

Disclosure to or reproduction
for others without the specific
written authorization of AhnLab
is prohibited.

Copyright (c) AhnLab, Inc.
All rights reserved.

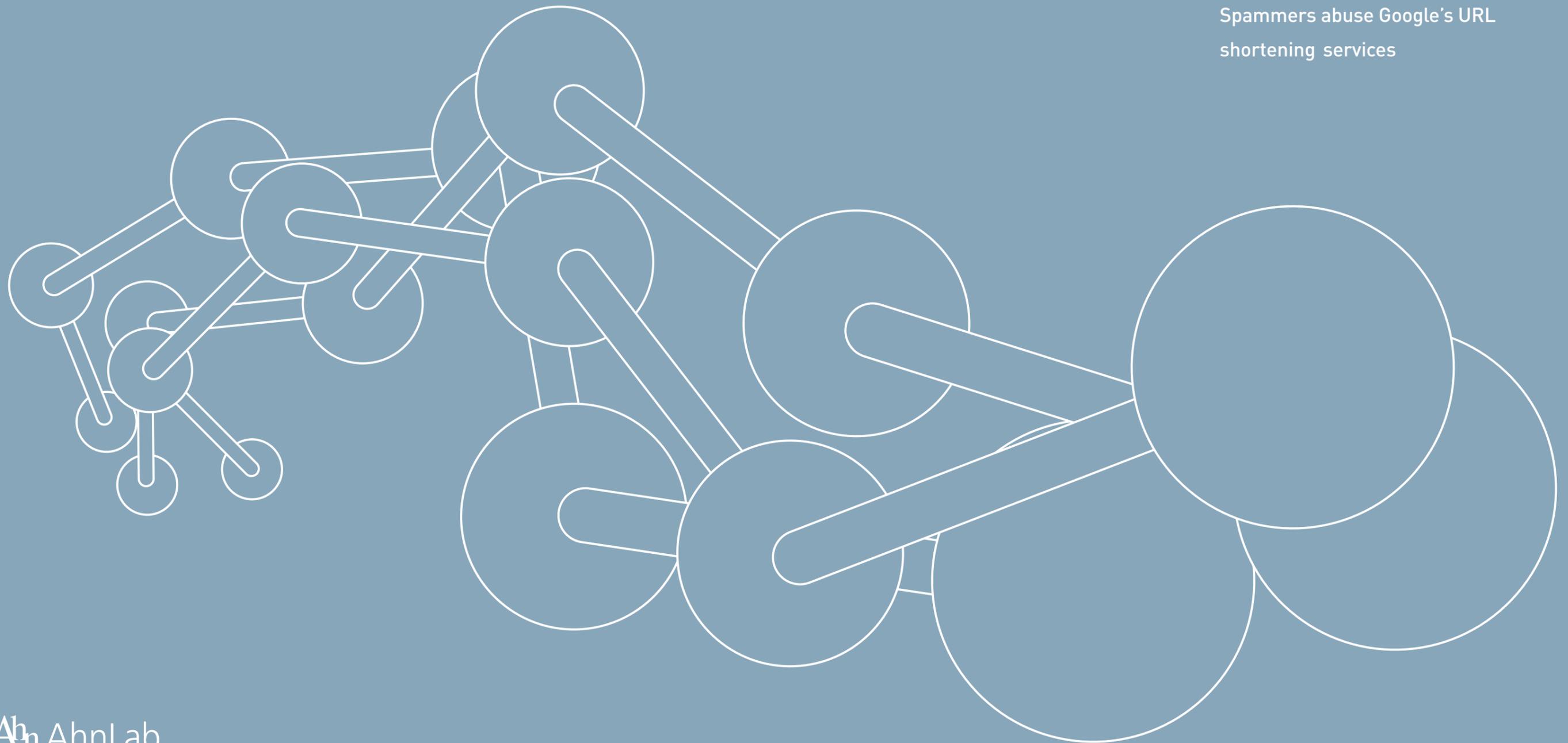
ASEC REPORT

VOL.20 | 2011.9

AhnLab Monthly Security Report

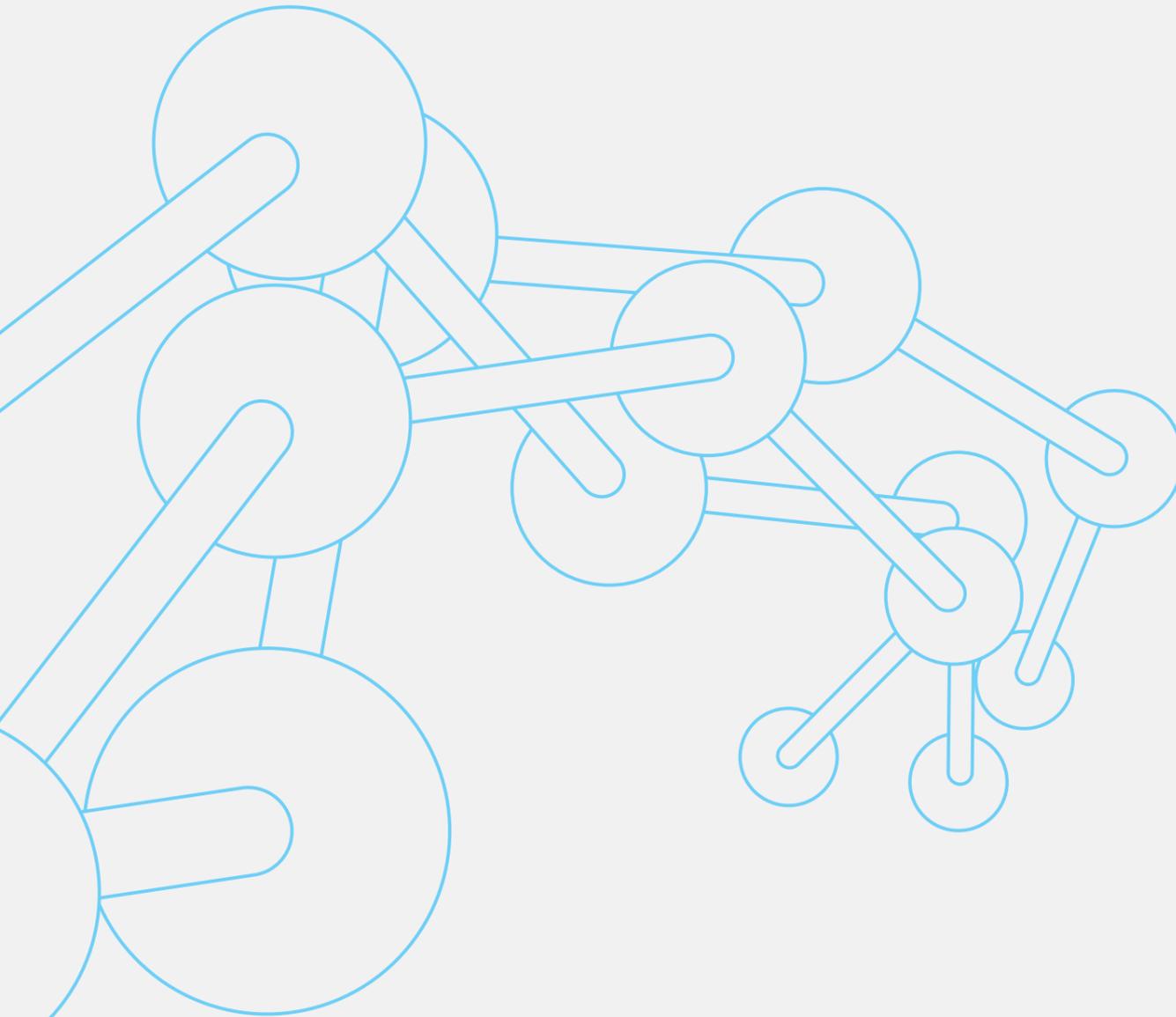
Risk of targeted attacks

Spammers abuse Google's URL
shortening services



AhnLab Security Emergency response Center

ASEC (AhnLab Security Emergency Response Center) is a global security response group consisting of virus analysts and security experts. This monthly report is published by ASEC, and it focuses on the most significant security threats and the latest security technologies to guard against these threats. For further information about this report, please refer to AhnLab, Inc.'s homepage (www.ahnlab.com).



CONTENTS

01. Malicious Code Trend

a. Malicious Code Statistics 05

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

b. Malicious Code Issues 10

- Risk of targeted attacks
- Operation Shady RAT- a massive APT type attack campaign
- File used to hack RSA found
- Amazon S3 exploited through SpyEye
- Ice IX built with Zeus source codes
- Spammers abuse Google's URL shortening services
- Credit card scam via Twitter
- Fake 'wrong transaction' hotel spam
- AV (19+) needs an AV (Anti-virus)
- Increasing smartphone security threats
- Android-Spyware/Nicky
- Beware of Android malware that steals personal information
- Android malware app Google++ disguised as Google+

02. Security Trend

a. Security Statistics 21

- Microsoft Security Updates- August 2011

03. Web Security Trend

a. Web Security Statistics 22

- 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 25

- August 2011 Malicious Code Intrusion: Website

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 August 2011. As of August 2011, Swf/Agent is the most reported malicious code, followed by JS/Agent and Textimage/Autorun, respectively. 7 new malicious codes emerged in the top 20 list this month.

Ranking	↑↓	Malicious Code	Reports	Percentage
1	NEW	Swf/Agent	712,068	15.2 %
2	▼1	JS/Agent	566,422	12.1 %
3	▼1	Textimage/Autorun	536,746	11.5 %
4	NEW	JS/Exploit	382,509	8.2 %
5	▼2	Html/Agent	377,665	8.1 %
6	▲5	JS/Iframe	352,920	7.5 %
7	▼1	Swf/Cve-2011-2110	314,156	6.7 %
8	NEW	Swf/Exploit	231,482	4.9 %
9	NEW	Win-Trojan/Startpage.118784.AO	168,327	3.6 %
10	▼5	Win32/Induc	119,831	2.6 %
11	NEW	Win-Trojan/Onlinegamehack69.Gen	113,211	2.4 %
12	▼5	Win-Trojan/Downloader.217088.AE	105,520	2.3 %
13	NEW	Win-Trojan/Overtls57.Gen	99,524	2.1 %
14	▼5	Win32/Palevo1.worm.Gen	95,424	2.0 %
15	NEW	Als/Bursted	89,103	1.9 %
16	▼12	Swf/Cve-2010-2884	88,173	1.9 %
17	▲2	Win-Trojan/Onlinegamehack57.Gen	87,640	1.9 %
18	▼8	Win32/Conficker.worm.Gen	85,927	1.8 %
19	▼11	Win32/Virut.d	81,639	1.7 %
20	▼5	Win-Trojan/Downloader13.Gen	71,437	1.6 %
			4,679,724	100 %

[Table 1-1] Top 20 Malicious Code Reports

Top 20 Malicious Code Variant Reports

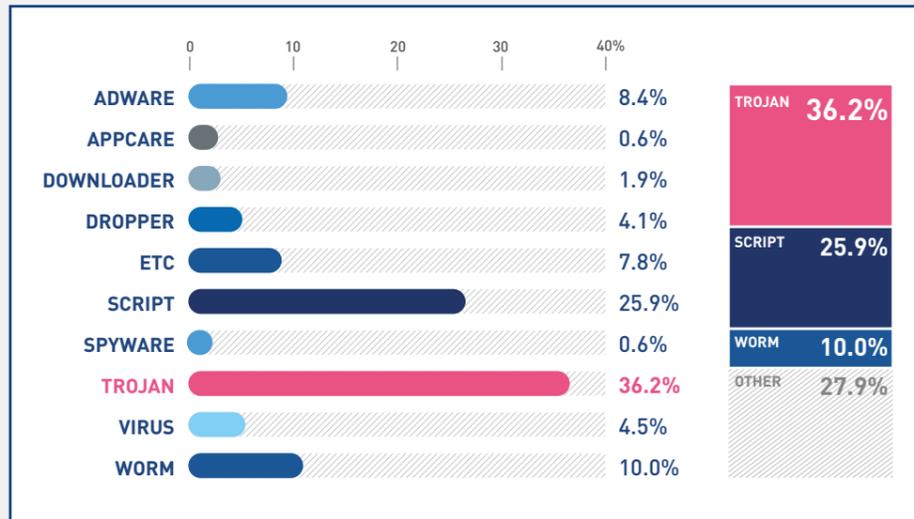
The table below shows the percentage breakdown of the top 20 malicious code variants reported this month, and identifies the malicious code trend of this month. As of August 2011, Win-Trojan/Downloader is the most reported malicious code, representing 10.4% (805,163 reports) of the top 20 reported malicious code variants, followed by Swf/Agent (712,068 reports) and Win-Trojan/Agent (698,272 reports).

Ranking	↑↓	Malicious Code	Reports	Percentage
1	▲1	Win-Trojan/Downloader	805,163	10.4 %
2	NEW	Swf/Agent	712,068	9.2 %
3	▲2	Win-Trojan/Agent	698,272	9.1 %
4	▼3	Win-Adware/Korad	605,372	7.9 %
5	▼2	JS/Agent	566,422	7.4 %
6	—	Textimage/Autorun	536,826	7.0 %
7	▼3	Win-Trojan/Onlinegamehack	425,786	5.5 %
8	NEW	JS/Exploit	382,509	5.0 %
9	▼1	Html/Agent	377,665	4.9 %
10	NEW	JS/Iframe	352,920	4.6 %
11	▼4	Win32/Virut	330,979	4.3 %
12	NEW	Swf/Cve-2011-2110	314,156	4.1 %
13	▼4	Win32/Conficker	276,149	3.6 %
14	NEW	Swf/Exploit	231,482	3.0 %
15	▼4	Win32/Autorun.worm	230,997	2.9 %
16	NEW	Win-Trojan/Startpage	198,144	2.6 %
17	▼5	Win-Trojan/Winsoft	176,097	2.3 %
18	▼3	Win32/Kido	175,725	2.3 %
19	▼6	Dropper/Malware	160,811	2.2 %
20	NEW	Win-Downloader/Korad	148,863	1.9 %
			7,706,406	100 %

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

Breakdown of Primary Malicious Code Types

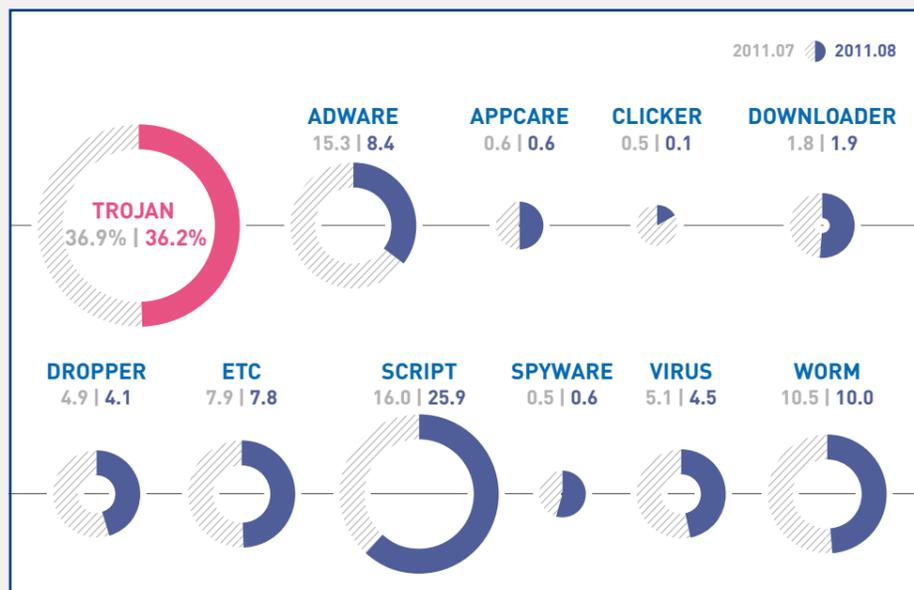
The chart below categorizes the top malicious codes reported this month. As of August 2011, Trojan is the most reported malicious code, representing 36.2% of the top reported malicious codes, followed by script (25.9%) and worm (10%).



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

Comparison of Malicious Codes with Previous Month

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



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

Monthly Malicious Code Reports

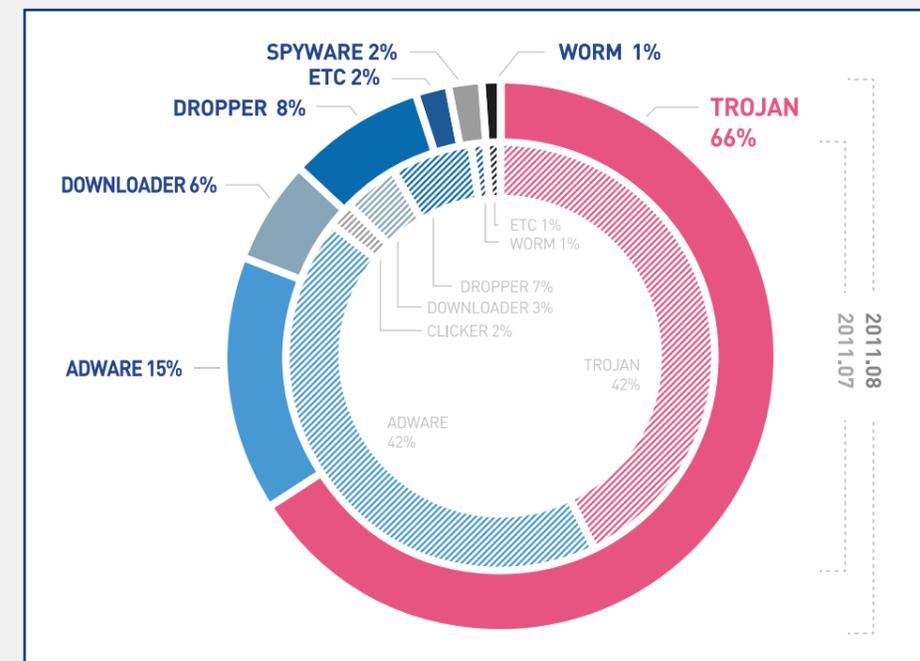
There has been a decrease in malicious code reports this month, which dropped 1,211,739 to 13,666,715 from 14,878,454 the previous month.



[Fig. 1-3] Monthly Malicious Code Reports

Breakdown of New Malicious Code Types

As of August 2011, Trojan is the most reported new malicious code, representing 66% of the top reported new malicious codes. It is followed by adware (15%) and dropper (8%).



[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 in August 2011. As of August 2011, Win-Trojan/Startpage.118784.AO is the most reported new malicious code, representing 27.3% (168,327 reports) of the top 20 reported new malicious codes, followed by Win-Trojan/Agent.28672.CFM (53,151 reports).

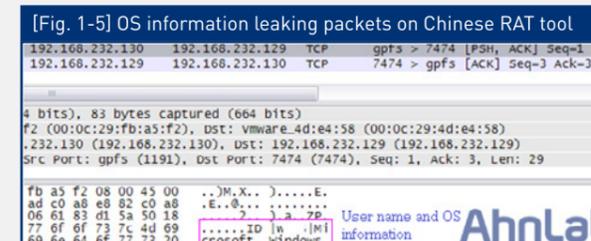
Ranking	Malicious Code	Reports	Percentage
1	Win-Trojan/Startpage.118784.AO	168,327	27.3 %
2	Win-Trojan/Agent.28672.CFM	53,151	8.6 %
3	Win-Trojan/Agent.257382	38,497	6.2 %
4	Win-Trojan/Fosniw.66560	35,404	5.7 %
5	Win-Trojan/Agent.978944.DT	30,600	5.0 %
6	Dropper/Agent.1995028	28,918	4.7 %
7	Win-Adware/AdCenter.254865	23,257	3.8 %
8	Win-Trojan/Downloader.461824.C	21,236	3.4 %
9	Win-Spyware/Agent.499712.C	20,299	3.3 %
10	Win-Trojan/Downloader.1235968.B	19,691	3.2 %
11	Win-Adware/KorAd.446464	19,149	3.1 %
12	Dropper/Malware.198144.BT	19,116	3.1 %
13	Win-Adware/KorAd.294912.B	18,053	2.9 %
14	Win-Trojan/Downloader.414208.G	17,771	2.9 %
15	Win-Adware/KorAd.239616	17,755	2.9 %
16	Win-Trojan/Downloader.1307648.D	17,317	2.8 %
17	Win-Trojan/Downloader.1650688.B	17,217	2.8 %
18	Win-Trojan/Downloader.422400.L	17,124	2.8 %
19	Win-Adware/KorAd.273920	17,027	2.8 %
20	Win-Trojan/Agent.1077248.AL	16,973	2.7 %
		616,882	100 %

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

01. Malicious Code Trend b. Malicious Code Issues

Risk of targeted attacks

Recently, several large web portals and websites have been hacked - a lot of personal data have been compromised in the attack. We have been hearing more and more about targeted attacks or APTs (Advanced Persistent Threat) as aforementioned. There are two general forms of targeted attacks: those that attack the corporate network and those that attack the server network. The first form is a common hacking method, and the latter form is more diverse: social engineering, malware attack, phishing, keylogging, exploitation of vulnerabilities, reverse shell command execution and database hacking. A more complex security system is needed to defend against these various threats. If a computer on a corporate network gets infected by malware, the hacker will have access to the targeted computer's OS information. The packet data could be encrypted to avoid detected on the network.

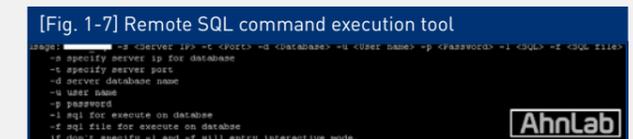


The reverse shell provides the attacker access to the target machine across the network to steal information on the OS and



executed processes, log keystrokes, support proxy and remotely control the system.

The attacker also uses a vulnerable machine on the network to access the DB server to steal private data. Since a trusted machine on the network is attempting access to the DB server, it will not be detected as an attack.



Companies can protect their confidential information from hackers by following the countermeasures below. Administrators that are allowed to access the DB server should use a separate network (physical or logical), and LINUX or UNIX operating system.

1. Control inside information and employees' information
2. Monitor all network traffic and potential security threats, and analyze the logs
3. Educate employees on security regularly (P2P, webhard, automatic SW updates)
4. Install security software installed on all endpoint PCs and update the latest virus signatures regularly
5. Keep whitelist of certified applications to prevent installation/execution of unwanted applications
6. Block unauthorized accounts from accessing important systems
7. Prevent employees from accessing critical system network
8. Patch the OS and applications installed to PCs regularly
9. Encrypt sensitive data

Operation Shady RAT- a massive APT type attack campaign

McAfee published a report about a five-year hacking campaign dubbed Operation Shady RAT. The same technique was used to break into security company RSA and many oil and gas companies this year.

Operation Shady RAT breached networks of 72 organizations across the globe since 2006.



Spear phishing emails were sent to the target containing a link to a malicious file or URL that automatically loaded a malicious RAT program on the computer, thus gaining access to the network and the high-value information. C&C servers are used to launch and manage the operation. ASEC found 25 malware to be involved in the attack. While we cannot ignore the old approaches and steps for data protection, we need a new step. Organizations need to do more than deploy signature-based antivirus on their endpoints. They need a comprehensive endpoint security product that includes additional layers of protection.

- V3 detects this Trojan as:
 - Win-Trojan/Sharat.114455
 - Win-Trojan/Sharat.28160
 - Win-Trojan/Sharat.107361
 - Win-Trojan/Sharat.114456

File used to hack RSA found

EMC's RSA Security acknowledged it had been hit by an "extremely sophisticated" attack and that information related to the SecurID two-factor authentication products have been stolen. RSA said two different phishing emails were sent to two small groups of low-level users who received emails that contained an attachment called "2011 Recruitment plan.xls". After 5 months, an analyst from F-Secure found the file and F-Secure posted in their blog the complete description on how the file was found under the title, "How we found the file that was used to Hack RSA".

RSA was hacked by an exploit known as the zero day exploit which was embedded in the Adobe Flash Player application. The vulnerability exploited is CVE-2011-0609. The breach of RSA's intellectual property is a classic case of social engineering. V3 detects this malware as:

- Dropper/Cve-2011-0609

Amazon S3 exploited through SpyEye

ASEC predicted the top 7 security threats of 2011 in January. The top 7 threats include social network service used as a platform for malware distribution and exploitation of zero-day vulnerabilities. The list also includes cloud and virtualization technology used in cyber attacks for significant benefits and cost-savings. A Kaspersky Lab blog post on July 28, "Amazon S3 exploiting through SpyEye", describes cybercriminals using Amazon S3 cloud storage to host SpyEye toolkit to steal banking information. Amazon S3 was included in domain names that distribute SpyEye which added legitimacy to the attacks. Those behind the campaign are using stolen identity and credit card data to open Amazon accounts needed to use the web storage service.

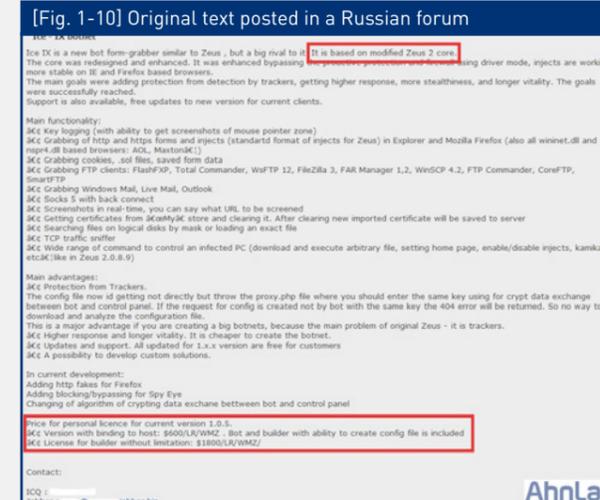


[Fig. 1-9] Amazon S3 hosting SpyEye toolkit

A cloud storage service platform gives IT managers significant cost savings, but the biggest concerns about cloud computing are security and privacy. Cybercriminals are increasingly turning to cloud storage services to distribute their malware, which they can use to host Web based attacks. Cloud service providers need to build and deliver managed security services for their customers.

Ice IX built with Zeus source codes

Ice IX has been built with the help of the ZeuS information stealer's source code, which got exposed this year (2011). According to Kaspersky Lab's blog post, "Ice IX, the first crimeware based on the leaked ZeuS sources" on August 24, 2011, Ice IX was built with the publicly exposed source code belonging to Zeus botnet. It was initially introduced to cybercriminals in the Russian-speaking underground.

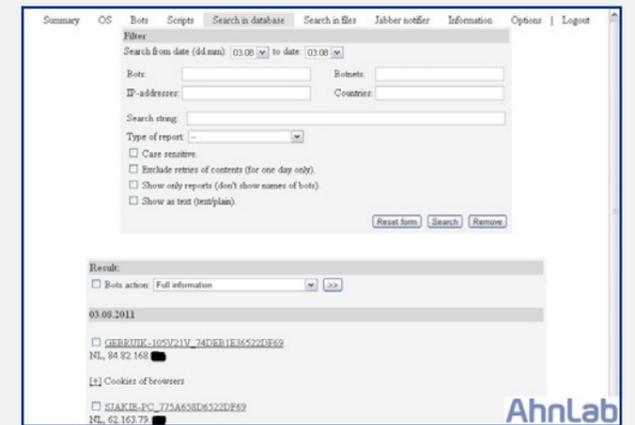


[Fig. 1-10] Original text posted in a Russian forum

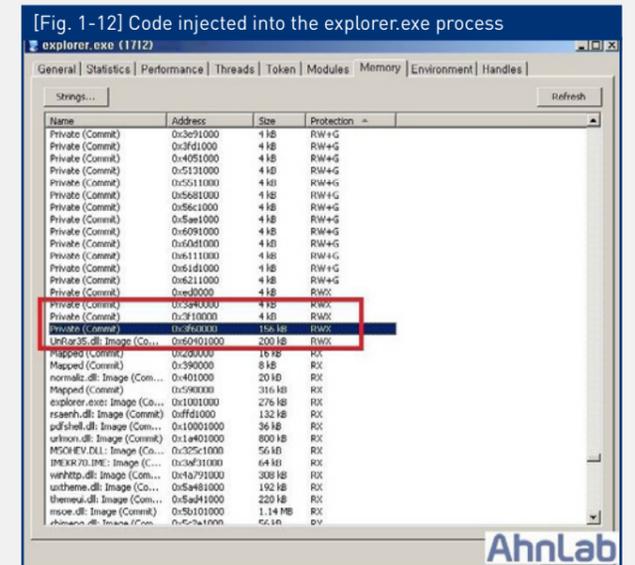
The Trojan with hardcoded C&C server sells for US\$600. You get the bot and the builder that generates the configuration file. Open Trojan with unlimited builder license sells for \$1,800. Ice IX's control panel are as below. It is similar to the Spyeye Bot web-based remote control panel.



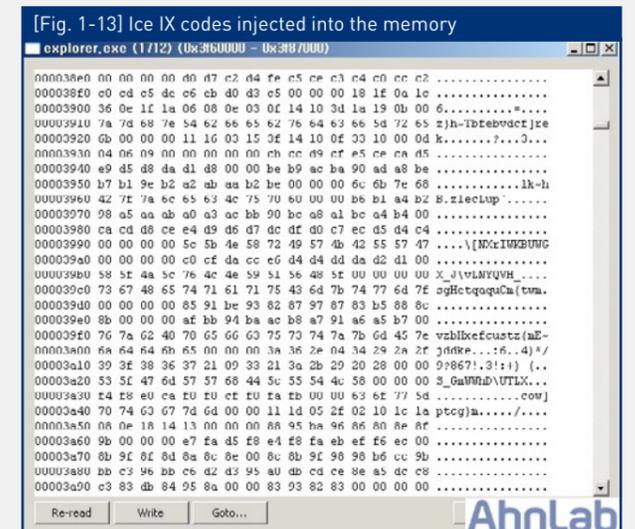
[Fig. 1-11] Ice IX control panel



The Ice IX botnet is similar to Zeus bot and its main purpose is to steal financial information.



[Fig. 1-12] Code injected into the explorer.exe process



[Fig. 1-13] Ice IX codes injected into the memory

The Ice IX bot injects its codes into the memory of explorer.exe process, and attempts to connect to the C&C server to remotely control the explorer.exe process.

It then sends information on the infected system and receives commands from the attacker.

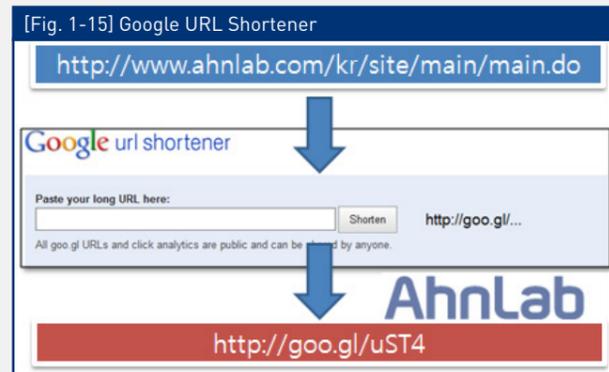


V3 detects this Trojan as:
- Win-Trojan/Zbot.99840.BC

Spammers abuse Google's URL shortening services

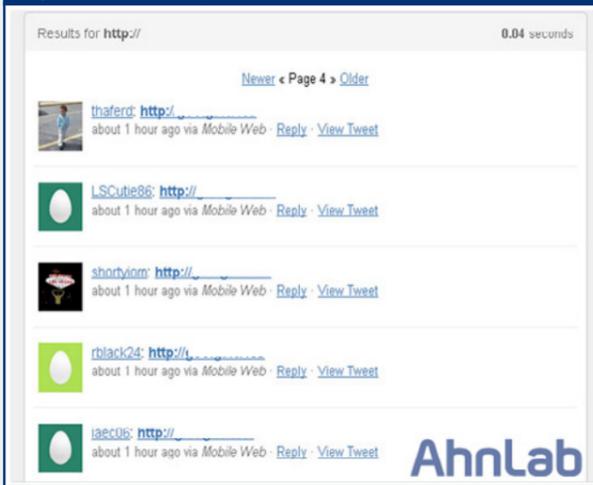
* What is URL shortening service?

URL shortening is used a lot by SNS users to make standard URLs fit into the character limit of the service.



Using a URL shortener can make it easier to include a URL within a short message. But, you must be careful with shortened links as they may point to malicious websites or advertisements. The problem is the shortening process removes some key data points that you need to decide whether to click the link. You won't know what domain it is from. You will not be sure whether it has been compromised. You might be directed to the spammers' website containing spam advertising or malware.

[Fig. 1-16] Malware spread via shortened URL

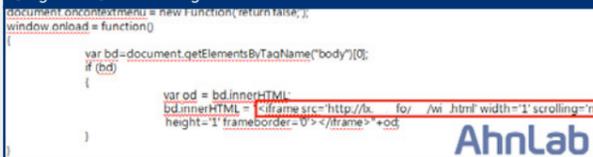


The image above shows a shortened URL posted on Twitter to spread malware. If you click the link, you will be directed to a site that downloads malicious scripts. The iframe tag checks the Internet Explorer version you are using to run the proper vulnerable scripts.

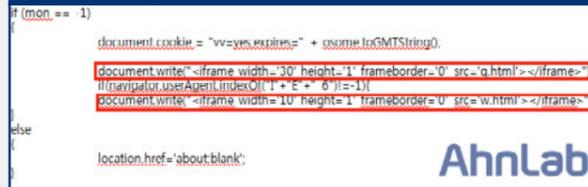
[Fig. 1-17] Malware distributed via Google shortened URL



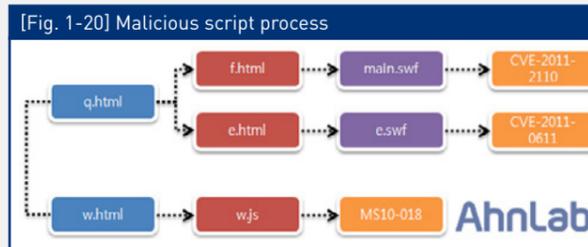
[Fig. 1-18] iframe tag inserted into the malicious shortened URL



[Fig. 1-19] Script that checks the IE version



Several vulnerabilities were exploited to infect as many PCs as possible as below:



imm32.dll will be replaced in infected systems. When the malicious imm32.dll file is executed, the clean backed up imm32.dll (shell64.dll) will get loaded.

[Fig. 1-21] Malicious imm32.dll's API call function

File pos	Mem pos	ID	Text
0000E2F2	100160F2	0	CtlImmActivate
0000E302	10016102	0	shell64.CtlImmActivate
0000E31A	1001611A	0	CtlImmDeactivate
0000E32C	1001612C	0	shell64.CtlImmDeactivate
0000E346	10016146	0	CtlImmSlIME
0000E353	10016153	0	shell64.CtlImmSlIME
0000E368	10016168	0	CtlImmCoUninitialize
0000E37D	1001617D	0	shell64.CtlImmCoUninitialize
0000E39A	1001619A	0	CtlImmDispatchDeflmeMessage
0000E3B6	100161B6	0	shell64.CtlImmDispatchDeflmeMessage
0000E3DA	100161DA	0	CtlImmEnterColnitCountSkipMode
0000E3F9	100161F9	0	shell64.CtlImmEnterColnitCountSkipMode
0000E420	10016220	0	CtlImmGenerateMessage
0000E436	10016236	0	shell64.CtlImmGenerateMessage
0000E454	10016254	0	CtlImmGetGuidAtom
0000E466	10016266	0	shell64.CtlImmGetGuidAtom

to the information below and install the latest security updates to prevent this attack.

- 1) Install the latest Adobe Flash Player version. (http://get.adobe.com/kr/flashplayer/)
- 2) Install the security updates for vulnerabilities in Internet Explorer.

Updating Microsoft Windows

1. Open Internet Explorer.
2. From the menu, click Tools and select Windows Update.
3. When prompted to install ActiveX component, select "Yes".
4. Click Install Updates to start updating.

Credit card scam via Twitter

A shortened URL to a malicious site that tricks victims into entering their credit card details was reported in the beginning of the month. The malicious link was spread via multiple Twitter accounts.

[Fig. 1-22] Malicious link on Twitter



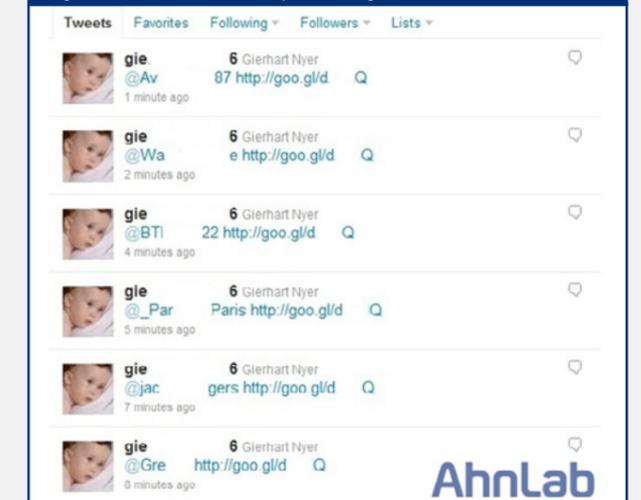
The tweet does not include a message. It just shows a shortened URL.

[Fig. 1-23] Tweet with shortened URL only



The account that sends the malicious link contains no other tweets than the tweet containing the shortened URL.

[Fig. 1-24] Account that keeps sending the malicious link



If you click on the malicious link, you will be directed to a site that tries to trick you into paying to download the program.

If you click Download Now, you will be asked to enter your credit card details.



You must be careful not to give out your credit card details online unless the site is a secure and reputable, as scammers may use your credit card to make purchases. Be careful not to click on shortened links or any links sent by people you don't really know from your social network site.

Fake 'wrong transaction' hotel spam

Spam mails have been making the rounds informing people that a hotel made a "wrong transaction" while processing their credit card and that they should fill out an attached form to process the refund. The claim that a credit card transaction problem has been found is a lie designed to trick recipients into opening the attached file. The attachment contains malware. There are slight variants of the spam as below:

[Table 1-4] Fake 'wrong transaction' hotel spam	
Subject	<ul style="list-style-type: none"> - Hotel [name] made wrong transaction - [Hotel name] made wrong transaction - Wrong transaction from your credit card in [resort name] Golf Resort - Wrong transaction from your credit card in [hotel name]

Message	<p>Dear Customer!</p> <p>Transaction: Visa [5-digit number]_r We are sorry to inform you that on July 26th, 2011 Hotel transaction debiting from your account for an overall amount of \$1232.</p> <p>For noncompliance of the service contract this Hotel was divested accreditation in Moverick Company. For the return of funds please contact your bank and fill information in the attached form. You'll need the attached detalization of your account transactions to apply for the return of funds. Company just mediates and bears no responsibility for any money transactions made by Hotel. Thank you for understanding. We trust you can solve this unpleasant problem.</p> <p>Victorine Mccrandle, Manager of Reception Desk & Reservation Department</p>
	<p>Dear Guest!</p> <p>Transaction: Visa [5-digit number]_oxi8q On July 26th, 2011 Hotel made wrong transaction debiting from your credit card for an overall amount of \$1122.</p> <p>For noncompliance of the service contract this Hotel was divested accreditation in Moverick Company. For the return of funds please contact your bank and fill information in the attached form. In the attachment you will find expense sheet with the sum of wrong transaction writing-down. Company just mediates and bears no responsibility for any money transactions made by Hotel. Thank you for understanding. We trust you can solve this unpleasant problem.</p> <p>Silver Rousch, Manager of Reception Desk & Reservation Department</p>
Attachment	- RefundForm[4-digit number].zip

Recipients who are intrigued to find that they may be owed some money might open the malicious attachment. The malicious file is masked as an executable download called RefundForm.exe, but it's actually a Trojan.



If the file is opened, it executes svchost.exe on the Windows system and overwrites the memory. It then uses the svchost.exe process to download soft.exe (385,024 bytes) from a system in Russia.



The subsequently downloaded malware is a rogue anti-virus. Once installed, rogue anti-virus programs can pop-up false "results" designed solely to trick users into submitting their credit card details.

V3 detects this Trojan as:

- Win-Trojan/Yakes.55296.C
- Win-Trojan/Yakes.56320
- Win-Trojan/Yakes.52736
- Win-Trojan/Yakes.51200
- Win-Trojan/Yakes.865792
- Win-Trojan/Hmblocker.385024

AV (19+) needs an AV (Anti-virus)

Be careful when downloading files from file sharing websites, torrents and P2P programs.

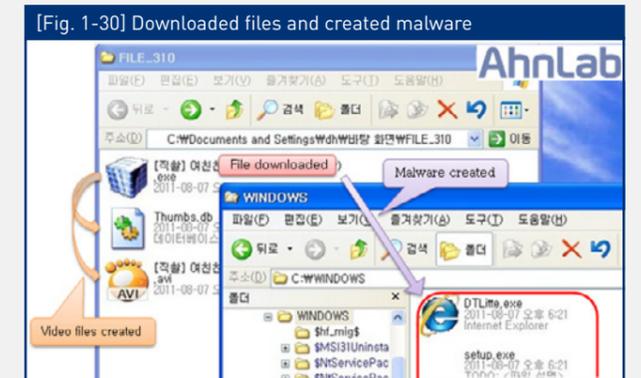
One of the main reasons people use file sharing websites is because it is easy to use and find files. But, there have been reports on systems getting infected after using some file sharing websites. Will it be safe to use these sites when you have installed the latest security patches for your system and application programs?

If your system is updated with the latest security patches, your system will not get infected just by visiting these sites. But,

Report Date	Process	Module	Behavior	Data
2011-08-01 16:22:47	[한노]잡은부끄...결합...서브계생...	[한노]잡은부끄...결합...서브계생...	create PE	setup.exe
2011-08-01 11:29:35	[한노]잡은부끄...결합...서브계생...	[한노]잡은부끄...결합...서브계생...	create PE	setup.exe
2011-08-01 00:49:41	[신철] 여자...구...어라고...	[신철] 여자...구...어라고...	create PE	setup.exe
2011-08-01 00:08:04	[국노] 클라...스...어...	[국노] 클라...스...어...	create PE	setup.exe
2011-07-31 04:23:49	일 해구선수...서...서...서...	일 해구선수...서...서...서...	create PE	setup.exe
2011-07-31 02:01:04	일 해구선수...서...서...서...	일 해구선수...서...서...서...	create PE	setup.exe

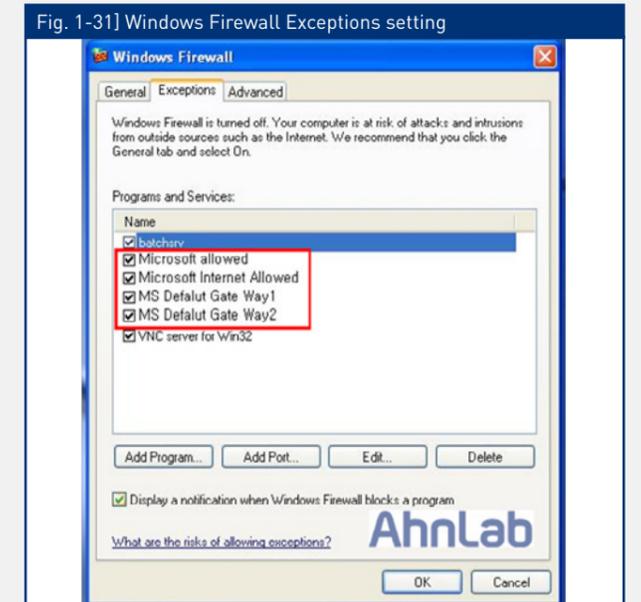
downloading files from these sites could infect your system. These sites may be used by cyber criminals not only to share, but also to distribute malware.

The video files downloaded from these sites are actually malicious.



- The video files are compressed into exe file.
- If you decompress the exe file, a video file will appear, making the victim believe it is a safe video file.
- The victim will not be aware of the malware that is created and executed on the background.
- setup.exe, DTLite.exe and _info.inf file will be created on the C:\WINDOWS folder.

The malware may bypass the firewall and use it as a backdoor.



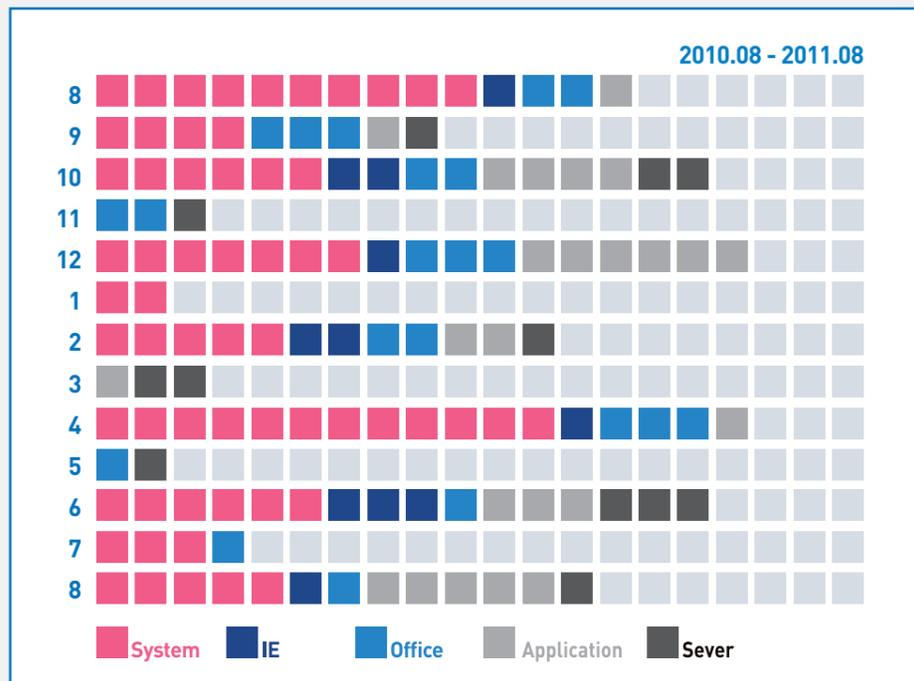
V3 detects this malware as:

- Dropper/Agent.1995028
- Win-Trojan/Agent.1724928

02. Security Trend
a. Security Statistics

Microsoft Security Updates- August 2011

Microsoft issued 13 security updates (2 critical, 9 important and 2 moderate) this month.



[Fig. 2-1] MS Security Updates

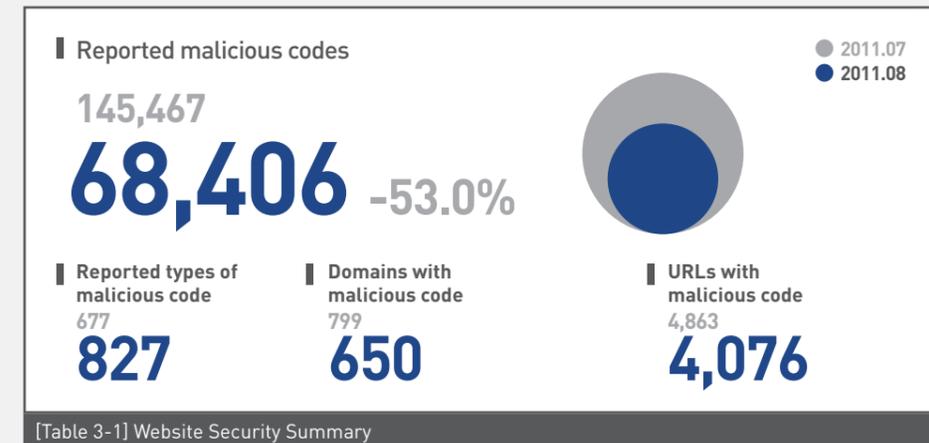
Severity	Vulnerability
Critical	Cumulative security update for Internet Explorer [2559049]
Critical	Vulnerabilities in DNS server could allow remote code execution [2562485]
Important	Vulnerability in Data Access Components could allow remote code execution [2560656]
Important	Vulnerabilities in Microsoft Visio could allow remote code execution [2560978]
Important	Vulnerability in Remote Desktop Web Access could allow elevation of privilege [2546250]
Important	Vulnerability in Remote Access Service NDISTAPI driver could allow elevation of privilege [2566454]
Important	Vulnerability in Windows Client/Server Run-time Subsystem driver could allow elevation of privilege [2567680]
Important	Vulnerabilities in TCP/IP stack could allow denial of service [2563894]
Important	Vulnerability in Remote Desktop Protocol could allow denial of service [2570222]
Important	Vulnerability in Microsoft Chart Control could allow information disclosure [2567943]
Important	Vulnerability in Microsoft Report Viewer could allow information disclosure [2578230]

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

03. Web Security Trend
a. Web Security Statistics

Web Security Summary

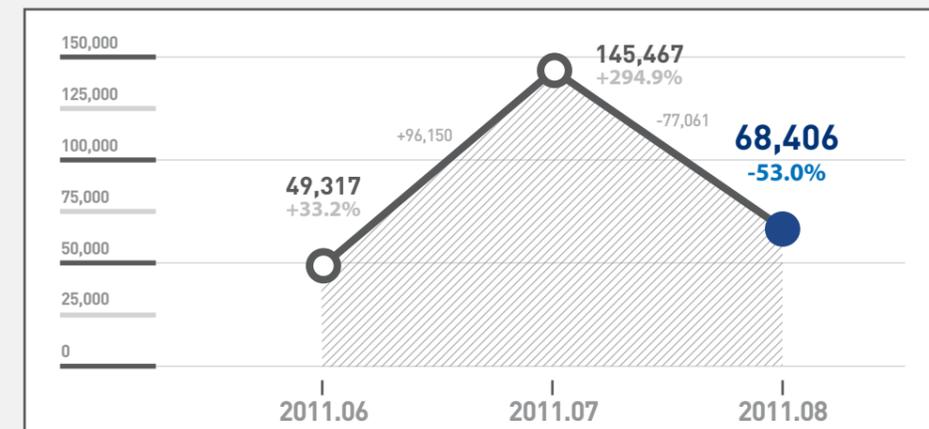
This month, SiteGuard (AhnLab's web browser security service) blocked 68,406 websites that distributed malicious codes. There were 827 types of reported malicious code, 650 reported domains with malicious code, and 4,076 reported URLs with malicious code. The number of reported malicious codes, domains with malicious code and URLs with malicious code decreased from the previous month, but the number of reported types of malicious code increased.



[Table 3-1] Website Security Summary

Monthly Blocked Malicious URLs

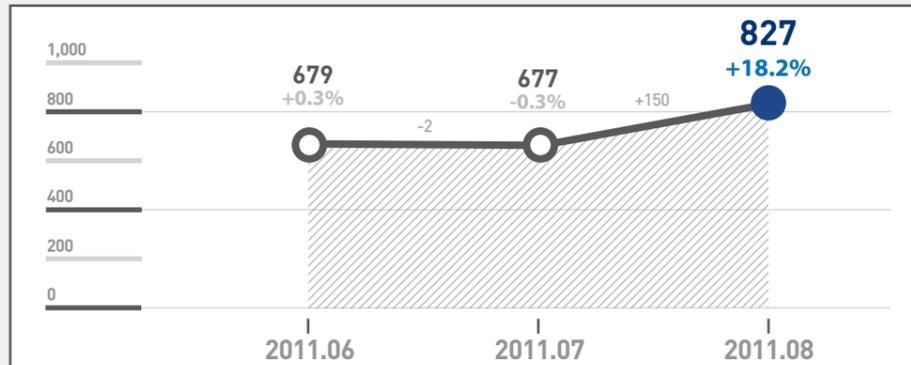
As of August, the number of blocked malicious URLs decreased 53% from 145,467 the previous month to 68,406.



[Fig. 3-1] Monthly Blocked Malicious URLs

Monthly Reported Types of Malicious Code

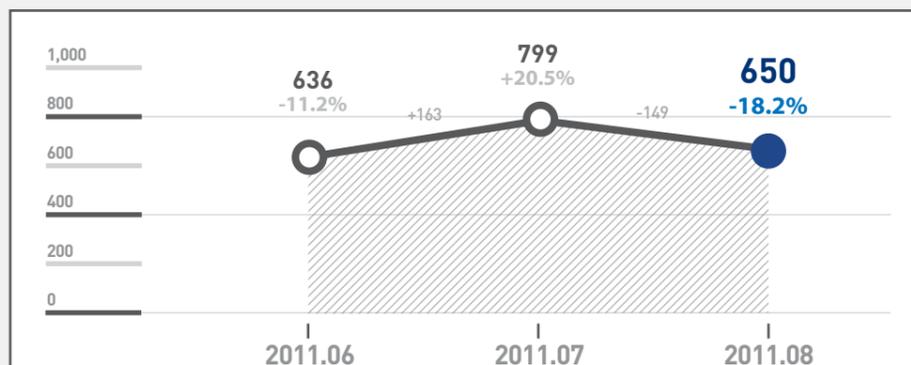
As of August 2011, the number of reported types of malicious code increased 22% from 677 the previous month to 827.



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

Monthly Domains with Malicious Code

As of August 2011, the number of reported domains with malicious code decreased 19% from 799 the previous month to 650.



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

Monthly URLs with Malicious Code

As of August 2011, the number of reported URLs with malicious code decreased 16% from 4,863 the previous month to 4,076.



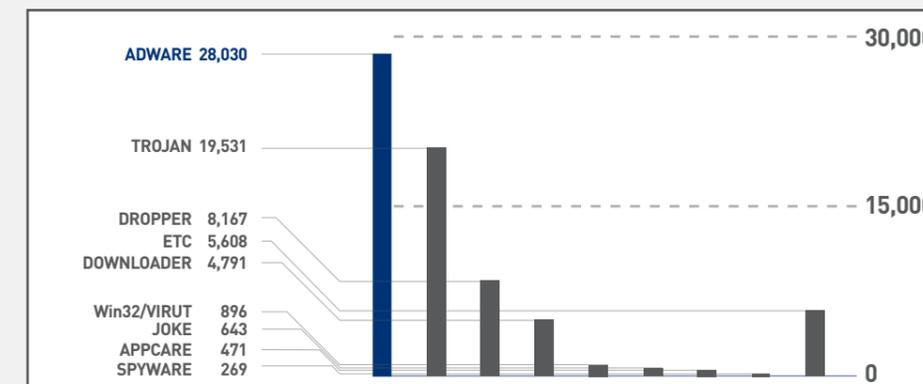
[Fig. 3-4] Monthly URLs with Malicious Code

Top Distributed Types of Malicious Code

As of August, the number of blocked malicious URLs decreased 53% from 145,467 the previous month to 68,406.

TYPE	Reports	Percentage
ADWARE	28,030	41.0 %
TROJAN	19,531	28.6 %
DROPPER	8,167	11.9 %
DOWNLOADER	4,791	7.0 %
Win32/VIRUT	896	1.3 %
JOKE	643	0.9 %
APPCARE	471	0.7 %
SPYWARE	269	0.4 %
ETC	5,608	8.2 %
	68,406	100 %

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



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

Top 10 Distributed Malicious Codes

As of August 2011, Win-Adware/ADPrime.837241 is the most distributed malicious code with 18,447 cases reported. 6 new malicious codes, including Dropper/SennaOneMaker.6556, emerged in the top 10 list this month.

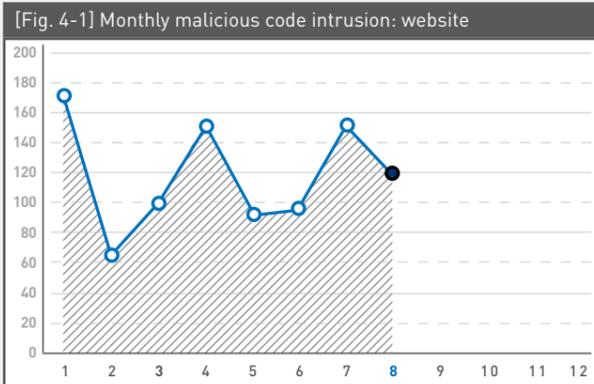
Ranking	↑↓	Malicious Code	Reports	Percentage
1	—	Win-Adware/ADPrime.837241	18,447	49.2 %
2	—	Win-Trojan/Downloader.765408	5,532	14.8 %
3	NEW	Dropper/SennaOneMaker.6556	2,812	7.5 %
4	NEW	Dropper/Kgen.225280.M	1,835	4.9 %
5	NEW	Win-Trojan/Genome.57344.QK	1,740	4.6 %
6	NEW	Win32/Induc	1,526	4.1 %
7	▼4	Win-Downloader/KorAd.83968	1,478	3.9 %
8	▼2	Win-Adware/Adprime.1766400	1,438	3.8 %
9	NEW	Downloader/Win32.Totoran	1,393	3.7 %
10	NEW	Dropper/Small.Gen	1,264	3.5%
			37,465	100 %

[Table 3-3] Top 10 Distributed Malicious Codes

03. Web Security Trend
b. Web Security Issues

August 2011 Malicious Code Intrusion: Website

The number of monthly malicious code intrusion decreased from last month. It is because the number of attacks via banner ads decreased this month.



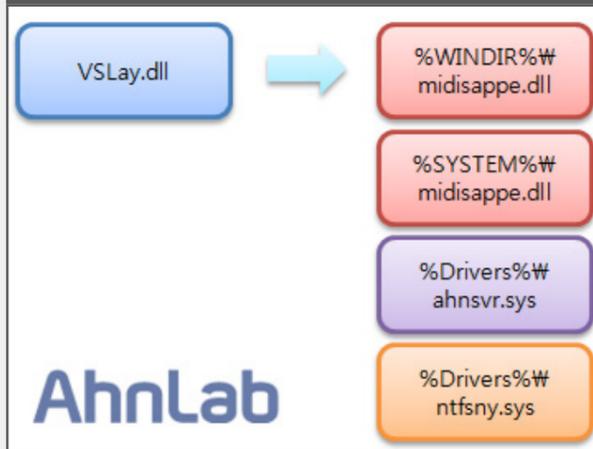
[Table 4-1] Top 10 Distributed Malicious Codes

Ranking	Threat	URL
1	Win-Trojan/Patched.CO	60
2	Win-Trojan/Onlinegamehack55.Gen	53
3	Win-Trojan/Onlinegamehack56.Gen	53
4	Win-Trojan/Onlinegamehack.100517	17
5	Dropper/Onlinegamehack.48294	17
6	Win-Trojan/Patched.DE	17
7	Win-Trojan/Onlinegamehack.89797	16
8	Win-Trojan/Onlinegamehack.33605796.B	16
9	Win-Trojan/Onlinegamehack.25760	15
10	Dropper/Onlinegamehack.67166890	15

The table above shows the top 10 distributed malicious codes. Trojan/Patched.CO is the most distributed malicious code, followed by Win-Trojan/Onlinegamehack55.Gen and Win-Trojan/Onlinegamehack56.Gen, respectively.

Some of the malicious codes distributed via hacked websites are DLL that steals online game account information, and rootkit driver that protects the DLL.

[Fig. 4-2] midisappe.dll constantly gets replaced by its variants, but the two SYS files do not change



VOL. 20
ASEC REPORT Contributors

Contributors
Senior Researcher Jung-hyung Lee
Senior Researcher Chang-yong Ahn
Senior Researcher Young-jun Chang
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.
6th Fl, CCMM Bldg,
12 Yeouido-dong,
Yeongdeungpo-gu,
Seoul 150-869,
South Korea
T. +82-2-2186-6000
F. +82-2-2186-6100

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

Copyright (c) AhnLab, Inc.
All rights reserved.

