separate email confirming your order has been dispatched. Your purchase and delivery information appears below in attached file. Thanks again for shopping at Bobijou Inc.
Attachment	- Order details.zip (7,345 bytes)

When you decompress the attached 'Order details.zip' (7,345 bytes) file, it reveals 'Order details.exe' (17,920 bytes). Running the executable file will execute svchost.exe on your system and overwrite some codes in the svchost.exe memory. The svchost.exe process will then attempt to connect to a system in Russia to download pusk.exe (352,25 bytes). Executing the downloaded pusk.exe file will open a rogue antivirus that will scan your system as below:

[Fig. 1-10] False scan result



When the scan is complete, it will show a fake alert claiming your PC has multiple security issues and infections to trick you into purchasing a license for the rogue software.

[Fig. 1-11] False security alert

If you click Register, you will be asked to purchase a license.

V3 detects this Trojan as:

- Win-Trojan/Chepvil.17920.E
- Win-Trojan/Chepvil.17920.F
- Win-Trojan/Zbot.17920.D
- Win-Trojan/Kazy.352256

[Fig. 1-12] Webpage instructing user to purchase license

The names of the file attachment are slightly different, but when executed, it attempts to connect to pool.ntp.org and microsoft.com to check whether the system is connected to a network. If the infected system is connected to a network, it tries to download a file from a system in the US, but when we tested, we could not download the file. It should download a rogue antivirus. It terminates security programs such as kav.exe and navapsvc.exe, and also Windows Security Center by manipulating the Registry. V3 detects this Trojan as below. You must be careful not to open file attachments from untrusted sources, as new variants keep being detected.

- **Win-Trojan/Zbot.54784.F**
- **Win-Trojan/Kazy.54272.B**
- **Win-Trojan/Downloader.54784.AY**

Spam Promising Nude Photo Spreads Malware

ASEC discovered the 'naked picture' scam for the first time on February 2011 and again on March 18. This scam started spreading again from around April 27 and is still being detected. Below is a sample of the spam:

[Table 1-5] Spam mail promising nude photo

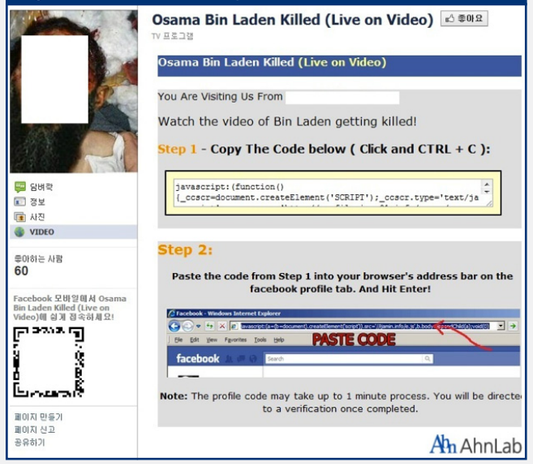
Subject	my naked picture my naked pic :) naked picture of me sending you my nude pic my hot pic :) sending you my nude pic for a good day :) my naked pic is attached
Message	hi sweetie... sending you my naked pictures i made today, hope you like em :) kisses.. hi sweetie... +--------- sending you my naked pictures i made today, hope you like em :) c ya tommorow kisses.. +--------- I love wild sex and looking for a discreet partner. I have my picture attached to this email. Take a look at it and get back if you like what you see.
Attachment	- pictures.zip (45,003 bytes) - mypicture.scr (54,784 bytes)

Osama Bin Laden Themed Malware

As news of Osama Bin Laden's death spread around the world on May 2, Internet scammers wasted no time in exploiting the situation. ASEC used Twitter to warn computer users to exercise caution when they receive emails that purport to show photos or videos of bin Laden's killing. It is not the first time news events have given hackers the opportunity to spread malware attacks around the world - Michael Jackson has been used as bait to distribute malware on June 2009. Malware based on Osama Bin Laden's death proliferated through the following methods:

- A link which claims to point to a video of the death of Osama bin Laden posted as updates on Facebook users' walls.

[Fig. 1-13] Link which claims to point to Osama bin Laden's death video



- Emails with attachments that purport to show photos or videos of bin Laden's killing.

[Fig. 1-14] Malicious attachments exploiting bin Laden's killing

- Spam containing malicious attachment that exploits the vulnerabilities in Microsoft Word, "MS10-087: Vulnerabilities in Microsoft Office could allow remote code execution". The vulnerabilities were also exploited on March 2011, abusing Japan's tragic disaster.

- BlackHat SEO campaigns in popular search engines trying to lure users to install rogueware.

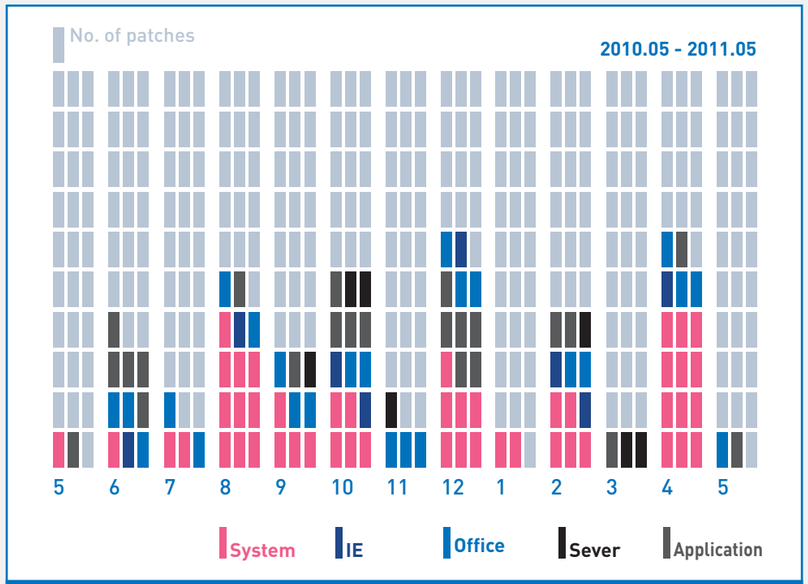
Social networking service, spam and websites were used to propagate malware, as above. V3 detects this malware as:

- Win-Trojan/Downloader.490496.P
- Win-Trojan/Fakeav.520704
- Win-Trojan/Agent.334336.BE
- Win-Trojan/Banload.664576
- Dropper/Cve-2010-3333
- Win-Trojan/Dingu.44504

02. Security Trend
a. Security Statistics

Microsoft Security Updates- May 2011

Microsoft released 2 security updates this month.



[Fig. 2-1] MS Security Updates

Bulletin	Reason for update	KB article
MS11-035	Addresses a vulnerability in Microsoft Windows	2524426
MS11-036	Addresses vulnerabilities in Microsoft PowerPoint	2545814

[Table 2-1] MS Security Updates for May 2011

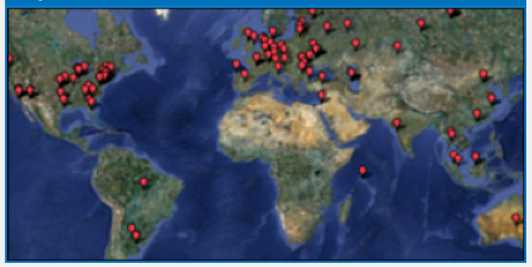
3 security updates were released this month, MS11-035 vulnerability allows remote control if a user received a specially crafted WINS replication packet on an affected system running the WINS service. MS11-036 vulnerability allows remote code execution if a user opens a specially crafted PowerPoint file. An attacker who successfully exploited either of this vulnerability could gain the same user rights as the logged-on user.

02. Security Trend
b. Security Issues

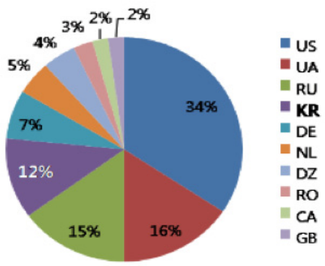
Zeus Source Code Leaked and Spyeye Trend

News broke that the source code for the Zeus Trojan, a profitable tool for cybercriminals, was released to the public. This source code for this bank-robbing Zeus Trojan is not the latest version, but with the source code out there, cybercriminals can improve it, expand on it, and use components of it in new malware.

[Fig. 2-2] Zeus Command and Control (C&C) Servers



[Fig. 2-3] World Distribution of SpyEye C&C Server's

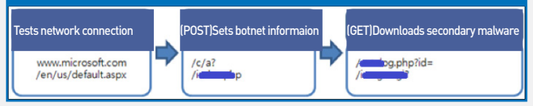


Reports on SpyEye decreased since December last year, but new C&C servers are emerging – this means SpyEye is still active. As it can be seen in the above pie chart, 34% of SpyEye C&C servers are located in the US, followed by 16% in Ukraine, 15% in Russia and 12% in South Korea.

Coreflood, a Banking Trojan

Coreflood first emerged in 2002 and specialized in stealing bank details. On April 2011, the FBI and U.S. Department of Justice obtained a temporary restraining order enabling them to disable the Coreflood botnet and respond to infected PCs. AhnLab TrusGuard detects this Trojan as Win32/CoreFlood.gen, and V3 detects it as Win-Trojan/Afcore.x.

[Fig. 2-4] Coreflood network

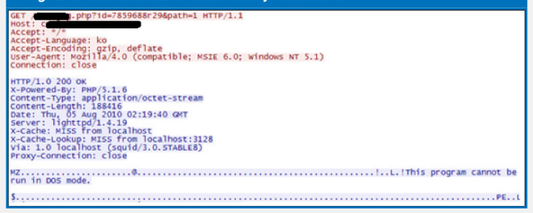


Tests network connection -> (POST) Sets botnet information -> (GET) Downloads secondary malware

In the POST step, it sets the botnet information and sends it to the C&C server to get various commands and information of the file to download.

[Fig. 2-5] Botnet information set by POST request

[Fig. 2-6] Download of secondary malware



[Fig. 2-7] Microsoft connection

```
GET /en/us/default.aspx HTTP/1.1
Host: www.microsoft.com
Accept: */*
Accept-Language: en
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Connection: close

HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Last-Modified: Tue, 03 Aug 2010 21:40:20 GMT
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 20738
```

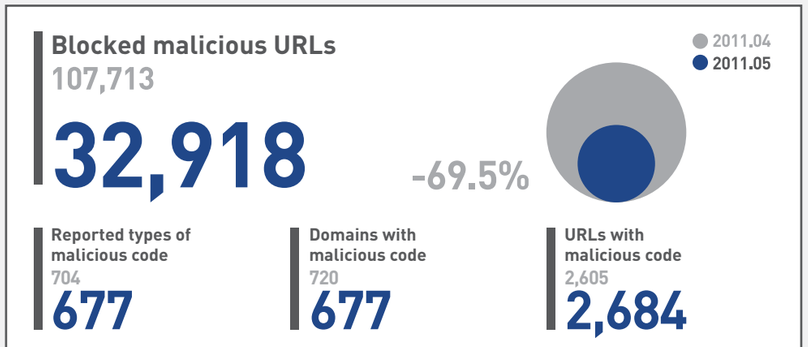
Online Banking Hacking Scam

Cybercriminals hacked several Korean online banking websites over the last few months to steal account information, paralyze the banking network or delete data from the server. Stolen account information could be used to send email or SMS spam and launch phishing attacks, and increases the chance of secondary damage. This time, hackers used the technique of stealing the user's digital certificate password from the targeted online banking site. To prevent this attack, it is advisable to use an antivirus and regularly update it to the latest version and turn on real-time monitoring.

03. Web Security Trend
a. Web Security Statistics

Web Security Summary

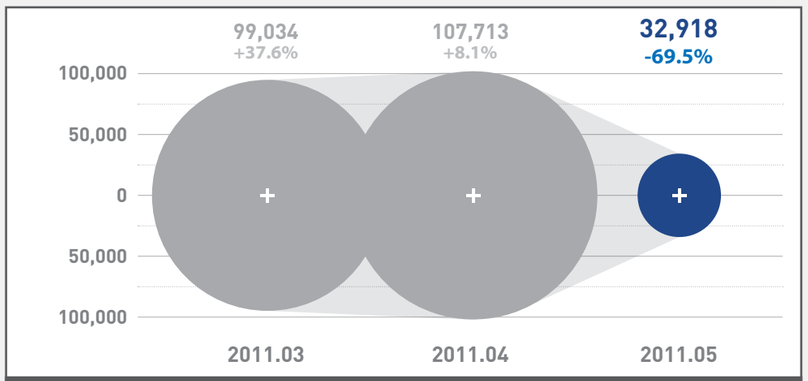
As of April 2011, there were 107,713 reported malicious codes, 704 types of reported malicious code, 720 reported domains with malicious code, and 2,605 reported URLs with malicious code. The type of reported malicious codes and domains and URLs with malicious code decreased, but the number of reported malicious codes increased from last month.



[Table 3-1] Website Security Summary

Monthly Blocked Malicious URLs

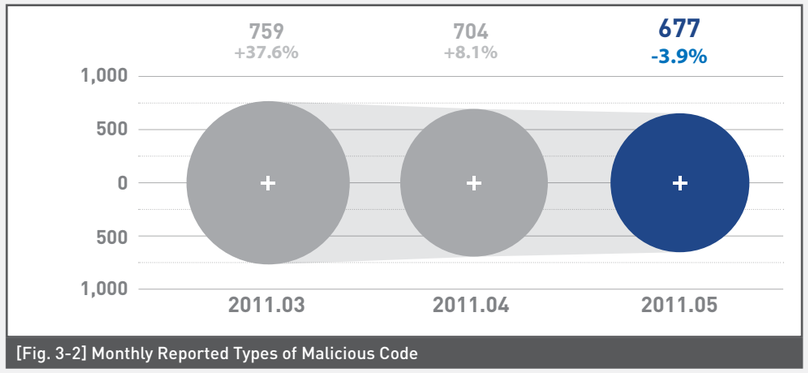
As of May, the number of blocked malicious URLs decreased 69% from 107,713 the previous month to 32,918.



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

Monthly Reported Types of Malicious Code

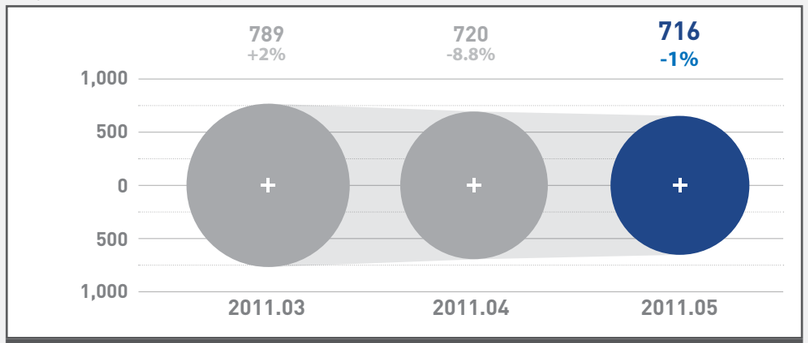
As of May 2011, the number of reported types of malicious code decreased 4% from 704 the previous month to 677.



[Fig. 3-2] Monthly Reported Types of Malicious Code

Monthly Domains with Malicious Code

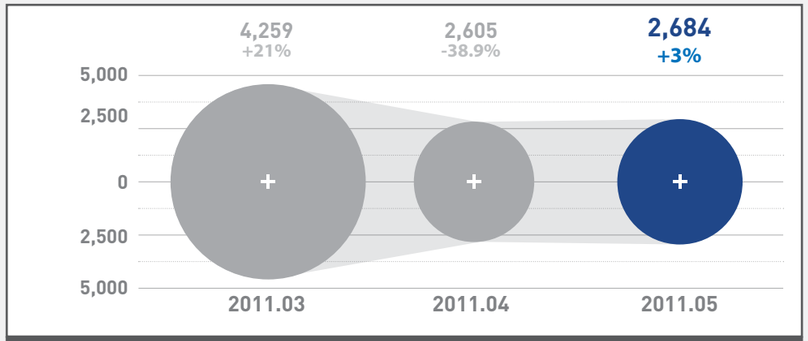
As of May 2011, the number of reported domains with malicious code decreased 1% from 720 the previous month to 716.



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

Monthly URLs with Malicious Code

As of May 2011, the number of reported URLs with malicious code Increased 3% from 2,605 the previous month to 2,684.



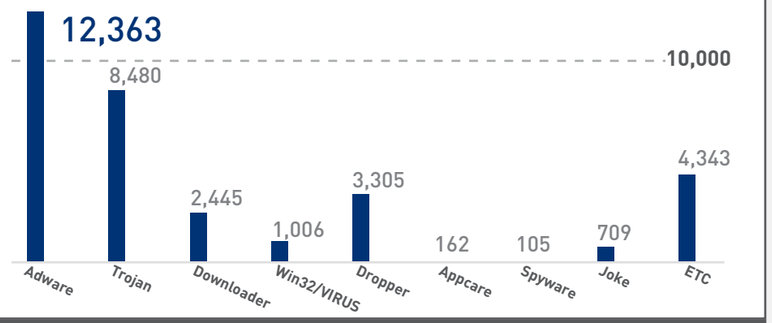
[Fig. 3-4] Monthly URLs with Malicious Code

Distribution of Malicious Codes by Type

As of May 2011, adware is the top distributed type of malicious code with 12,363 (37.6%) cases reported, followed by Trojan with 8,480 (25.8%) cases reported.

TYPE	Reports	Percentage
ADWARE	12,363	37.6 %
TROJAN	8,480	25.8 %
DROPPER	3,305	10.0 %
DOWNLOADER	2,445	7.4 %
Win32/VIRUT	1,006	3.1 %
JOKE	709	2.2 %
APPCARE	162	0.5 %
SPYWARE	105	0.3 %
ETC		13.2 %
Total	**32,918**	**100 %**

[Table 3-2] Distribution of Malicious Codes by Type



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

Top 10 Distributed Malicious Codes

As of May 2011, Win-Adware/Shortcut.InlivePlayerActiveX.234 is the most distributed malicious code, with 2,029 cases reported. 5 new malicious codes, including Win-Adware/KorAd.1661440, emerged in the top 5 list this month.

Ranking ↑↓		Malicious Code	Reports	Percentage
1	▲2	Win-Adware/Shortcut.InlivePlayerActiveX.234	2,029	13.5 %
2	▲4	Win-Adware/ToolBar.Cashon.308224	1,913	12.7 %
3	▲1	Win-Adware/Shortcut.Unni82.3739648	1,676	11.1 %
4	NEW	Win-Adware/KorAd.1661440	1,644	10.9 %
5	▲4	Adware/Win32.ToolBar	1,642	10.9 %
6	NEW	Win-Dropper/PWS.Infostealer.196945	1,525	10.1 %
7	NEW	Win-Trojan/Downloader.1557504.ANB	1,351	9.0 %
8	▼3	Win-Adware/Shortcut.Bestcode.0002	1,263	8.4 %
9	NEW	Win-Trojan/Downloader.1557504.AEE	1,136	7.5 %
10	NEW	Win-Downloader/KorAd.1504768	877	5.8 %
			15,056	100 %

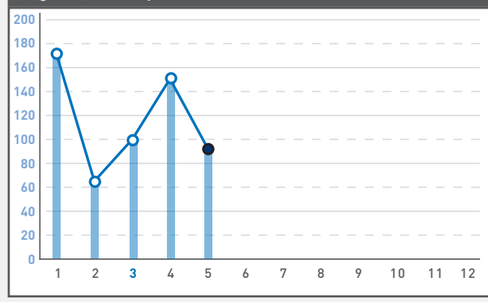
[Table 3-3] Top 10 Distributed Malicious Codes

03. Web Security Trend
b. Web Security Issues

May 2011 Malicious Code Intrusion: Website

As it can be seen in the chart above, the number of malicious code intrusion rose consistently from February, but fell in May.

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



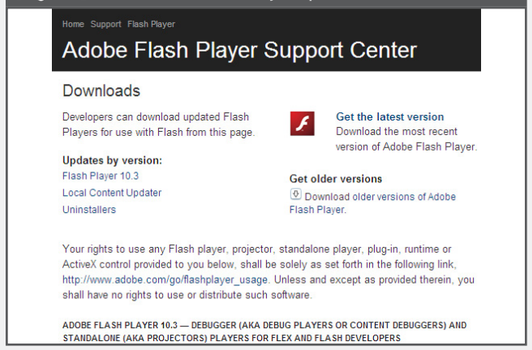
[Table 3-4] Top 10 Distributed Malicious Codes

Ranking	Malicious Code	URL
1	Win-Trojan/Patched.DE	44
2	Win-Trojan/Onlinegamehack.36864.FI	24
3	Win-Trojan/PatchedImm.Gen	24
4	Win-Trojan/Downloader.40960.VY	21
5	Win-Trojan/PatchedImm.Gen	17
6	Dropper/Xema.37376.P	16
7	Dropper/Onlinegamehack.10500558	15
8	Win-Trojan/Downloader.40960.VX	14
9	Dropper/Onlinegamehack.72192.B	14
10	Win-Trojan/Killav.12288.N	13

The table above shows the top 10 distributed malicious codes. Most of malicious codes patches Windows files or replaces the files with malicious ones. The vulnerabilities that are the most exploited by the malicious codes are MS10-018, MS10- 090, CVE-2011-0609 and CVE-2011-0611. The malicious codes that rank 3rd and 4th on the list exploit vulnerabilities in Adobe Flash Player. There was an increase in malicious codes exploiting Adobe Flash Player vulnerabilities this month. Always update your Adobe Flash Player to the latest version.

*** Download the latest Adobe Flash Player from:** http://www.adobe.com/support/flashplayer/downloads.html

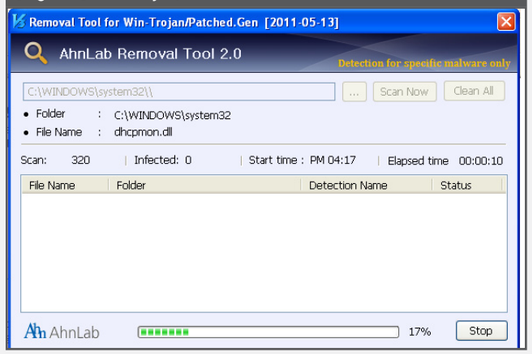
[Fig. 3-7] Latest Adobe Flash Player update



If the malicious code that patches Windows files infects your system, it will prevent your antivirus from getting updated and running properly. You must remove the malicious code by downloading the removal tool below:

*** Download the removal tool from:** http://download.ahnlab.com/vaccine/v3removaltool_patched.exe

[Fig. 3-8] Win-Trojan/Patched.Gen removal tool



VOL. 17
ASEC REPORT Contributors

Executive Editor

Senior Researcher	Hyung-bong Ahn

Contributors

Senior Researcher	Chang-yong Ahn
Senior Researcher	Young-jun Chang
Researcher	Jung-woo Park
Researcher	Do-han Lee
Researcher	Bo-hwa Cho

Reviewer

CTO	Si-haeng Cho

Key Sources

ASEC Team
SiteGuard Team

AhnLab