# ASEC REPORT

VOL.24 | 2012.01

AhnLab Monthly Security Report

1. Security Trend- Dec. 2011
2. 2011 Security Trend
3. 2011 World Security Trend
4. 2012 Security Threat Forecast

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- Dec. 2011

01. Malicious Code Trend

a. Malicious Code Statistics 05

- Top 20 Malicious Code Reports
- Top 20 Malicious Code Variant Reports
- Breakdown of Primary Malicious Codes
- Comparison of Malicious Codes with Previous Month
- Monthly Malicious Code Reports
- Breakdown of New Malicious Codes
- Top 20 New Malicious Code Reports

b. Malicious Code Issues 10

- Kim Jong-il's death used to spread malware
- Spam exploiting the death of Kim Jong-il hitting inboxes
- Fake videos of Korean celebrities put malware on PC
- Cloud AV 2012 threat
- Private AV Checker
- Zero-day PDF exploit used in a targeted attack
- "I'm in trouble" scam
- Malicious apps infiltrate Google's Android Market

02. Security Trend

a. Security Statistics 19

- Microsoft Security Updates- Dec. 2011

03. Web Security Trend

a. Web Security Statistics 21

- Web Security Summary
- Monthly Blocked Malicious URLs
- Monthly Reported Types of Malicious Code
- Monthly Domains with Malicious Code
- Monthly URLs with Malicious Code
- Top Distributed Types of Malicious Code
- Top 10 Distributed Malicious Codes

b. Web Security Issues 24

- Dec. 2011 Malicious Code Intrusion: Website

### 2. 2011 Security Trend

01. Malicious Code Trend

a. Malicious Code Statistics 25

- Top 20 Malicious Code Reports
- Top 20 Malicious Code Variant Reports
- Breakdown of Primary Malicious Code Types
- Breakdown of New Malicious Code Types
- Top 20 New Malicious Code Reports

b. Malicious Code Issues 29

- Surge in mobile malware
- Storm worm botnet
- Exploitation of Vulnerability in Windows Graphics Rendering Engine
- 3.4 DDoS: Types of network
- LizaMoon mass SQL injection
- 7.7 million account information exfiltrated from Sony PlayStation network
- Zeus source code leaked and Spyeye trend
- Adobe Flash Player zero-day vulnerability
- Jailbreak 3.0 exploits PDF vulnerability
- Zero-day BIND flaw crashes DNS servers

02. Security Trend

a. Security Statistics 32

- 2011 Microsoft Security Updates

03. Web Security Trend

a. Web Security Statistics 33

- Web Security Summary
- Monthly Blocked Malicious URLs
- Monthly Reported Types of Malicious Code
- Monthly Domains with Malicious Code
- Monthly URLs with Malicious Code
- Top Distributed Types of Malicious Code
- Top 10 Distributed Malicious Codes

b. Web Security Issues 36

### 3. 2011 World Security Trend

World Security Trend 38

### 4. 2012 Security Threat Forecast

Security Threat Forecast 39

# 1. Security Trend- Dec. 2011

## 01. Malicious Code Trend

### a. Malicious Code Statistics

### Top 20 Malicious Code Reports

Just like last month, JS/Agent was the most reported malicious code, followed by Exploit/Cve-2011-2140 and Swf/Dropper, respectively. 7 new malicious codes were reported this month.

| Ranking | ↑↓ | Malicious Code | Reports | Percentage |
|---|---|---|---|---|
| 1 | — | JS/Agent | 1,414,471 | 23.6 % |
| 2 | ▲1 | Exploit/Cve-2011-2140 | 673,093 | 11.2 % |
| 3 | ▲6 | Swf/Dropper | 602,840 | 10.0 % |
| 4 | NEW | Java/Cve-2010-0886 | 501,160 | 8.4 % |
| 5 | NEW | Swf/Exploit | 472,412 | 7.9 % |
| 6 | ▼2 | Textimage/Autorun | 464,306 | 7.7 % |
| 7 | ▲3 | Html/Agent | 312,722 | 5.2 % |
| 8 | ▼3 | Win-Trojan/Agent.465408.T | 196,643 | 3.3 % |
| 9 | ▼7 | JS/Downloader | 163,062 | 2.7 % |
| 10 | NEW | Html/Iframe | 160,986 | 2.7 % |
| 11 | ▼3 | JS/Redirector | 150,603 | 2.5 % |
| 12 | ▲1 | Swf/Agent | 115,136 | 1.9 % |
| 13 | ▼2 | JS/Exploit | 108,185 | 1.8 % |
| 14 | NEW | JS/Cve-2010-0806-cc | 106,364 | 1.8 % |
| 15 | ▼9 | Swf/Cve-2011-2140 | 105,452 | 1.8 % |
| 16 | ▼4 | Als/Bursted | 97,523 | 1.6 % |
| 17 | ▼2 | Win32/Induc | 95,597 | 1.6 % |
| 18 | NEW | JS/Shellcode | 89,320 | 1.5 % |
| 19 | NEW | Win-Trojan/Adload.428032.B | 85,293 | 1.4 % |
| 20 | NEW | JS/Cve-2010-0806 | 83,779 | 1.4 % |
| | | | 5,998,947 | 100.0 % |

[Table 1-1] Top 20 Malicious Code Reports

### Top 20 Malicious Code Variant Reports

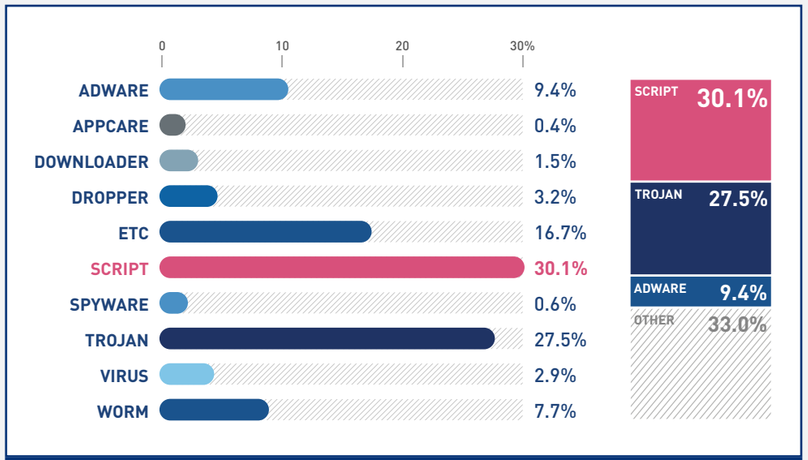
The table below shows the percentage breakdown of the top 20 malicious code variants reported this month. As of December 2011, JS/Agent is the most reported malicious code, representing 16.5% (1,426,157 reports) of the top 20 malicious code variants, followed by Win-Trojan/Agent (1,049,476 reports) and Win-Adware/Korad (777,141 reports).

| Ranking | ↑↓ | Malicious Code | Reports | Percentage |
|---|---|---|---|---|
| 1 | — | JS/Agent | 1,426,157 | 16.5 % |
| 2 | — | Win-Trojan/Agent | 1,049,476 | 12.1 % |
| 3 | ▲2 | Win-Adware/Korad | 777,141 | 9.0 % |
| 4 | — | Exploit/Cve-2011-2140 | 673,093 | 7.8 % |
| 5 | ▲11 | Swf/Dropper | 602,840 | 7.0 % |
| 6 | NEW | Java/Cve-2010-0886 | 501,160 | 5.8 % |
| 7 | NEW | Swf/Exploit | 472,412 | 5.5 % |
| 8 | ▼2 | Textimage/Autorun | 464,418 | 5.4 % |
| 9 | — | Win-Trojan/Onlinegamehack | 457,790 | 5.3 % |
| 10 | ▲8 | Html/Agent | 312,722 | 3.6 % |
| 11 | ▼4 | Win-Trojan/Downloader | 282,250 | 3.3 % |
| 12 | NEW | Win-Trojan/Korad | 213,595 | 2.5 % |
| 13 | ▼3 | Win32/Conficker | 211,492 | 2.4 % |
| 14 | ▼1 | Win32/Virut | 197,554 | 2.3 % |
| 15 | ▼3 | Win32/Autorun.worm | 186,953 | 2.2 % |
| 16 | ▲4 | Win-Downloader/Korad | 179,518 | 2.1 % |
| 17 | ▼14 | JS/Downloader | 163,062 | 1.9 % |
| 18 | ▼4 | Win32/Kido | 162,139 | 1.8 % |
| 19 | NEW | Html/Iframe | 160,986 | 1.8 % |
| 20 | ▼5 | JS/Redirector | 150,603 | 1.7 % |
| | | | 8,645,361 | 100.0 % |

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

## Breakdown of Primary Malicious Code Types

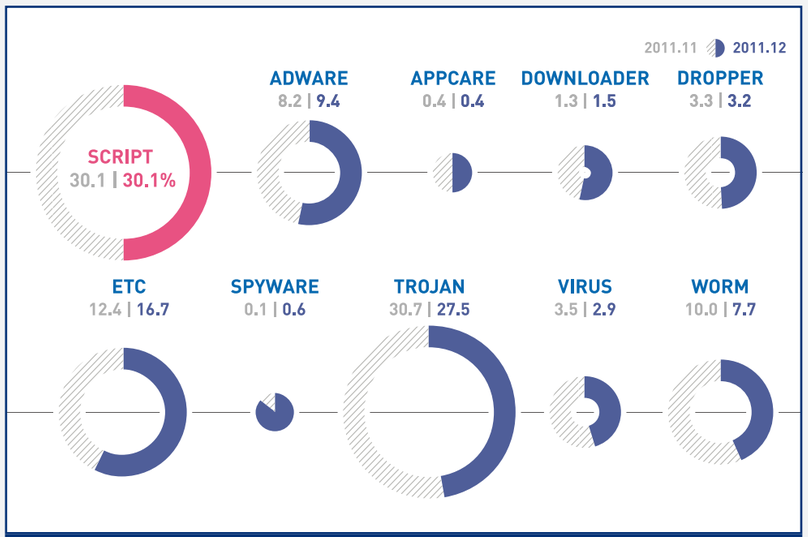
The chart below categorizes the top malicious codes reported this month. As of December 2011, script is the most reported malicious code, representing 30.1% of the top reported malicious codes, followed by Trojan (27.5%) and adware (9.4%).




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

## Comparison of Malicious Codes with Previous Month

Compared to last month, the number of downloader and spyware increased, whereas, the number of Trojan, worm, dropper and virus decreased. The number of appcare is similar to the previous month.

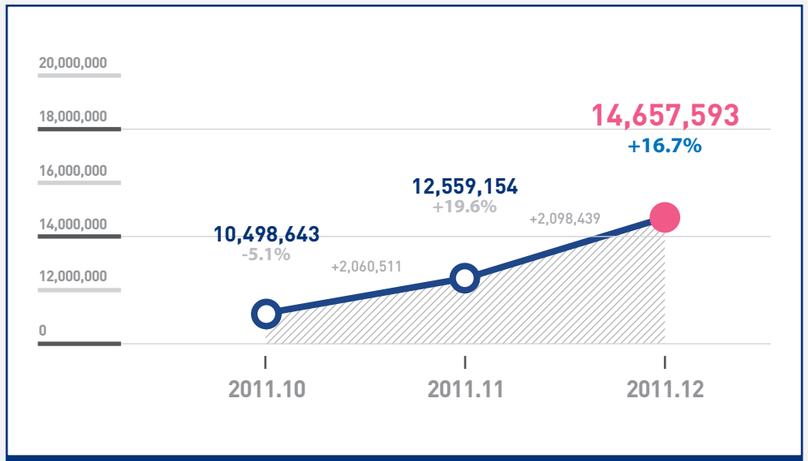



[Fig. 1-2] Comparison of Malicious Codes with Previous Month



## Monthly Malicious Code Reports

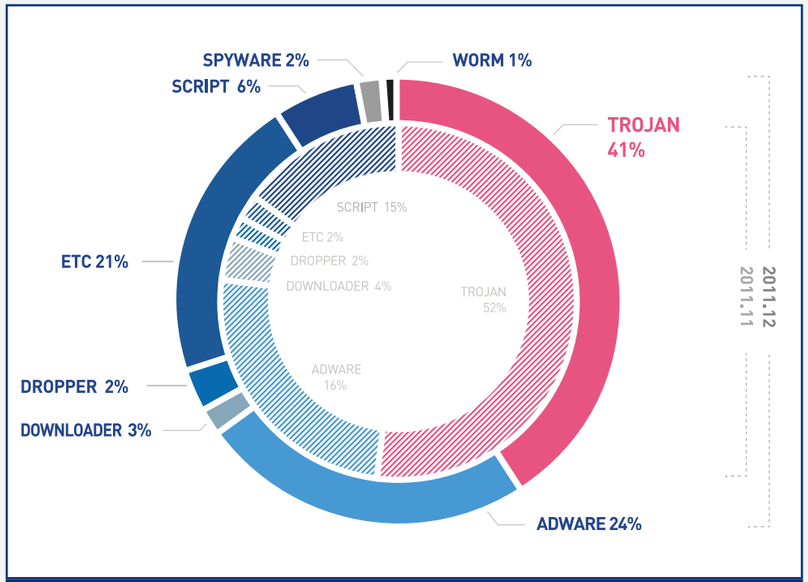
There has been an increase in malicious code reports in December, which climbed 2,098,439 from 12,559,154 the previous month to 14,657,593.




[Fig. 1-3] Monthly Malicious Code Reports

## Breakdown of New Malicious Code Types

As of December 2011, Trojan is the most reported new malicious code, representing 41% of the top reported new malicious codes, followed by adware (24%) and script (6%).




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

## Top 20 New Malicious Code Reports

The table below shows the percentage breakdown of the top 20 new malicious codes reported this month. As of December 2011, JAVA/Cve-2010-0886 is the most reported new malicious code, representing 29.5% (501,160 reports) of the top 20 new malicious codes, followed by JS/Cve-2010-0806-cc (106,364 reports).

| Ranking | Malicious Code | Reports | Percentage |
|---|---|---|---|
| 1 | JAVA/Cve-2010-0886 | 501,160 | 29.5 % |
| 2 | JS/Cve-2010-0806-cc | 106,364 | 6.3 % |
| 3 | Win-Trojan/Adload.428032.B | 85,293 | 5.1 % |
| 4 | Win-Trojan/Agent.907888 | 82,717 | 4.9 % |
| 5 | Win-Spyware/Agent.65536.F | 76,663 | 4.5 % |
| 6 | Win-Adware/KorAd.760832 | 73,991 | 4.4 % |
| 7 | Win-Adware/KorAd.1131008 | 70,406 | 4.1 % |
| 8 | Win-Trojan/Onlinegamehack.45094 | 67,053 | 4.0 % |
| 9 | Win-Trojan/Agent.238608 | 66,520 | 3.9 % |
| 10 | Dropper/Tesa.2764800 | 61,612 | 3.6 % |
| 11 | Win-Adware/KorAd.901632 | 61,227 | 3.6 % |
| 12 | Win-Trojan/Sadenav.325728 | 59,632 | 3.5 % |
| 13 | Win-Trojan/Agent.849488 | 54,626 | 3.2 % |
| 14 | Win-Trojan/Korad.450560.B | 52,721 | 3.1 % |
| 15 | Win-Trojan/Agent.446464.CW | 49,986 | 2.9 % |
| 16 | JS/Expliot | 49,670 | 2.9 % |
| 17 | Win-Trojan/Korad.458752 | 49,147 | 2.9 % |
| 18 | Win-Adware/KorAd.733184 | 43,425 | 2.6 % |
| 19 | Win-Adware/StartPage.114593 | 42,316 | 2.5 % |
| 20 | Win-Trojan/Agent.554496.S | 42,263 | 2.5 % |
| | | 1,696,792 | 100.0 % |

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



# 01. Malicious Code Trend
## b. Malicious Code Issues

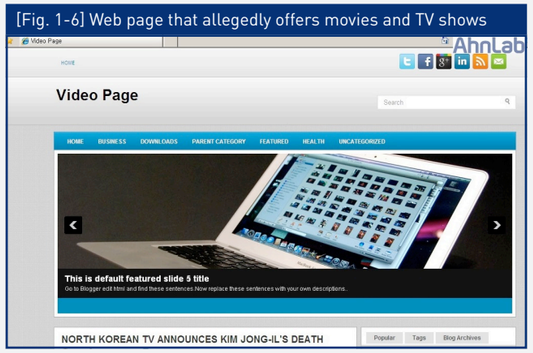
### Kim Jong-il's death used to spread malware

A video about the death of North Korean leader Kim Jong-il has been used to spread malware since the news was announced on December 19, 2011. The video prompts users to click a certain web-link so they can see the whole story:

[Fig. 1-5] Malicious URL link in the description of the YouTube video

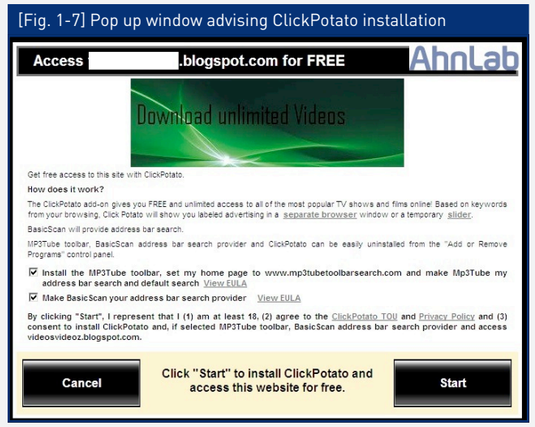

If you click on the link, a new page is opened that appears to offer unlimited TV shows and movies:

[Fig. 1-6] Web page that allegedly offers movies and TV shows




Further a pop up comes up urging you to install an add-on called ClickPotato which comes with additional suspicious toolbars:

[Fig. 1-7] Pop up window advising ClickPotato installation




If a user proceeds to do the installation, a software program mechanically gets copied to the PC before a browser download manager sees a new incoming file.

This file normally contains ad tools, or bots and spyware that give access to target computers via bait for software downloads.

[Fig. 1-9] Toolbar installed

The bait, in the current instance, is a promise for accessing well-known TV films and serials online, free of cost.

V3 detects this malware as:

- Trojan/Win32.ADH
- Adware/Win32.Hotbar
- Trojan/Win32.ADH

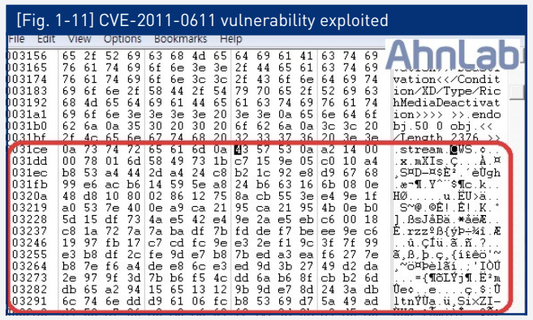
## Spam exploiting the death of Kim Jong-il hitting inboxes

On December 20, 2011, Trend Micro researchers reported that the North Korean leader's death was being leveraged to distribute a Trojan. Spam messages with malicious attachments which contain a Trojan have been detected with subject lines referring to the death of Kim Jong-il.

[Fig. 1-10] Malicious spam using Kim Jong-il as a lure


The attached PDF file is found to be exploiting CVE-2010-2883 and CVE-2011-0611 Vulnerabilities in Adobe Acrobat Reader.

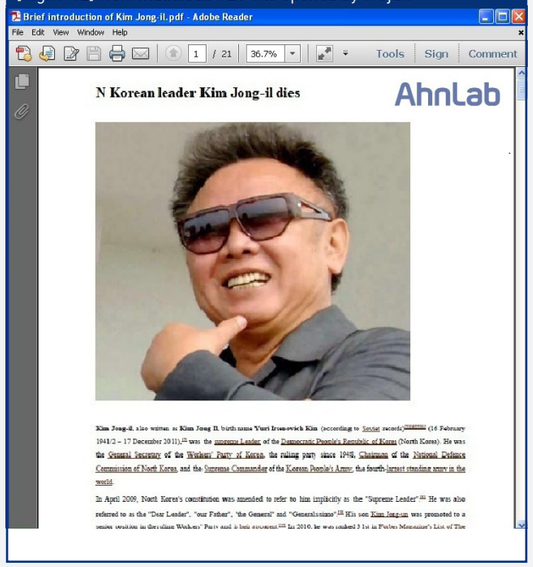
[Fig. 1-11] CVE-2011-0611 vulnerability exploited




The Trojan drops and opens a non-malicious pdf file that contains a picture of Kim Jong-il and his short biography. Upon execution, it checks the version of the Adobe Acrobat on the system. If the version is 9.4 or below, it attempts to exploit the vulnerabilities to drop and execute files.

- C:\Documents and Settings\Tester\Local Settings\Brief introduction of Kim Jong-il.pdf
- C:\Documents and Settings\Tester\Local Settings\abc.scr

[Fig. 1-12] Non-malicious PDF file opened by Trojan




The Trojan joins the files, LOG1.TXT and FABC.SCR, to form ABC.SCR, which it executes afterwards. ABC.SCR creates the following file:

-C:\Documents and Settings\Tester\Local Settings\Application Data\GoogleUpdate.exe

It also creates the following registry key to runs automatically upon boot:

-HKCU\Software\Microsoft\Windows\CurrentVersion\Run
GoogleUpd = ""C:\Documents and Settings\[User]\Local Settings\Application Data\GoogleUpdate.exe""

GoogleUpdate.exe handles outbound connections. After the connection has been made, it connects reversely to a specific system to receive various commands from the attacker.

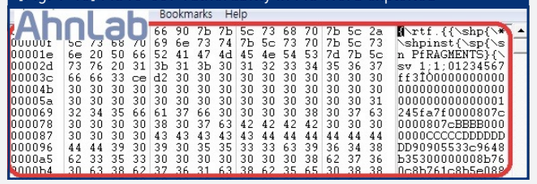
GoogleUpdate.exe:

- forcefully terminates processes;
- executes CMD shell commands; and
- uploads, downloads and deletes files.

Researchers at Trend Micro also encountered other variants of the same theme with file names mentioning the late Korean leader. One of the files was found to exploit MS10-087 vulnerability.



[Fig. 1-13] MS10-087 vulnerabilty in MS Word exploited




V3 detects this malware as:

- PDF/Cve-2010-2883
- Dropper/Cve-2010-3333
- SWF/Cve-2011-0611
- Win-Trojan/Infostealer.156672
- Win-Trojan/Infostealer.91136.B
- Win-Trojan/PcClinet.80384
- Win-Trojan/PcClinet.118784

## Fake videos of Korean celebrities put malware on PC

Recently, a sex tape of a Korean newscaster 'A' was leaked. This was leveraged to spread a fake footage across social network services, including Twitter.

[Fig. 1-14] Twitter account luring users to download fake footage


The twitter account that tweeted the sex video has been created recently and does not show any information about the user. It is used to post the fake sex video disguised as a normal ZIP file If you click the link to download the file, a fake video will get downloaded.

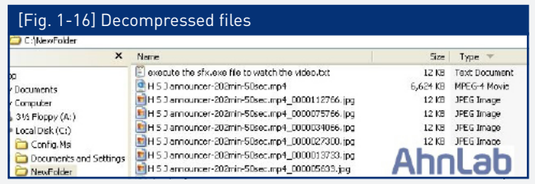
The ZIP file contains JPG files and an SFX file.

[Fig. 1-15] Files in ZIP folder


It make it seem like you have to execute the SFX.EXE file to watch the video.

If you run the EXE file, you will be asked to select the path to decompress the file. The following files will be created on the decompressed folder.

[Fig. 1-16] Decompressed files




Without being aware, netsecurity.exe file will also get decompressed and executed, and netdrvsrty.exe will be created at C:\Windows\System32. Then, the following registry key will be created to run automatically upon boot:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
netsecurityDRV = "C:\WINDOWS\system32\netdrvsrty.exe"

The netdrvsrty.exe is created with Microsoft Visual C++ MFC. It collects the IP addresses of infected systems and creates shortcuts in the IE Shortcuts folder. This malware can be regarded as an adware that changes shortcuts according to the commands of the attacker.

V3 detects this malware as:

- Downloader/Win32.Korad
- Trojan/Win32.Sysckbc
- Dropper/Agent.6596635

## Cloud AV 2012 threat

Christmas and New Year-related social engineering threats increase at the end of every year. We have discovered several malware posing as Christmas cards in December 2011.

On November 30, 2011, Cloud AV 2012, a direct successor of AV Protection 2011 virus, was found. Cloud AV 2012 pretends to be a genuine product to deceive Windows users.

[Fig. 1-17] Fake virus report


This new version performs the same as the previous version. It pretends to update its virus definitions from the Internet. In fact, when you update the program, it is not actually downloading anything but rather just pretending to do so. It was developed to scare you into purchasing the program by misguiding you think your computer is infected.

[Fig. 1-18] License purchase window


Do not trust this hoax and make sure to entirely wipe it off from your PC.

V3 detects this malware as:
- Trojan/Win32.Jorik
- Win-Trojan/Fakescanti.1976320

## Private AV Checker

Most of the APT (Advanced Persistent Threat) launched recently attempted to insert a backdoor into the corporate network via email, instant messenging or SNS.

The malware used are usually tested using a checking tool to see whether it is detected by regular antivirus programs released in the market to maximize success rate. Private AV checker is a paid service that helps cyber criminals pretest whether such malware is detected harmful by usual antivirus programs. We found a private AV checker that checks 35 antiviruses, and charges 1 cent for 1 check, and up to 500 checks for 20USD.

[Fig. 1-19] Private AV checker


The private AV checker website is built using a Russian API (Application Program Interface). The Russian private AV checker we found below also checks 35 antiviruses, including AhnLab's V3 Internet Security 8.0. It charges 15 cents per check, and 25 USD for one month scanning.

[Fig. 1-20] Russian private AV checker




The private AV checker also checks whether the websites used to distribute malware are in the blackList of security companies, and provides VPN service. This is a big threat as it helps increase the success rate of security attacks.

## Zero-day PDF exploit used in a targeted attack

On December 7, 2011, Adobe released an advisory for CVE-2011-2462 vulnerability in the Adobe Reader and Adobe Acrobat products (APSA11-04 Security Advisory for Adobe Reader and Acrobat). The versions affected are:

- Adobe Reader X (10.1.1) and earlier 10.x versions for Windows and Macintosh
- Adobe Reader 9.4.6 and earlier 9.x versions for Windows, Macintosh and UNIX
- Adobe Acrobat X (10.1.1) and earlier 10.x versions for Windows and Macintosh
- Adobe Acrobat 9.4.6 and earlier 9.x versions for Windows and Macintosh

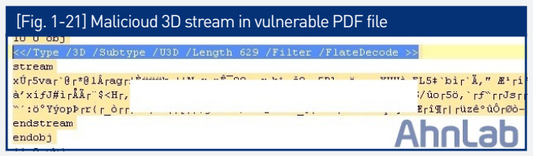
This vulnerability was discovered by Lockheed Martin's Computer Incident Response Team and was found that it is part of a targeted attack.

Security researchers at Symantec confirmed that exploits of an unpatched Adobe Reader vulnerability targeted defense contractors, among other businesses, including telecommunications, manufacturing, computer hardware and chemical companies.

ASEC found at least two vulnerable PDF files circulating using email around the end of November and beginning of December.

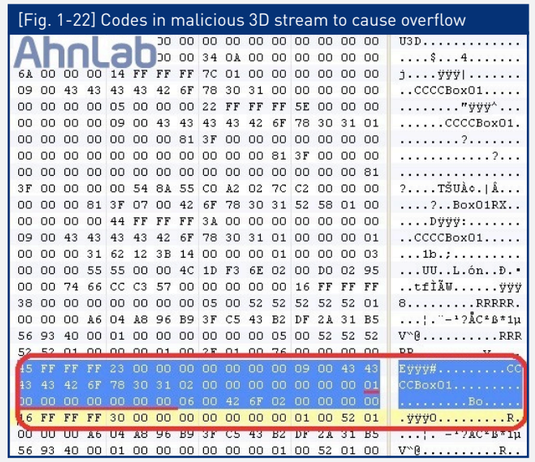
PDF files can contain U3D (Universal 3D) images. The vulnerable PDF files contained malicious 3D stream as below:

[Fig. 1-21] Malicioud 3D stream in vulnerable PDF file




When the user decompresses the malicious 3D stream, a U3D file will be created to cause overflow as shown in the red box below:

[Fig. 1-22] Codes in malicious 3D stream to cause overflow




When the vulnerable file is executed by OpenAction, object number 15 that contains AcroJS is executed in object number 14 as below:

[Fig. 1-23] AcroJS code in object number 14

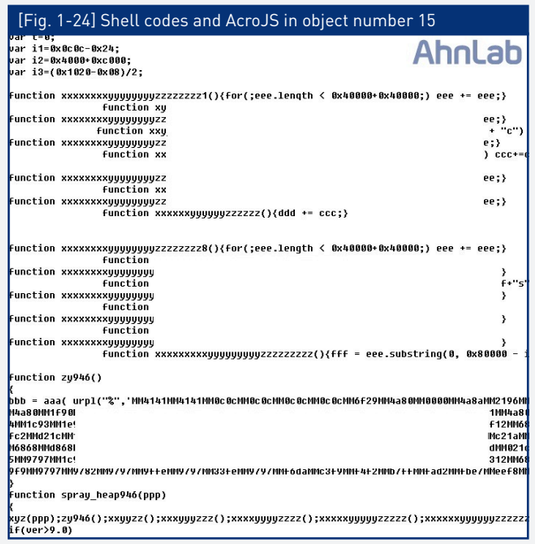
```
4 0 obj
<</Type /Catalog /Outlines 5 0 R /Pages 6 0 R /OpenAction 14 0 R /AcroForm 3 0 R >>
endobj

14 0 obj
<</S /JavaScript /JS 15 0 R >>
endobj
```

AhnLab

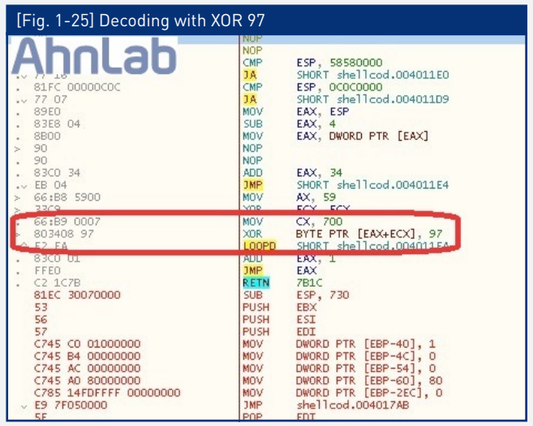
Object number 15 contains AcroJS that loads shellcodes in the memory through heap-spray as below:

[Fig. 1-24] Shell codes and AcroJS in object number 15



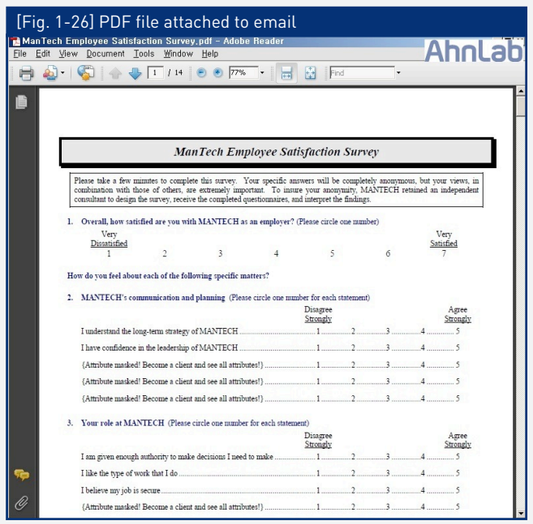
The shell codes get decoded with 'XOR 97' and creates a malware that acts as a backdoor.

[Fig. 1-25] Decoding with XOR 97




When the user opens the vulnerable PDF file, a clean decoy file will open as below:

[Fig. 1-26] PDF file attached to email




And, the following files will be created on the user's system:

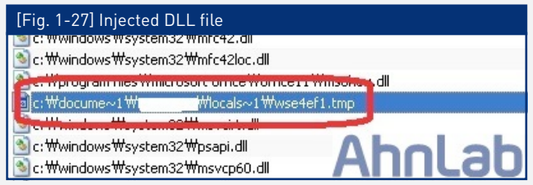
- C:\Documents and Settings\[User]\Local Settings\ctfmon.exe
- C:\Documents and Settings\[User]\Local Settings\Temp\ ManTech Employee Satisfaction Survey.pdf
- C:\Documents and Settings\[User]\Local Settings\pretty.exe
- C:\Documents and Settings\[User]\Local Settings\WSE4EF1. TMP

ManTech Employee Satisfaction Survey.pdf is rigged file disguised as an employee satisfaction survey for employees. The first file to be dropped is "ctfmon.exe" which is later "pretty.exe" after several registry changes. All the files are created with MS Visual C++ and are not compressed. The ctfmon.exe file creates the following registry key to run automatically upon boot:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run
office = "C:\Documents and Settings\[User]\Local Settings\ pretty.exe"

The original malware scans the list of running process looking for Outlook, Internet Explorer o Firefox. If found it injects the dropped DLL file, WSE4EF1.TMP, into the process.

[Fig. 1-27] Injected DLL file




If not successfully injected, it attempts HTTPS connection as below:
'hxxps://www.pr[removed]her.com/asp/kys[removed]_get.asp?name=getkys.kys'

If properly connected, it:
- uploads and downloads files;
- executes CMD shell commands;
- forcefully terminates and restarts the system; and
- acts as a proxy server.

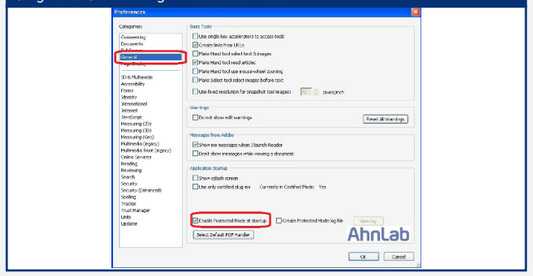
This attack was conducted to steal sensitive information. Adobe has released an update for Adobe Reader 9.x and Acrobat 9.x for Windows on December 12, 2011.

The bug is mitigated by the Protected Mode and Protected View functionality.

On the top menu, go to Edit and select Preferences. Then select 'General'. Check the 'Enable protected mode at startup' checkbox and click OK.

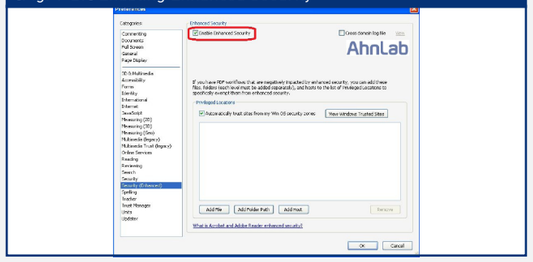


[Fig. 1-28] Enabling Protected Mode




On the top menu, go to Edit and select Preferences. Then select 'Security (Enhanced)' and check the option to 'Enable Enhanced Security'.

[Fig. 1-29] Enabling Enhanced Security



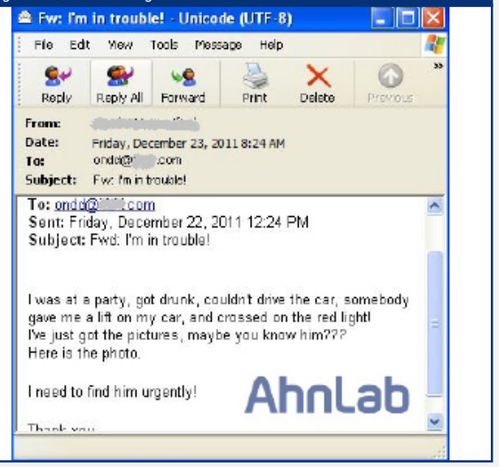

V3 detects this malware as:

- PDF/CVE-2011-2462
- Win-Trojan/Agent.39936.BAT
- Backdoor/Win32.CSon

## "I'm in trouble" scam

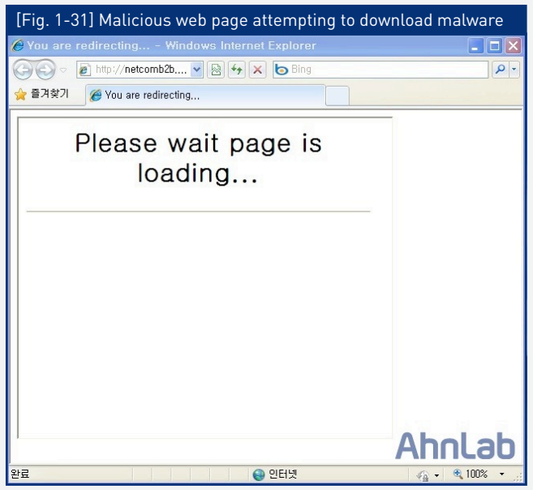
On December 23, 2011, we found several malicious emails that distributed Zeus bot by luring users to connect to webpages by exploiting vulnerabilities in applications. We also found a series of email outbreaks with subjects like "Need your help!" and "I'm in trouble," containing links that lure you into downloading malware. The messages vary, but the goal is the same, to distribute more and more malware to unsuspecting end-users through a hyperlink within the email message. An example of the message is as below:

[Fig. 1-30] Scam using "I'm in trouble" theme




According to Commtouch, the messages and name of the sender varies, but the same approach is used. If you click the link, you will be directed to a malicious web page. The compromised page will display the message, 'Please wait page is loading...', while attempting to download malware onto your system.

[Fig. 1-31] Malicious web page attempting to download malware




Once the malware gets downloaded, it will exploit vulnerabilities in Windows Help and Support Center, Java and Adobe Flash Player.

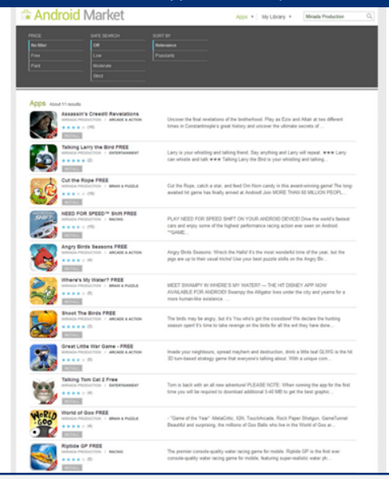
V3 detects this malware as:
- Win-Trojan/Obfuscated.Gen

## Malicious apps infiltrate Google's Android Market

Attackers uploaded malware-laden copies of a number of popular apps, such as Angry Birds, to Google's official Android Market. The malicious apps trick European users into paying premium SMS charges. South Korean users have not been affected by any of the malicious apps.

Google has reportedly removed the malicious applications from Android Market.

[Fig. 1-32] List of malicious apps (Source: Symantec's official blog)



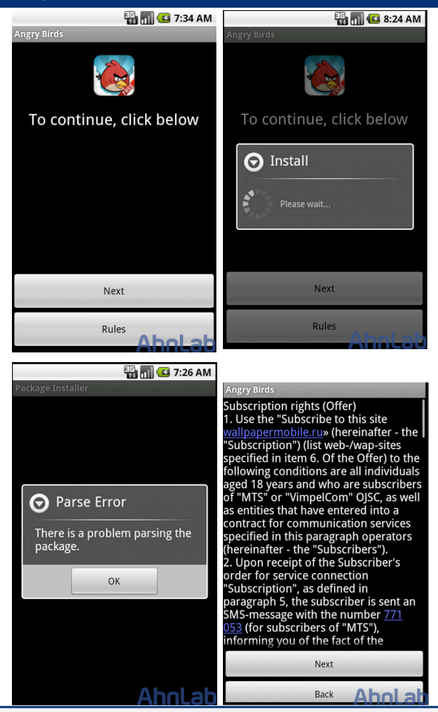

The malicious apps masqueraded as wildly popular games such as Angry Birds and Assassin's Creed.

[Fig. 1-33] Fake application


[Fig. 1-34] Legimate application


When downloaded, the games install a Trojan that sends out text messages to premium-rate phone lines from the user's Android device.

[Fig. 1-35] Installation screen




In the page "Rules", it shows term and condition page. It is similar to the FakeInst variants in last month's ASEC report.

The app comes with terms of service that disclose users would be subscribed to premium services.

The premium-rate Trojans targeted users in 18 countries:

[Table 1-5] Targeted countries

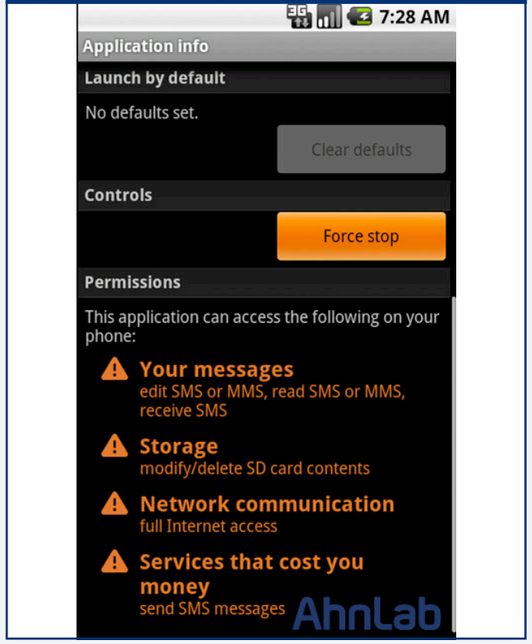
| Country Code | Premium Rate Number | Country |
|---|---|---|
| am | 1121 | Armenia |
| az | 9014 | Azerbaijan |
| by | 7781 | Belarus |
| cz | 90901599 | Czech Republic |
| de | 80888 | Germany |
| ee | 17013 | Estonia |
| fr | 81185 | France |
| gb | 79067 | United Kingdom |



| | | |
|---|---|---|
| ge | 8014 | Georgia |
| il | 4545 | Israel |
| kg | 4157 | Kyrgyzstan |
| kz | 7790 | Kazakhstan |
| lt | 1645 | Lithuania |
| lv | 1874 | Latvia |
| pl | 92525 | Poland |
| ru | 7781 | Russian Federation |
| tj | 1171 | Tajikistan |
| ua | 7540 | Ukraine |

Permissions are displayed by the Android operating system. Understanding these permissions can help users avoid applications which make unnecessary requests.

[Fig. 1-36] Permissions requested by malicious application



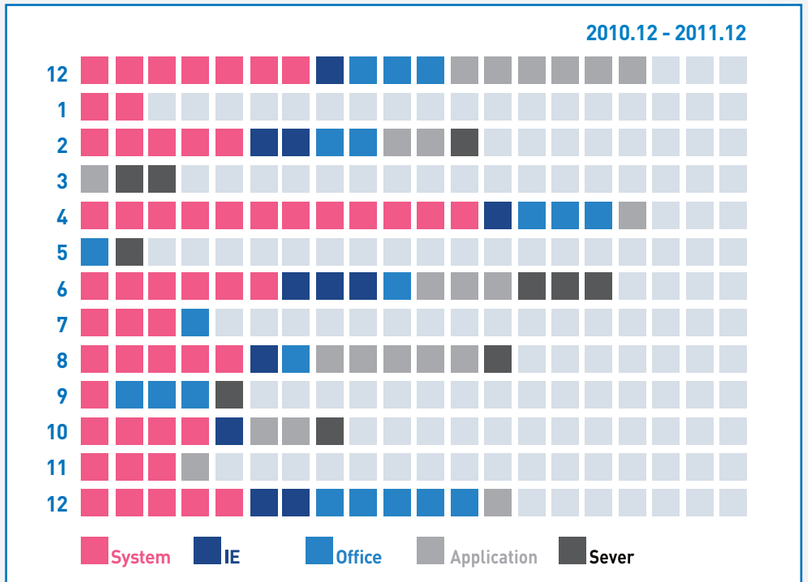

V3 Mobile detects this malware as:

- Android-Trojan/Pavelsms

## 02. Security Trend
### a. Security Statistics

### Microsoft Security Updates- Dec. 2011

Microsoft issued 13 security updates this month. You are advised to apply the updates immediately as 9 of the vulnerabilities can be exploited by malware.




[Fig. 2-1] MS Security Updates

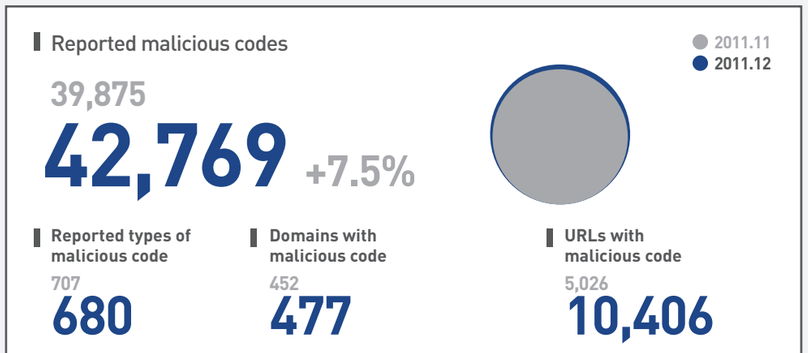
| Severity | Vulnerability |
|---|---|
| Critical | Vulnerability in Windows kernel-mode drivers could allow remote code execution (2639417) |
| Critical | Cumulative Security Update for ActiveX Kill Bits (2618451) |
| Critical | Vulnerability in Windows Media could allow remote code execution (2648048) |
| Important | Vulnerability in Microsoft Office IME (Chinese) could allow elevation of privilege (2652016) |
| Important | Vulnerabilities in Microsoft Office could allow remote code execution (2590602) |
| Important | Vulnerabilities in Microsoft Publisher could allow for elevation of privilege (2607702) |
| Important | Vulnerability in OLE could allow remote code execution (2624667) |
| Important | Vulnerabilities in Microsoft PowerPoint could allow remote code execution (2639142) |
| Important | Vulnerability in Active Directory could allow remote code execution (2640045) |
| Important | Vulnerability in Microsoft Excel could allow remote code execution (2640241) |
| Important | Vulnerability in Windows Client/Server Runtime Subsystem could allow elevation of privilege (2620712) |
| Important | Vulnerabilities in Windows Kernel could allow elevation of privilege (2633171) |
| Important | Cumulative Security Update for Internet Explorer (2618444) |

[Table 2-1] MS Security Updates for Dec. 2011

# 03. Web Security Trend
## a. Web Security Statistics

### Web Security Summary

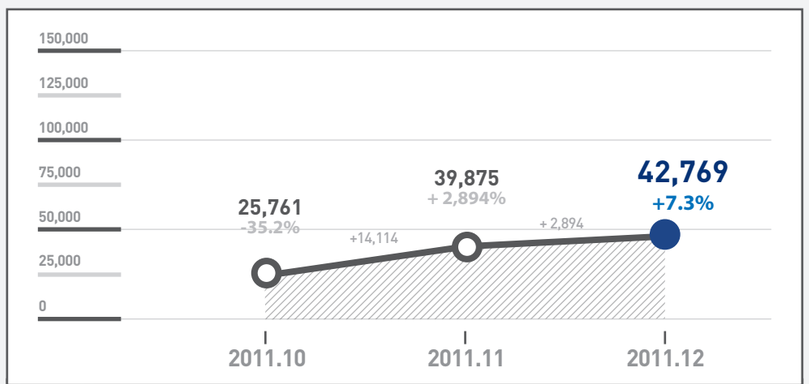
This month, SiteGuard (AhnLab's web browser security service) blocked 42,769 websites that distributed malicious codes. There were 680 types of reported malicious code, 477 reported domains with malicious code, and 10,406 reported URLs with malicious code. The number of reports increased from last month, except for the types of malicious code that decreased.




[Table 3-1] Website Security Summary

### Monthly Blocked Malicious URLs

As of December, the number of reported blocked malicious URLs increased 7% from 39,875 the previous month to 42,769.

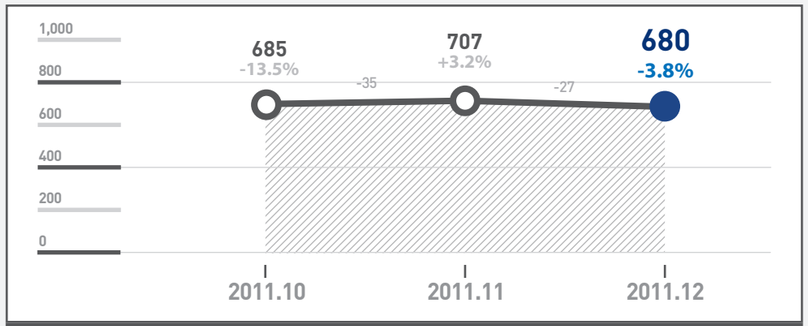



[Fig. 3-1] ] Monthly Blocked Malicious URLs



### Monthly Reported Types of Malicious Code

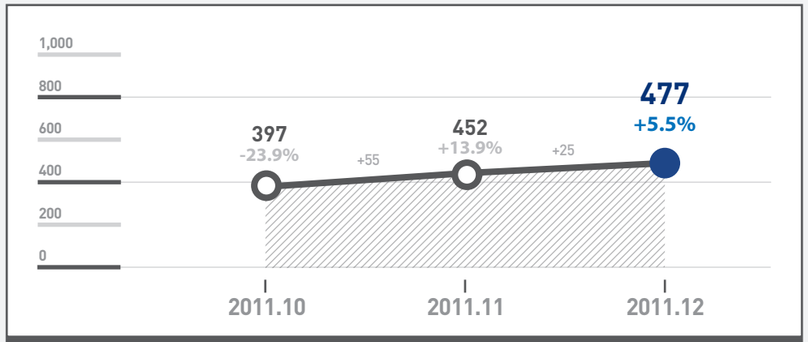
As of December 2011, the number of reported types of malicious code decreased 4% from 707 the previous month to 680.




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

### Monthly Domains with Malicious Code

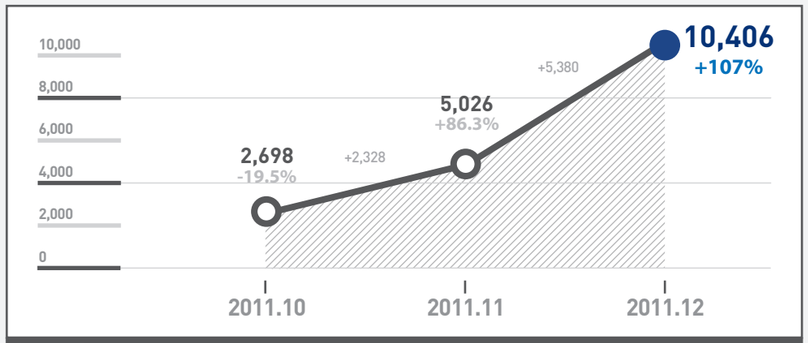
As of December 2011, the number of reported domains with malicious code increased 5% from 452 the previous month to 477.




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

### Monthly URLs with Malicious Code

As of December 2011, the number of reported URLs with malicious code increased 107% from 5,026 the previous month to 10,406.



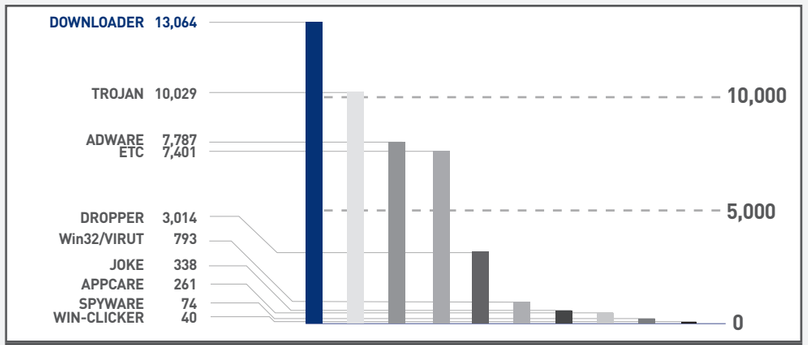

[Fig. 3-4] Monthly URLs with Malicious Code

## Top Distributed Types of Malicious Code

As of December 2011, downloader is the top distributed type of malicious code with 13,064 (30.5%) cases reported, followed by Trojan with 10,029 (23.4%) cases reported.

| TYPE | Reports | Percentage |
|---|---|---|
| **DOWNLOADER** | **13,064** | **30.5 %** |
| TROJAN | 10,029 | 23.4 % |
| ADWARE | 7,787 | 18.2 % |
| DROPPER | 3,014 | 7.0 % |
| Win32/VIRUT | 793 | 1.9 % |
| JOKE | 338 | 0.8 % |
| APPCARE | 229 | 0.5 % |
| SPYWARE | 74 | 0.2 % |
| WIN-CLICKER | 40 | 0.1 % |
| ETC | 7,401 | 17.4 % |
| | **42,769** | **100.0 %** |

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




[Table 3-5] Top Distributed Types of Malicious Code

## Top 10 Distributed Malicious Codes

As of December 2011, Downloader/Win32.Genome is the most distributed malicious code with 4,499 cases reported. 6 new malicious codes, including Win-Adware/Woowa.28672.B, emerged in the top 10 list this month.

| Ranking ↑↓ | | Malicious Code | Reports | Percentage |
|---|---|---|---|---|
| **1** | **▲1** | **Downloader/Win32.Genome** | **4,499** | **20.5 %** |
| 2 | ▲3 | Downloader/Win32.Korad | 3,469 | 15.8 % |
| 3 | ▲5 | Downloader/Win32.Totoran | 3,152 | 14.3 % |
| 4 | ▲2 | Unwanted/Win32.WinKeygen | 2,337 | 10.6 % |
| 5 | NEW | Win-Adware/Woowa.28672.B | 1,653 | 7.5 % |
| 5 | NEW | Win-Downloader/Woowa.270336 | 1,653 | 7.5 % |
| 7 | NEW | Win-Adware/Woowa.61440.B | 1,652 | 7.5 % |
| 8 | NEW | Win-Trojan/Downloader.765408 | 1,417 | 6.5 % |
| 9 | NEW | Adware/Win32.KorAd | 1,225 | 5.6 % |
| 10 | NEW | Unwanted/Win32.WinKeyfinder | 909 | 4.2 % |
| | | | **21,966** | **100.0 %** |

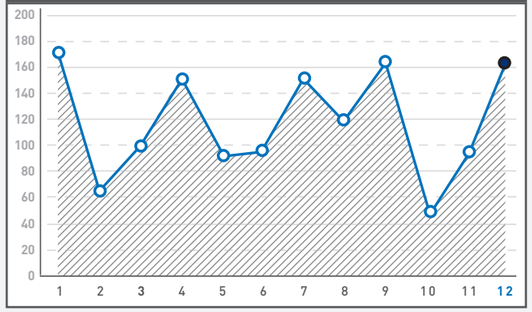
[Table 3-3] Top 10 Distributed Malicious Codes



# 03. Web Security Trend
## b. Web Security Issues

### Dec. 2011 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 doubled from November to December. Many websites, including P2P sites and media websites, were used to distribute malware.

### Top 10 malicious codes distributed via websites

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

| Ranking | Malicious Code | Reports |
|---|---|---|
| **1** | **Win-Trojan/Onlinegamehack.86528.BW** | **59** |
| 2 | Dropper/Win32.OnlineGameHack | 54 |
| 3 | Win-Trojan/Onlinegamehack.74752.AO | 31 |
| 4 | Trojan/Win32.OnlineGameHack | 28 |
| 5 | Win-Trojan/Onlinegamehack.76288.BL | 28 |
| 6 | Win-Trojan/Onlinegamehack.111616.AJ | 26 |
| 7 | Win-Trojan/Onlinegamehack.121487 | 21 |
| 8 | Win-Trojan/Onlinegamehack.136704.O | 21 |
| 9 | Win-Trojan/Onlinegamehack.129113 | 20 |
| 10 | Win-Trojan/Onlinegamehack.77312.AY | 20 |

The table above shows the top 10 malicious codes distributed via websites this month. Win-Trojan/Onlinegamehack.86528.BW was distributed via 59 compromised websites, but fast response prevented significant damages. Distribution of new malware variants is concentrated on the weekend, from Friday evening to Sunday, and there is a lull from Monday morning.

# 2. 2011 Security Trend

## 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 2011. In 2011, Textimage/Autorun was the most reported malicious code, followed by JS/Agent and Win32/Induc, respectively 8 new malicious codes were reported this year.

| Ranking | ↑↓ | Malicious Code | Reports | Percentage |
|---|---|---|---|---|
| 1 | — | Textimage/Autorun | 9,458,847 | 24.2 % |
| 2 | ▲1 | JS/Agent | 6,217,163 | 15.9 % |
| 3 | ▼1 | Win32/Induc | 2,149,558 | 5.5 % |
| 4 | ▲12 | Html/Agent | 1,859,891 | 4.8 % |
| 5 | ▲9 | JS/Downloader | 1,789,695 | 4.6 % |
| 6 | NEW | JS/Redirect | 1,580,959 | 4.1 % |
| 7 | ▼2 | JS/Exploit | 1,545,389 | 4.0 % |
| 8 | — | JS/Iframe | 1,446,928 | 3.7 % |
| 9 | NEW | Swf/Agent | 1,432,679 | 3.7 % |
| 10 | NEW | Win32/Palevo1.worm.Gen | 1,389,561 | 3.6 % |
| 11 | NEW | Exploit/Cve-2011-2140 | 1,351,151 | 3.5 % |
| 12 | ▼6 | Win32/Olala.worm | 1,090,949 | 2.8 % |
| 13 | ▼6 | Win32/Conficker.worm.Gen | 1,045,633 | 2.7 % |
| 14 | ▼10 | Win32/Parite | 1,036,725 | 2.7 % |
| 15 | NEW | Swf/Dropper | 997,347 | 2.6 % |
| 16 | NEW | JS/Redirector | 974,413 | 2.5 % |
| 17 | NEW | Swf/Exploit | 938,527 | 2.4 % |
| 18 | NEW | Win32/Virut.f | 929,265 | 2.3 % |
| 19 | — | JS/Cve-2010-0806 | 926,738 | 2.3 % |
| 20 | ▼8 | Als/Bursted | 870,959 | 2.1 % |
| | | | 39,032,377 | 100 % |

[Table 1-1] Top 20 Malicious Code Reports

#### Top 20 Malicious Code Variant Reports

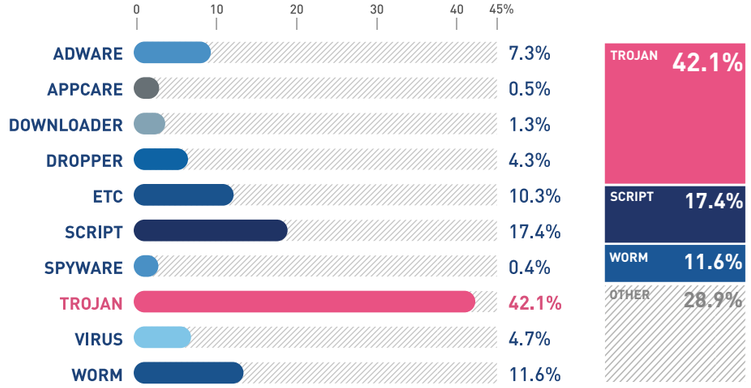
In 2011, Win-Trojan/Onlinegamehack was the most reported malicious code, representing 12.3% (10,770,803 reports) of the top 20 malicious code variants, followed by Win-Trojan/Agent (9,637,067 reports) and Textimage/Autorun (9,460,413 reports).

| Ranking | ↑↓ | Malicious Code | Reports | Percentage |
|---|---|---|---|---|
| 1 | — | Win-Trojan/Onlinegamehack | 10,770,803 | 12.3 % |
| 2 | — | Win-Trojan/Agent | 9,637,067 | 11.0 % |
| 3 | ▲1 | Textimage/Autorun | 9,460,413 | 10.8 % |
| 4 | ▼1 | Win-Trojan/Downloader | 8,788,092 | 10.0 % |
| 5 | ▲4 | JS/Agent | 6,339,235 | 7.2 % |
| 6 | NEW | Win-Trojan/Winsoft | 5,319,281 | 6.1 % |
| 7 | NEW | Win-Adware/Korad | 4,630,273 | 5.3 % |
| 8 | ▼1 | Win32/Conficker | 3,886,522 | 4.4 % |
| 9 | ▼4 | Win32/Autorun.worm | 3,845,424 | 4.4 % |
| 10 | ▼2 | Win32/Virut | 3,491,801 | 4.0 % |
| 11 | ▲6 | Win-Trojan/Adload | 3,220,138 | 3.7 % |
| 12 | ▲2 | Dropper/Malware | 2,634,813 | 3.0 % |
| 13 | ▼2 | Win32/Kido | 2,587,269 | 3.0 % |
| 14 | ▼8 | Win32/Induc | 2,150,951 | 2.5 % |
| 15 | NEW | Win-Trojan/Patched | 1,905,777 | 2.2 % |
| 16 | NEW | Html/Agent | 1,859,894 | 2.1 % |
| 17 | ▼4 | Dropper/Onlinegamehack | 1,847,805 | 2.1 % |
| 18 | NEW | JS/Downloader | 1,789,696 | 2.0 % |
| 19 | ▼4 | Win32/Palevo | 1,739,145 | 2.0 % |
| 20 | NEW | VBS/Solow | 1,604,220 | 1.9 % |
| | | | 87,508,619 | 100 % |

[Table 1-2] 2011 Top 20 Malicious Code Variant Reports

## Breakdown of Primary Malicious Code Types

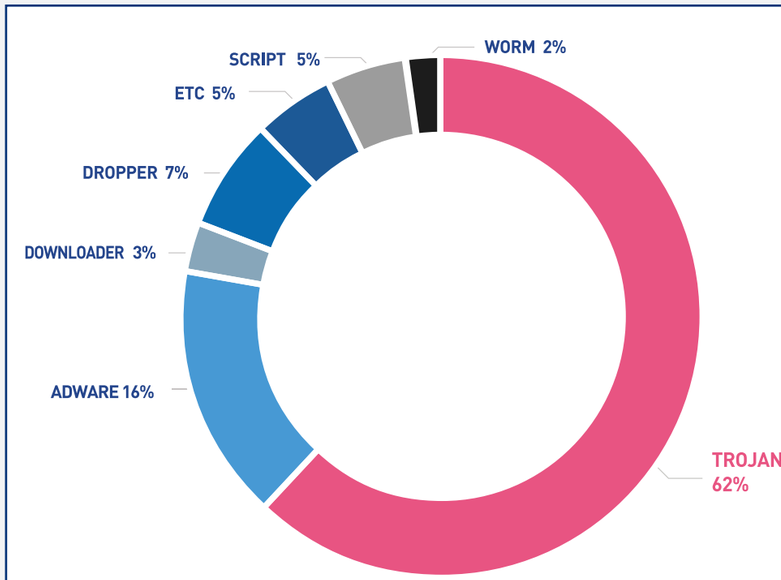
The chart below categorizes the top malicious codes reported this year. In 2011, Trojan was the most reported malicious code, representing 42.1% of the top reported malicious codes, followed by script (17.4%) and worm (11.6%).




[Fig. 1-1] 2011 Breakdown of Primary Malicious Code Types

## 2011 Breakdown of New Malicious Code Types

In 2011, Trojan was the most reported new malicious code, representing 62% of the top reported new malicious codes, followed by adware (16%) and dropper (7%).




[Fig. 1-2] 2011 Breakdown of New Malicious Code Types



## 2011 Top 20 New Malicious Code Reports

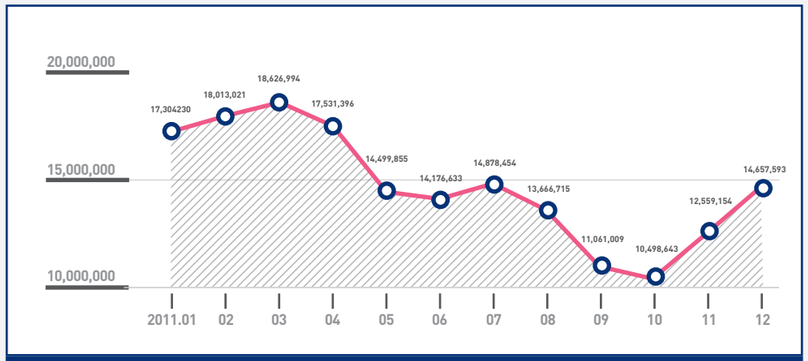
The table below shows the percentage breakdown of the top 20 new malicious codes reported this year. In 2011, Win-Trojan/Patched.CR was the most reported new malicious code, representing 25.8% (757,876 reports) of the top 20 reported new malicious codes, followed by Win-Trojan/Overtls11.Gen (700,456 reports).

| Ranking | Malicious Code | Reports | Percentage |
|---|---|---|---|
| 1 | Win-Trojan/Patched.CR | 757,876 | 25.8 % |
| 2 | Win-Trojan/Overtls11.Gen | 700,456 | 23.9 % |
| 3 | Win-Trojan/Downloader.59904.AK | 278,527 | 9.5 % |
| 4 | Win-Trojan/Winsoft17.Gen | 222,208 | 7.6 % |
| 5 | Win-Trojan/Adload.77312.LPU | 181,176 | 6.2 % |
| 6 | Win-Trojan/Winsoft18.Gen | 104,026 | 3.5 % |
| 7 | Win-Trojan/Winsoft.263168.KX | 75,337 | 2.6 % |
| 8 | Win-Trojan/Winsoft.263168.LO | 73,994 | 2.5 % |
| 9 | Win-Trojan/Agent.339968.EI | 69,762 | 2.4 % |
| 10 | Win-Trojan/Agent.323584.FK | 68,946 | 2.3 % |
| 11 | Win-Trojan/Winsoft.281088.GHF | 52,943 | 1.8 % |
| 12 | Win-Trojan/Winsoft.281088.GGM | 46,160 | 1.6 % |
| 13 | Win-Trojan/Winsoft.263168.LR | 40,889 | 1.4 % |
| 14 | Win-Trojan/Fakeav.182312 | 40,350 | 1.4 % |
| 15 | Win-Trojan/Adload.267776.F | 39,963 | 1.4 % |
| 16 | Win-Trojan/Adload.267264.B | 39,301 | 1.3 % |
| 17 | Win-Trojan/Downloader.163840.BG | 38,461 | 1.3 % |
| 18 | Win-Trojan/Downloader.550912 | 37,049 | 1.3 % |
| 19 | Win-Adware/BHO.WowLinker.615424 | 34,842 | 1.2 % |
| 20 | Win-Trojan/Adload.321536.D | 33,034 | 1.0 % |
| | | 2,935,300 | 100 % |

[Table 1-3] 2011 Top 20 New Malicious Code Reports

## Monthly Malicious Code Reports

This year, there has been an increase in malicious code reports. The number of reports climbed 31,376,435, from 146,097,262 last year to 177,473,697 this year.




[Fig. 1-3] Monthly Malicious Code Reports

# 01. Malicious Code Trend
## b. Malicious Code Issues

### Surge in mobile malware

**1. Rise in mobile pickpocketing**

In 2011, monetization was a key factor that increased the number of mobile malware. Malware writers steal money directly from smartphone users by accessing their mobile devices' ability to charge phone bills via SMS and phone calls. This type of malware sends SMS messages to premium rate numbers without the user's knowledge. Android-Trojan/Pavelsms is the

most recently discovered monetizing malware, which is also known as the 'ruFraud'. The fraudulent SMS code is gated on the user's country (as indicated by their SIM).

**2. Fake malware disguised as famous applications**

Malware disguised as popular applications, such as Google Search, Google+, Angry Birds, Opera and Skype, were discovered in the Android Market. To the naked eye, there is no difference found between a legitimate app and a malicious one, except their span of permissions over the mobile device. Repackaging was also another increasingly used tactic in which a malware writer takes a legitimate application, modifies it to include malicious code, and then republishes it.

**3. Growth in mobile malware that invades privacy**

Malware that records phone calls and collects personal information such as GPS, text messages, e-mails, and call logs, among other things is on the rise. It is becoming a serious problem for Android users. Android-Spyware/Nicky steals text messages, GPS and call logs and sends them to a specific system (Refer to http://asec.ahnlab.com/320 and http://core.ahnlab.com/290). Mobile-stalking is going to increase as fast as mobile accessibility does.

**4. Malware steals online banking details**

Zeus Trojan, notorious for stealing banking information, has been readapted to mobile environments. Zitmo (ZeuS-in-the-Mobile), a mobile variant of Zeus, targeted Symbian, Windows Mobile and Blackberry. However, the latest version brings Zitmo to the rapidly growing mobile platform, Google's Android. The new variant of the Zitmo trojan cleverly passes itself as a security tool from the online security company, 'Trusteer'. It intercepts SMS messages

### Storm worm botnet

Storm worm was first reported on January 17, 2007, and spread fast from January 19 to infect 8% of computers worldwide. This worm disguises itself as an email news alert on the weather and urges email recipients to download and run an executable file. Another Storm worm attack disguised as 'FBI vs FaceBook' spread in 2008. This type of worm that spread using an email message with a subject line about a social issue is dubbed Storm worm or Wale Dac. Infected systems will send out spam to other computers. The number of such worm is on the rise and they usually spread via email. Users are advised to exercise increased caution before opening links or attachments in emails from unfamiliar addresses.

### Exploitation of Vulnerability in Windows Graphics Rendering Engine

Exploitation of a stack-based buffer overflow in the handling of thumbnails by Windows Graphics Rendering Engine (Shimgvw.dll) could cause remote code execution. The message was sent in Chinese, from a Korean hosting company's IP address, using a Yahoo Taiwan webmail address (@yahoo.com.tw) via zombie PCs in Korea. A malicious word document was sent inside a 7zip archive folder with 43 non-malicious image files. Due to this, a recipient is likely to switch to the 'Thumbnails' view, which triggers the exploit.

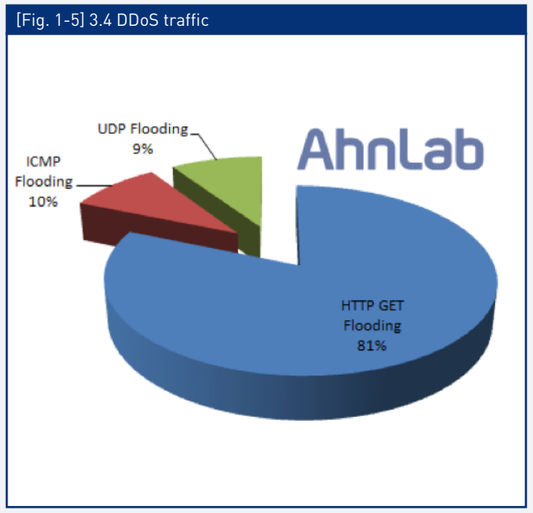


[Fig. 1-4] Email message


### 3.4 DDoS: Types of network

The DDoS client supports four different types of network for HTTP GET flooding, ICMP flooding, UDP flooding and C&C server communication as below:

[Fig. 1-5] 3.4 DDoS traffic




HTTP GET Flooding (81%) > ICMP Flooding (10%) > UDP Flooding (9-10%)

The table below shows the amount of traffic per infected botnet. 31,030 computers were found to be infected.

[Table 1-4] Traffic per botnet (per attack)

| Infected computers | Avg. packets/sec | Avg. packet size | Avg. bytes/sec | Avg. Mbit/sec |
|---|---|---|---|---|
| 1PC | 25 | 174 | 4.2K | 0.033M |
| 31,030PCs | 776K | - | 130M | 1G |

[Table 1-5] Traffic type per botnet (per active attack)

| Attack type | Avg. packets/sec | Avg. packet size | Avg. bytes/sec | Avg. Mbit/sec |
|---|---|---|---|---|
| HTTP GET Flooding | 20.43 | 144.522 | 2,952.56 | 0.024 |
| ICMP Flooding | 2.355 | 129.414 | 302.13 | 0.002 |
| UDP Flooding | 2.335 | 406.229 | 948.38 | 0.008 |
| attack total | 25.12 | | 4,203.07 | 0.034 |

### LizaMoon mass SQL injection

A US security provider, Websense, reported a mass SQL injection attack. This attack is called LizaMoon from lizamoon.com, which is the first domain users are redirected to. It hit over 226,000 websites.

[Fig. 1-6] Korean websites hacked by LizaMoon SQL injection


### 77 million account information exfiltrated from Sony PlayStation Network

Sony has admitted that hackers have stolen the personal information of customers who use the company's online PlayStation Network. While Sony officials don't believe credit card information was taken, they say that hackers may have taken names, addresses, email addresses, birthdates and passwords among other things. Sony discovered that between April 17 and April 19, 2011, certain PlayStation Network and Qriocity service user account information was compromised in connection with an illegal and unauthorized intrusion into their network. There is no evidence that credit card information has been stolen, but there is a possibility. Sony subscribers

need to be aware that the information stolen could be used in a multitude of ways, so it is essential to be on guard and implement basic measures.

### 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 to device new malware.

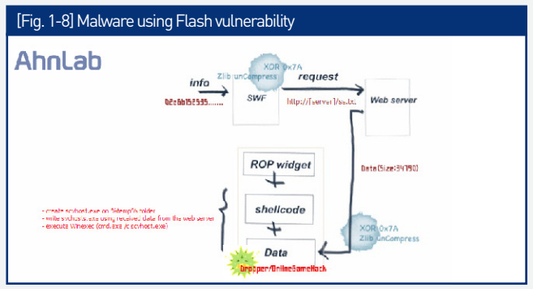
[Fig. 1-7] Zeus Command and Control (C&C) Servers


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.

### Adobe Flash Player zero-day vulnerability

A malware that exploits the vulnerabilities in Adobe Flash Player was distributed via compromised websites. Accessing these malicious websites will infect your system.

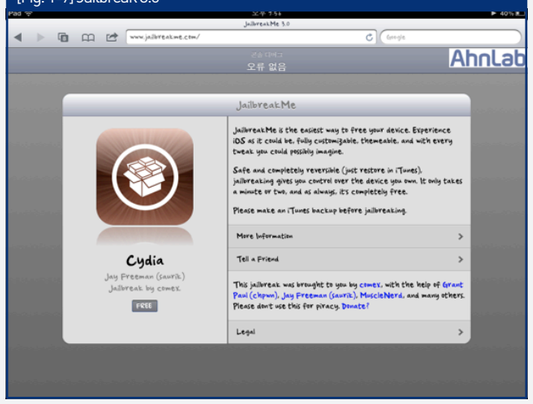
[Fig. 1-8] Malware using Flash vulnerability




### Jailbreak 3.0 exploits PDF vulnerability

Jailbreakme 3.0 that supports the latest and every available iOS device, including iPad 2, was released this month. It can jailbreak your device in 5 seconds. All you need to do is visit JailbreakMe.com on your iPhone, iPod Touch or iPad's Mobile Safari browser and tap on the Free button and then tap on the Install button. This should jailbreak your iOS device and install Cydia. The vulnerability was exploited for jailbreaking devices this time, but it could potentially be used by malicious hackers to install malware onto your device.

[Fig. 1-9] Jailbreak 3.0




### Zero-day BIND flaw crashes DNS servers

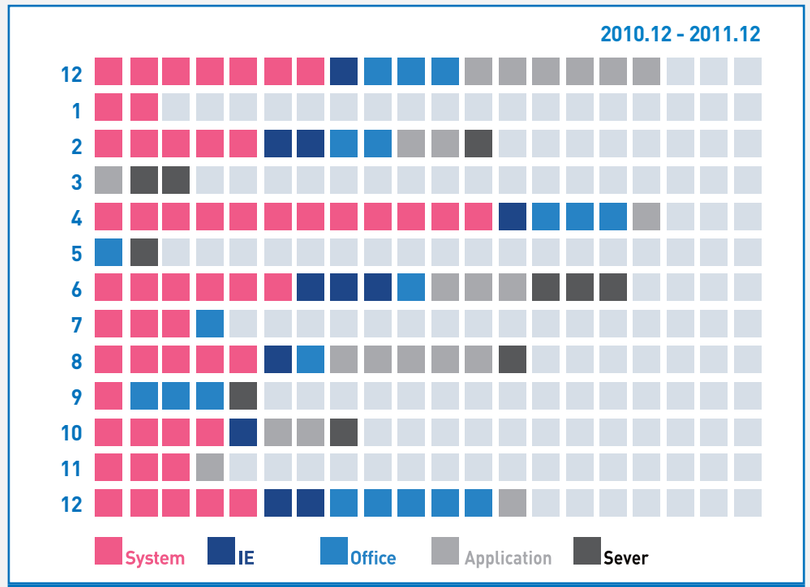
A zero-day vulnerability is causing BIND 9 DNS servers to crash. BIND (Berkeley Internet Name Daemon) is the most commonly used DNS server on the Internet in the US. The issue forces the servers to cache an invalid record, and affected servers crashed after logging an error in query.c with the following message: "INSIST(! dns_rdataset_isassociated(sigrdataset)).



## 02. Security Trend
## a. Security Statistics

### 2011 Microsoft Security Updates

Microsoft issued 99 security updates this year, which is 4 updates less than the 103 security updates released in 2010. Like last year, there were lots of flaws in the system, as well as application vulnerabilities in IE, MS Office, and Adobe PDF and SW.

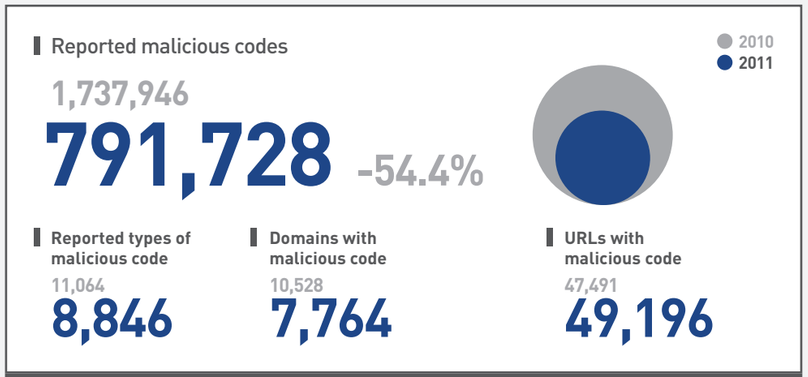



[Fig. 2-1] MS Security Updates

# 03. Web Security Trend
## a. Web Security Statistics

### Web Security Summary

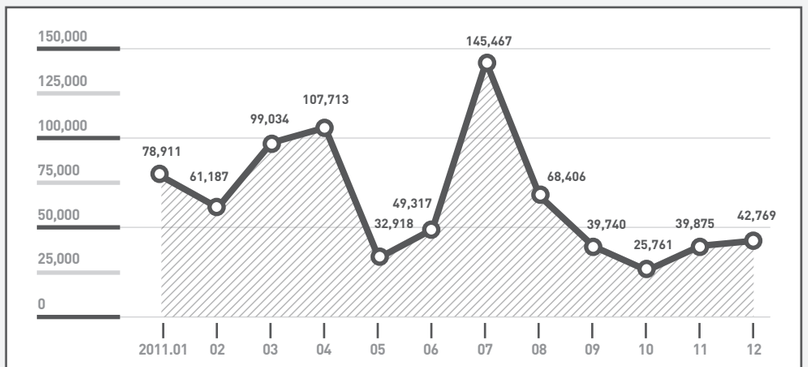
This year, SiteGuard (AhnLab's web browser security service) blocked 791,728 websites that distributed malicious codes. There were 8,846 types of reported malicious code, 7,764 reported domains with malicious code, and 49,196 reported URLs with malicious code.




[Table 3-1] 2011 Website Security Summary

### Monthly Blocked Malicious URLs

In 2011, the number of reported blocked malicious URLs decreased 54% from 1,737,946 last year to 791,728.

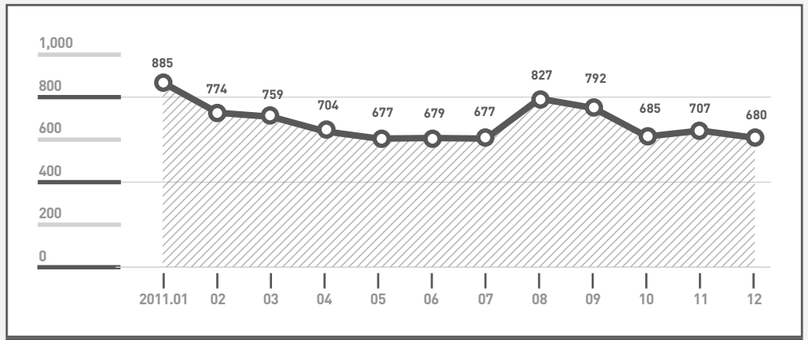



[Fig. 3-1] ] 2011 Monthly Reported Malicious Codes



### Monthly Reported Types of Malicious Code

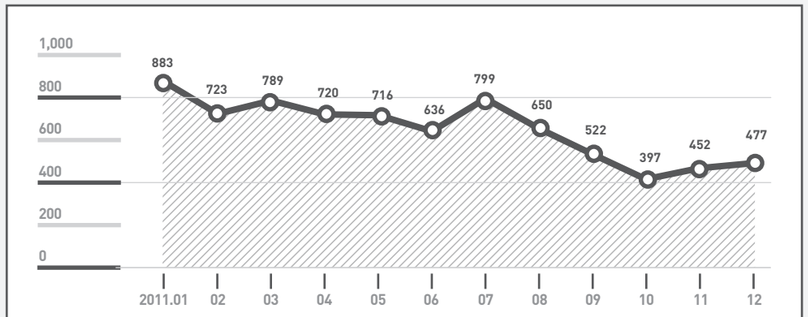
In 2011, the number of reported types of malicious code decreased 20% from 11,064 last year to 8,846.




[Fig. 3-2] 2011 Monthly Reported Types of Malicious Code

### Monthly Domains with Malicious Code

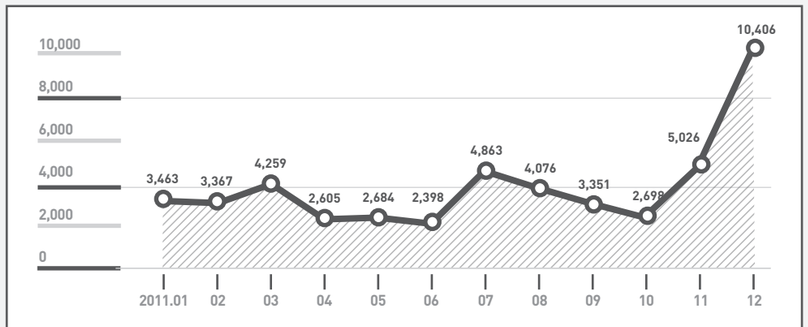
In 2011, the number of reported domains with malicious code decreased 26% from 10,528 last year to 7,764.




[Fig. 3-3] 2011 Monthly Domains with Malicious Code

### Monthly URLs with Malicious Code

In 2011, the number of reported URLs with malicious code increased 4% from 47,491 last year to 49,196.



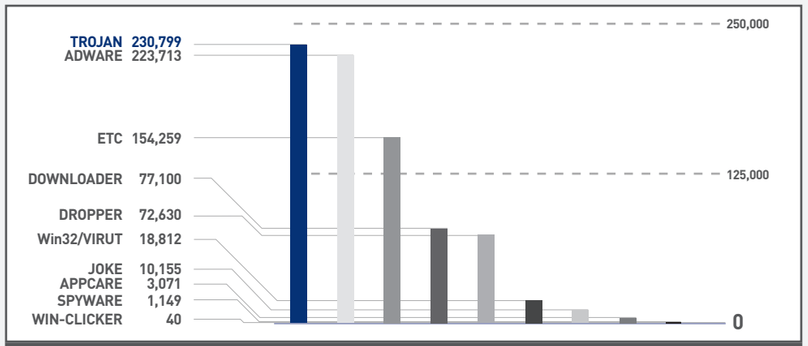

[Fig. 3-4] 2011 Monthly URLs with Malicious Code

## Top Distributed Types of Malicious Code

In 2011, Trojan was the top distributed type of malicious code with 230,799 (29.2%) cases reported, followed by adware with 223,713 (28.3%) cases reported.

| TYPE | Reports | Percentage |
|---|---|---|
| **TROJAN** | **230,799** | **29.2 %** |
| ADWARE | 223,713 | 28.3 % |
| DOWNLOADER | 77,100 | 9.7 % |
| DROPPER | 72,630 | 9.2 % |
| Win32/VIRUT | 18,812 | 2.4 % |
| JOKE | 10,155 | 1.3 % |
| APPCARE | 3,071 | 0.4 % |
| SPYWARE | 1,149 | 0.1 % |
| WIN-CLICKER | 40 | 0.1 % |
| ETC | 154,259 | 19.3 % |
| | **791,728** | **100.0 %** |

[Table 3-2] 2011 Top Distributed Types of Malicious Code




[Table 3-5] Top Distributed Types of Malicious Code

## Top 10 Distributed Malicious Codes

In 2011, Win32/Induc was the most distributed malicious code with 69,889 cases reported, followed by Win-Adware/ADPrime.837241 with 50,488 cases reported.

| Ranking | ↑↓ | Malicious Code | Reports | Percentage |
|---|---|---|---|---|
| **1** | **▲1** | **Win32/Induc** | **69,889** | **8.9 %** |
| 2 | NEW | Win-Adware/ADPrime.837241 | 50,488 | 6.4 % |
| 3 | ▼2 | Win-Adware/Shortcut.InlivePlayerActiveX.234 | 37,975 | 4.8 % |
| 4 | NEW | Win-Trojan/Agent.286616 | 34,689 | 4.4 % |
| 5 | NEW | Win-Trojan/Downloader.765408 | 32,665 | 4.2 % |
| 6 | NEW | Virus/Win32.Induc | 24,697 | 3.1 % |
| 7 | NEW | Win-Adware/ToolBar.Cashon.308224 | 22,782 | 2.9 % |
| 8 | NEW | Win-Downloader/KorAd.83968 | 22,549 | 2.9 % |
| 9 | NEW | Win-Adware/Shortcut.Unni82.3739648 | 19,412 | 2.5 % |
| 10 | NEW | Win-Adware/KorZlob.3919486 | 14,617 | 1.9 % |
| | | | **329,763** | **42.0 %** |

[Table 3-3] 2011 Top 10 Distributed Malicious Codes



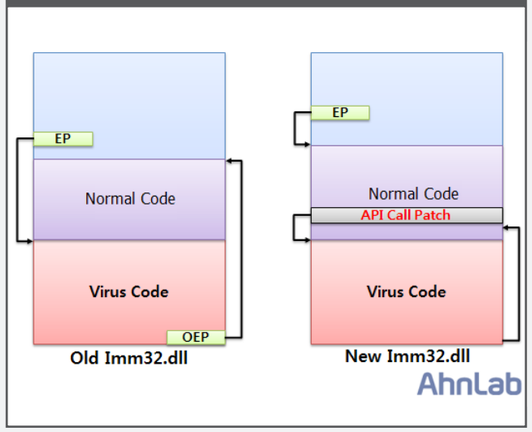
# 03. Web Security Trend
## b. Web Security Issues

The characteristics of malware distributed via compromised websites in 2011 are as below:

### System file tampering

System files, such as imm32.dll and ws2help.dll, can be modified to infect systems. Malware that uses imm32.dll to compromise systems modifies the imm32.dll to load the malicious DLL file it creates.

[Fig. 3-6] Modified imm32.dll




Malware that uses ws2help.dll to infect systems backs up the ws2help.dll in another name to replace the original ws2help.dll with a malicious one. There is a bug in some variants: it shows BSOD and inability to properly startup the system by copying the modified file to the wrong directory. If the BSOD has been shown once, it can repeat the symptoms of an infinite reboot.

[Fig. 3-7] Bug found in malware that replaces ws2help.dll

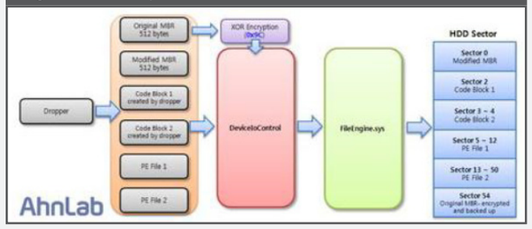
```
kd> dd 0006f718 + 0xb8
0006f7d0  10018132 0000001b 00010346 0006f9e4
0006f7e0  00000023 0000027f 00000000 00000000

kd> u 10018132
10018132 80b0000000ffff  xor     byte ptr [eax-1000000h],0FFh
10018139 ff              ???
                         ???
AhnLab                   inc     dword ptr [eax+088h]
```

### Bootkits

A bootkit is a type of malware that infects the Master Boot Record (MBR, the first 512 bytes of the physical hard drive) to allow the malicious program to be executed before the operating system boots.

[Fig. 3-8] Bootkit process



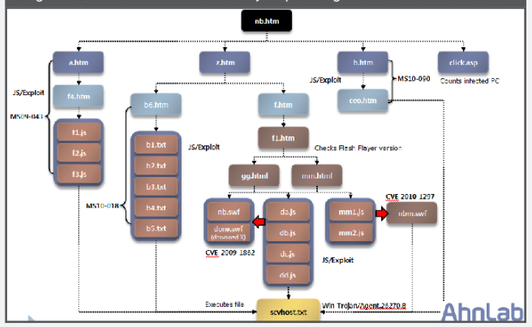

### Exploitation of multiple vulnerabilities

This year, Trojan horse that exploits the vulnerabilities in application programs, including Internet Explorer, Firefox and Adobe Flash Player, to monetize stolen information was distributed the most. Cyber criminals overseas used Zeus and SpyEye to steal online banking details; where as Korean hackers mostly stole account information from online game. The five most exploited vulnerabilities are as below:

[Table 3-4] Top 5 exploited vulnerabilities

| Rank | Vulnerability | Application |
|---|---|---|
| **1** | **MS10-018** | **Internet Explorer** |
| 2 | CVE-2011-2110 | Adobe Flash Player |
| 3 | CVE-2011-2140 | Adobe Flash Player |
| 4 | CVE-2011-0611 | Internet Explorer |
| 5 | CVE-2011-0609 | Adobe Flash Player |

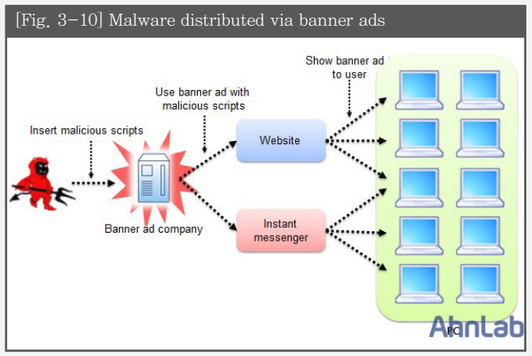
[Fig. 3-9] Malware distributed by exploiting vulnerabilities




### Distribution of malware via banner advertisements

This year, most of the malicious websites that distributed malware use banner ads as a source of malware. Hackers did not compromise websites to distribute the malware, but inserted malicious scripts into the banner ads provided by specific banner ad companies. Even though the websites themselves were not "malicious", they became malware distributors by using compromised banner ads.

[Fig. 3-10] Malware distributed via banner ads






## 3. 2011 World Security Trend

### World Security Trend

This year, many threats were targeted against specific companies and industries. Most security companies expect this trend to continue in 2012.

### World malicious code trend

The variants of malware are being restricted to specific regions. With the regionalization of malware, the world statistic of malicious codes is no longer significant. According to the malware statistics released by top security providers, Conficker worm, Autorun worm, Virut virus, Sality virus and rogue antivirus were reported in multiple countries.

### Malicious code distribution channels

Attackers still distribute malicious codes by hacking websites and exploiting vulnerabilities to insert malicious codes into websites, or via USB flash drive. The method of distributing malicious codes via email or social network sites, such as Facebook, MySpace and Twitter is also increasing.

### Data exfiltration and APT

Data exfiltration is on the rise, and so are Advanced Persistent Threats. A new threat called Duqu that appears to have evolved from the Stuxnet worm was discovered this year. Unlike Stuxnet, Duqu does not directly target industrial control systems though the information it gathers could be used to create the next Stuxnet. The threat uses a custom C&C protocol and is configured to run for 36 days. After 36 days, the threat will automatically remove itself from the system. McAfee revealed details of targeted attacks in August, and Symantec discovered an industrial espionage campaign using the Poisonlvy backdoor against 40 chemical companies in October. In November, hackers hit oil, gas and defense companies in Norway.

### Malwarefor political espionage

On October 26, the day of by-election in Korea, DDoS attacks temporarily paralyzed the National Election Commission (NEC) website. Massive DDoS attacks were launched against independent websites in Russia on election day, December 4. The hacker group, Anonymous, is currently engaged in an effort to hack Israeli websites as part of a campaign called Operation Free Palestine. Politically motivated attacks by "hacktivists" will increase.

## 04. IV. 2012 Security Threat Forecast

### Evolving APT threats

APT attacks targeting enterprises and organizations will continue in 2012, and the method to deliver the attack is expected to become increasingly sophisticated. Hitherto, the major attack route used for APT attack was sending a fake work email to specific members of enterprises or organizations targeted. The attackers collected information via SNS and then impersonated somebody trusted based on the details, to lure the targets into opening spam mail with malicious attachments or links. Some attackers modified update files of widely used software. In the future, intrusion is expected to increase using smartphones, or third-party devices or software.

### Elevated mobile threat level

In 2010, there was anticipation for possibilities of producing and distributing malicious applications that run on smartphones, especially on those based on the Android OS. In 2011, malicious applications were massively produced. In 2012, the malicious applications are expected to be more sophisticated. The techniques used to create PC malware will adopted by cyber criminals.

Examples of such techniques include stealth technique that hides malware inside the smartphone, and elevation of privilege to exploit the vulnerabilities in the mobile device's operating system. There are also social engineering techniques that can be used to lure users to download malware from malicious websites, or automatically infect mobile devices using the vulnerabilities in mobile browser. There are also likely to be malicious applications that steal financial or credit card information from online banking or shopping applications installed on smartphones.

### Increase in security threats on social media platforms

As SNS becomes an increasingly popular channel for instant communication and information-sharing worldwide, security threats on social networks are also on the rise. As shortened-URLs do not show the full website address, cyber criminals are using shortened URLs as links to malicious sites. In 2012, the use of shortened URLs as links to malicious sites is expected to increase, along with SNS to launch APT attacks.

### Regionalization of threats that exploit application vulnerabilities

In 2011, the number of attacks against the vulnerabilities in widely used applications decreased, while the number of exploits against the vulnerabilities in region-specific applications increased. A typical example includes Hangul, the Korean word processor program. A vulnerable Hangul file was



distributed via spam mail. This trend is expected to continue in 2012 and used in various security threats, such as APT attacks.

### Increase in attacks targeting infrastructure and industrial systems

Whether for financial gain, or for political or religious reasons, attacks against infrastructure and/or industrial systems are expected to increase. This could expand into fully-fledged cyber warfare between countries if a national institution is found to be directly or indirectly involved in such an attack. An internal system accidentally connected to the Internet or an external system can trigger an attack. Attacks are also likely to exploit the vulnerabilities in specific software used in national industrial or institutional systems.

### Threats specific to cloud-computing and virtualized environments

Recently, a large number of companies have been adopting cloud services, based on virtualization technologies. While offering the maximum utilization of resources, cloud services and virtualization technologies can be turned into a security threat, should their vulnerabilities become exploited. In fact, many security vulnerabilities were found in the virtualization products in 2011, and SpyEye, which steals financial information, was distributed by exploiting the vulnerability in Amazon's cloud-service. AhnLab predicts that with the increase in cloud-computing and virtualization services, they will become the target of various types of malware.

### Increase in threats against network-connected systems such as Smart TV

Security threats against smart devices, such as Smart TV and smartphone that have embedded software to link the device to a network, are expected to increase. In particular, home appliances, which usually have a long replacement cycle, are thought to possibly become exposed to persistent attacks. For example, in Japan, a DVD recorder connected to the Internet was attacked. Also, at a security conference, a hacker gave a demonstration on remotely controlling a system by installing Linux on a Nintendo DS terminal. With more embedded systems getting linked to a network, the more likely they are to become targeted in a hacking or DDoS attack.

In addition, hacktivism that is best explained as a combination of "hacking" and "activism" is expected to become more frequent in 2012, especially with the presidential elections in South Korea, the US and Russia.

VOL. 24
ASEC REPORT Contributors

Contributors

| | |
|---|---|
| Principal Researcher | Min-seok Cha |
| Senior Researcher | So-heon Kim |
| Senior Researcher | Chang-yong Ahn |
| Senior Researcher | Young-jun Chang |
| Assistant Researcher | Do-hyun Lee |
| Assistant Researcher | Ju-bong Cho |
| Researcher | Jung-shin Lee |

Key Sources
ASEC Team
SiteGuard Team

Executive Editor
Senior Researcher Hyung-bong Ahn

Editor
Marketing Department

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