ASEC REPORT

VOL.50 | 2014.02

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).

I. SECURITY TREND – FEBRUARY 2014

MALWARE TREND

01. Malware Statistics

About 3,200,000 malware were reported

Statistics collected by the ASEC show that 3,197,274 malware were reported in February 2014. The number of reports decreased by 150,457 from the 3,347,731 reported in the previous month. (See [Figure 1-1].) The malicious code name of the most frequently reported malware was Win- AppCare/Exploit.134544, followed by Trojan/Win32, OnlineGameHack and Win-Trojan/Patched.kg. (See [Table 1-1].) A total of 6 malware including Win-AppCare/Exploit.134544 were newly added to the Top 20. (See [Table 1-1].)

Figure 1-1 | Monthly Malware Reports

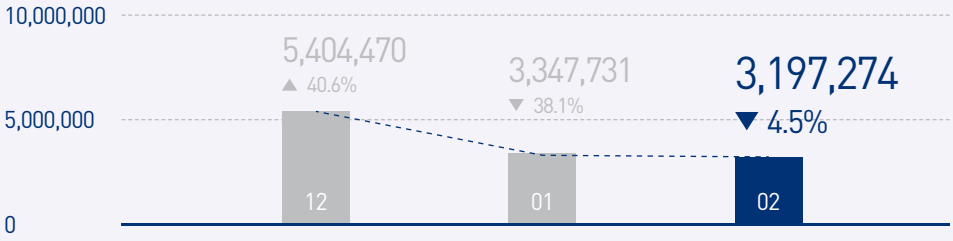


Table 1-1 | Top 20 Malware Reports in February 2014 (By Malicious Code Name)

Ranking	↑↓	Malicious Code	Reports	Percentage
1	NEW	Win-AppCare/Exploit.134544	186,210	13.4%
2	—	Trojan/Win32.OnlineGameHack	162,113	11.6%
3	▲1	Win-Trojan/Patched.kg	148,940	10.6%
4	▼1	Trojan/Win32.Agent	132,422	9.5%
5	▼14	PUP/Win32.SerchKey	79,990	5.7%
6	▲2	Trojan/Win32.Starter	76,937	5.5%
7	▼1	Adware/Win32.KorAd	65,363	4.7%
8	▲10	Trojan/Win32.Downloader	55,851	4.0 %
9	▼2	Trojan/Win32.Urelas	55,151	3.9 %
10	NEW	Worm/Win32.Mabezat	49,910	3.6 %
11	▲3	Textimage/Autorun	45,433	3.2 %
12	▲1	PUP/Win32.Helper	44,580	3.2 %
13	NEW	Als/Bursted	43,840	3.1 %
14	▲6	Unwanted/Win32.Keygen	40,920	2.9 %
15	▼4	Idx/Exploit.Gen	40,327	2.9 %
16	NEW	Trojan/Win32.Depok	39,369	2.8 %
17	▼1	Trojan/Win32.Gen	38,124	2.7 %
18	▼9	Trojan/Win32.Generic	37,062	2.6 %
19	NEW	Trojan/Win32.TopTool	28,832	2.1 %
20	NEW	Unwanted/Win32.Windowsnas	28,657	2.0 %
		TOTAL	1,400,031	100.0 %

Trojans account for 56% in February

[Table 1-2] below shows the percentage breakdown of the Top 20 new malware reported in February 2014. Among those, PUP/Win32.MicroLab was the most frequently reported malicious code (21,420 reports). It is followed by Trojan/Win32.OnlineGameHack (20,327 reports).

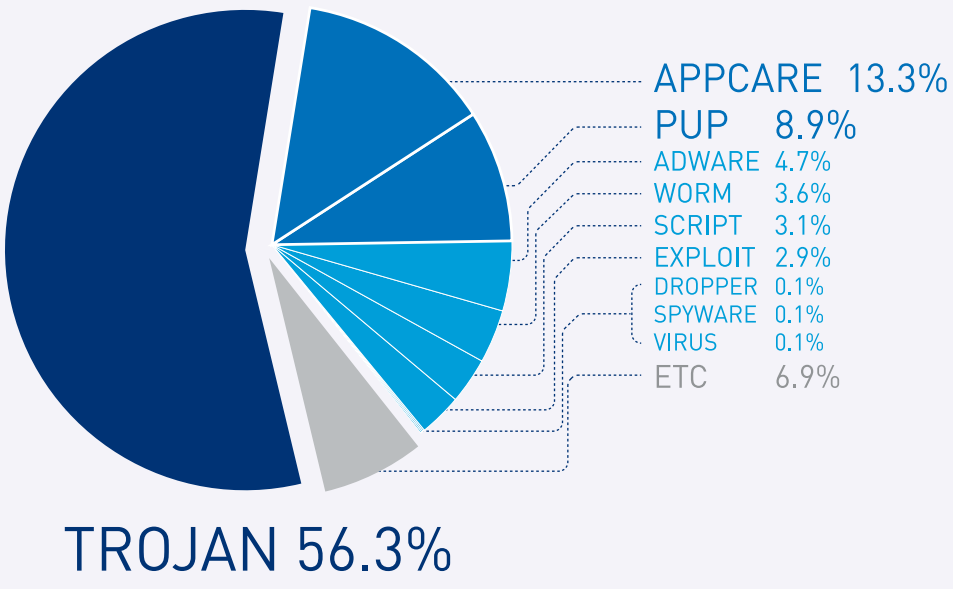
Table 1-2 | Top 20 New Malware Reports (By Malicious Code Name)

Ranking	Malicious Code	Reports	Percentage
1	PUP/Win32.MicroLab	21,420	10.3%
2	Trojan/Win32.OnlineGameHack	20,327	9.8%
3	Trojan/Win32.Agent	20,175	9.6%
4	PUP/Win32.SerchKey	18,881	9.1%
5	Trojan/Win32.Injector	18,319	8.7%
6	Trojan/Win32.Urelas	13,309	6.3%
7	PUP/Win32.ProcessClean	10,149	4.8%
8	Trojan/Win32.Depok	9,621	4.6%
9	Trojan/Win32.Zbot	9,033	4.3%
10	Trojan/Win32.Generic	8,894	4.2%
11	Backdoor/Win32.Plite	7,920	3.8%
12	Malware/Win32.Suspicious	7,339	3.5%
13	Adware/Win32.WindowsSearch	6,644	3.2%
14	PUP/Win32.LiveIcon	6,641	3.2%
15	Trojan/Win32.Dybalom	5,760	2.7 %
16	Trojan/Win32.Wgames	5,339	2.5 %
17	Trojan/Win32.Preloader	5,196	2.5 %
18	Worm/Win32.Mabezat	5,116	2.4 %
19	Packed/Win32.Morphinel	4,853	2.3 %
20	Unwanted/Win32.BitCoinMiner	4,681	2.2 %
	TOTAL	209,617	100.0 %

The number of AppCare and Scripts increased

[Figure 1-2] categorizes the top malware reported by AhnLab customers in February 2014. Trojan was the most reported malware type, representing 56.3% of the top reported malware types, followed by AppCare (13.3%) and PUP (8.9%).

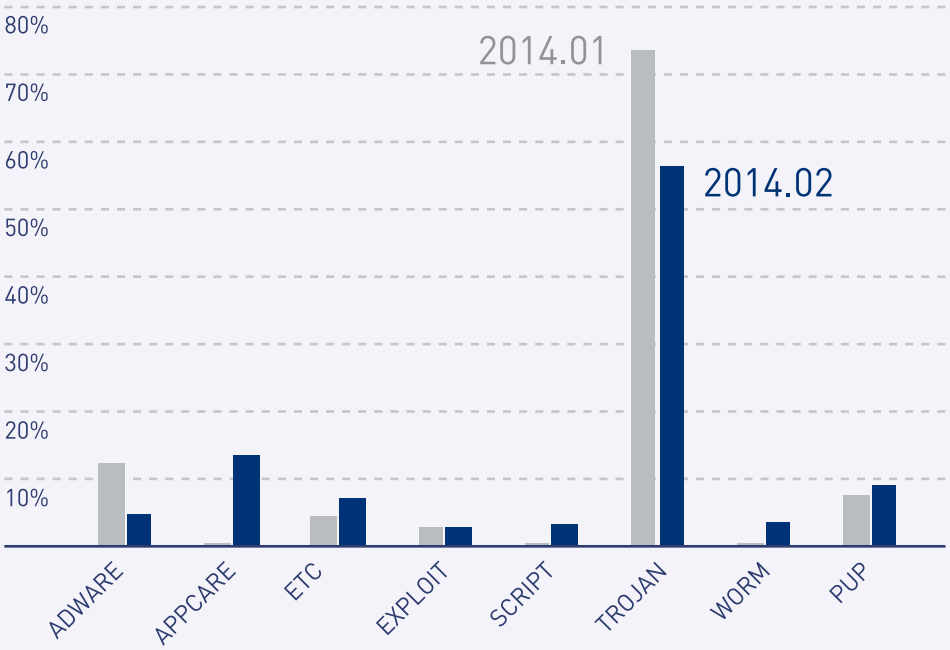
Figure 1-2 | Primary Malware Type Breakdown



Comparison of malware with previous month

[Figure 1-3] shows the malware breakdown compared to the previous month. The number of Appcare, Exploits, Scripts, Worms, and PUP increased, whereas the number of Adware and Trojan decreased.

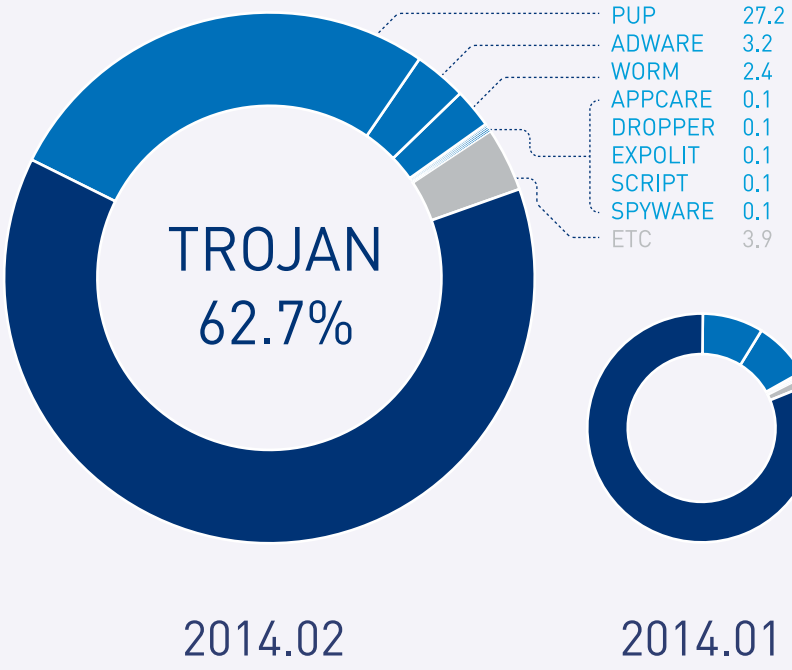
Figure 1-3 | Monthly Breakdown of Primary Malware Type (Jan vs. Feb 2014)



Breakdown of new malware types of February

Trojans was the most frequently reported type in February 2014, representing 62.7% of the new malware types, followed by PUP (27.2%), Adware (3.2%), and Worms (2.4%).

Figure 1-4 | Breakdown of New Malware Types



MALWARE TREND

02. Malware Issues

PlugX Variant, Presumed To Be Used for Targeted Attacks

There are multiple variant malware of PlugX have been generated and used to attack on various targets in Asian countries since 2012 when it has been discovered. Although PlugX has been distributed and modified for many years, there have been not so many changes made with it. The general infection process of PlugX malware is shown in [Figure 1-5].

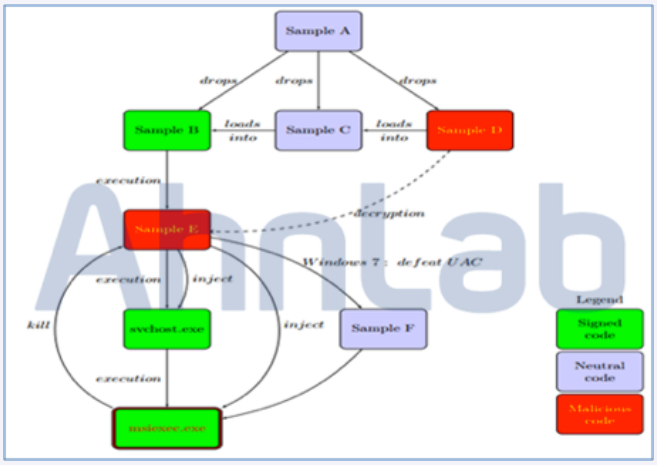


Figure 1-5 | Website used to distribute malware

As shown in [Figure 1-6], the PlugX variant recently discovered in South Korea has been presumed to spread through websites and e-mails. To deceive the user's suspicion, this variant downloads and runs a normal document file and malicious script at the same time. The relevant malicious script is to cause malware infection.

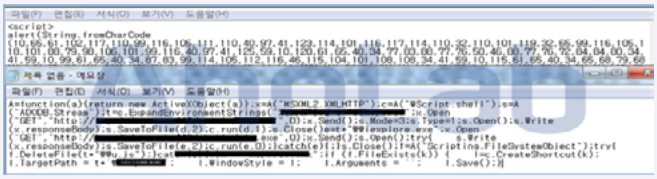


Figure 1-6 | Inserted script to infect malware

Most functions of the malware have not been changed much compared to the existing variants. Besides, previous variants used McAfee antivirus programs as the normal executable file to load the DLL file, whereas this newly discovered variant used the Kaspersky Lab's KAV instead. And, attackers could have used these files with PlugX variants without any alteration.

These files are normal executable files (EXE files) of the legitimate antivirus programs provided by security vendors. These EXE files automatically execute DLL file if there exists a DLL file that has a certain name in the same folder. Taking advantage of this process, attackers execute a malicious DLL file creating it with the same name as the normal DLL file that is supposed to be executed by the EXE files.

When a system is infected by the malware, the DLL file, which is recombined in memory, is injected into certain process as shown in [Figure 1-7]. Also, it is shown that the malware is executed through the winlogon.exe file. The malware continuously attempts to connect to a certain website to download additional malware, such as RAT. However, the relevant website was not available when ASEC analyzed the malware.

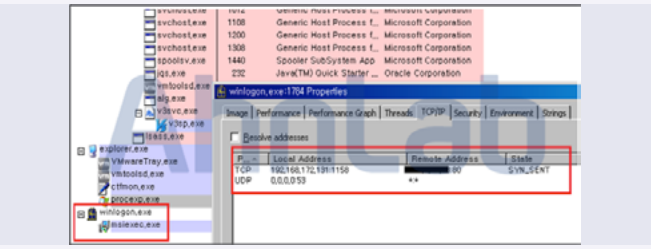


Figure 1-7 | winlogon.exe process status

Unlike the existing variants, this newly discovered variant encrypts the keylog data file that is generated after malware infection.

At the end of last year, Sohpos, a security vendor, reported that one of the PlugX variants was used in targeted attacks in Japan.

According to this report, the type of the compressed file was the same as the variant discovered in South Korea although the size was different, thus it was assumed that the similar attack might have happened in South Korea at that time.

http://nakedsecurity.sophos.com/2013/12/04/new-PlugX-malware-variant-takes-aim-at-japan/

In these cases, it is very difficult to recognize the PlugX and attacks for both security solutions and security managers due to the features and limited targets of the variants.

It may possibly surmise PlugX from the following peculiar file structure;

1. Malware is distributed via various methods such as e-mails.
2. An exe file of normal program is loaded as service and executed by the main dropper that is compressed as Rarsfx, and then the malicious DLL file is loaded.
3. The loaded DLL file is recombined by using a data file included in the RAR file during execution process, and the recombined DLL file is injected in a certain process.
4. The malicious file used during infection process is saved in a certain folder, and a normal EXE file is registered in the system service folder to run and re-infect the system at system booting.
5. Additional malware such as RAT is downloaded from C&C server and installed in the system.

V3 detects the relevant malware as shown below.

<Malicious code names in V3 products>
-Backdoor/Win32.PlugX (AhnLab, 2014.02.26.03)
-Trojan/Win32.PlugX (AhnLab, 2014.02.24.03)
-Binimage/PlugX (AhnLab, 2014.02.27.03)

BitCrypt; a Ransomware Demands Payment by Bitcoin

Ransomware is a type of malware that encrypts important files in PCs to block the access to those files and demands payment to restore the encrypted files. CryptoLocker, which has become known by ASEC and media report, is one of the ransomware. Recently, there have been reported of infection by another ransomware:BitCrypt. BitCrypt demands payments by Bitcoins to restore the encrypted files. It has not been yet discovered of the precise infection process of BitCrypt, and it is highly assumed that BitCrypt might have been distributed via attachment of spam e-mails or compromised websites. When a system is infected by BitCrypt,

*.dbf, *.mdb, *.mde, *.xls, *.xlw, *.docx, *.doc, *.cer, *.key, *.rtf, *.xlsm, *.xlsx, *.txt, *.xlc, *.docm, *.xlk, *.text, *.ppt, *.djvu, *.pdf, *.lzo, *.djv, *.cdx, *.cdt, *.cdr, *.bpg, *.xfm, *.dfm, *.pas, *.dpk, *.dpr, *.frm, *.vbp, *.php, *.wri, *.css, *.asm, *.jpg, *.jpeg, *.dbx, *.dbt, *.odc, *.sql, *.abw, *.pab, *.vsd, *.xsf, *.xsn, *.pps, *.lzh, *.pgp, *.arj, *.pst

Figure 1-8 | File extensions encrypted by BitCrypt

the files of various format types in [Figure 1-8] are encrypted, and the existing normal files are deleted. (See [Figure 1-9].)

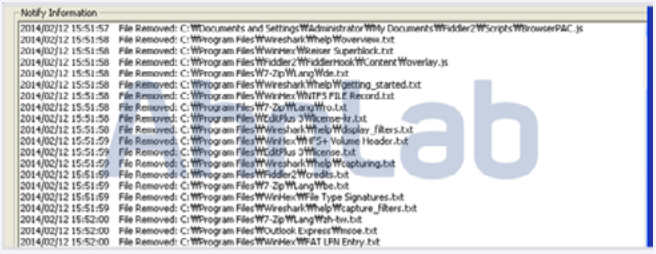


Figure 1-9 | Normal files deleted by BitCrypt

As shown in [Figure 1-10], the files encrypted by BitCrypt have extensions as [FileName.BitCrypt].

Figure 1-10 | Encrypted files by BitCrypt

When encrypting the files with extensions listed in [Figure 1-8] is completed, a BitCrypt.txt file is generated and displayed on the screen. (See [Figure 1-11].)

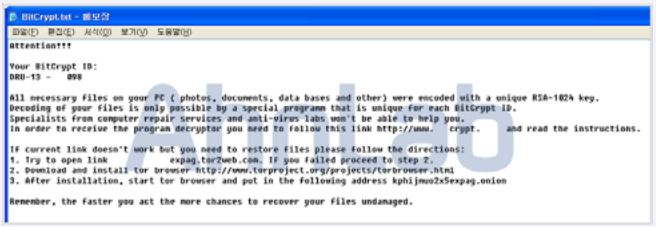


Figure 1-11 | BitCrypt.txt

In order to restore the encrypted files, BitCrypt provides information such as BitCrypt ID and a website address for recovery tool as shown in [Figure 1-12].

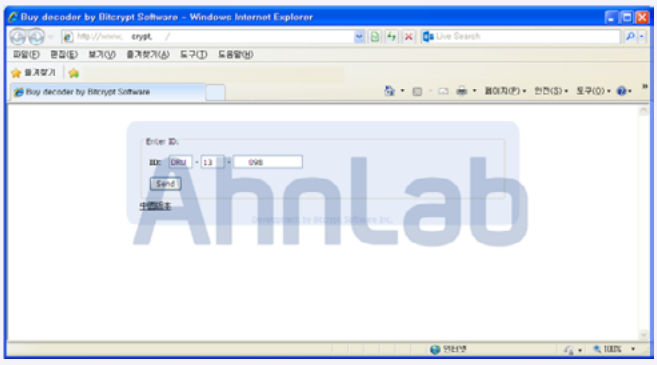


Figure 1-12 | Recovery tool website

If a user accesses the website in [Figure 1-12], it is asked of BitCrypt ID in the BitCrypt.txt file that is generated on the PC by BitCrypt. When the user inputs and sends the information, the download page for a recovery tool is displayed. It is required to fill the information fields to download the recovery tool. (See [Figure 1-13].)

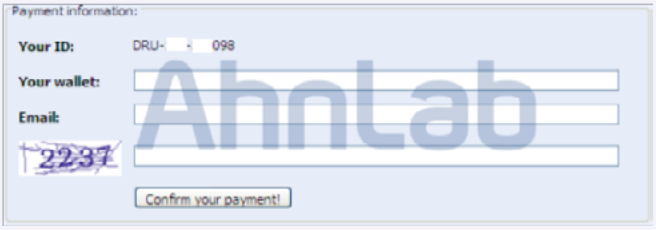


Figure 1-13 | Required fields to download a recovery tool

Also, BitCrypt provides a YouTube video link that shows how to recover encrypted files. (See [Figure 1-14].)

Figure 1-14 | BitCrypt decryption demonstration video link

V3 detects the malware as shown below.

<Malicious code names in V3 products>

-Trojan/Win32.Yakes (2014.02.12.03)

MALWARE TREND

03. Mobile Issues

Malicious Application Using "Tor" Emerged

As the number of malicious mobile applications increase, some of the malicious applications operate in the similar way to malware for Windows system. In this regard, it has been recently discovered that a malicious application "Tor" used anonymous network on Android OS.

Once the corresponding application is installed in an Android mobile phone, it collects data including phone numbers, location information, IMEI, model No. of the phone and the version of OS, and send the collected data to external servers. This malicious application uses the ".onion" domain to access to TOR servers that allows attackers to ensure anonymity and post anonymous websites in the ".onion" domain area. Also, it injects "Orbot", the Android open source, to enable to use TOR network on Android. (See [Figure 1-15].)

Figure 1-15 | Collected data and TOR server domain

This malicious application requests the user to register itself as a device administrator. When the user selects the "Activate" option to permit the application of the device administrator, it is able to obtain privileges to call, receive and send SMS, access to network, and be executed automatically at system startup. (See [Figure 1-16].) If the malicious application is registered as a device administrator, it is not deleted until the user canceled the registration manually.

This malicious application receives commands from C&C server shown as [Figure 1-17] and it intercepts incoming/outgoing SMS

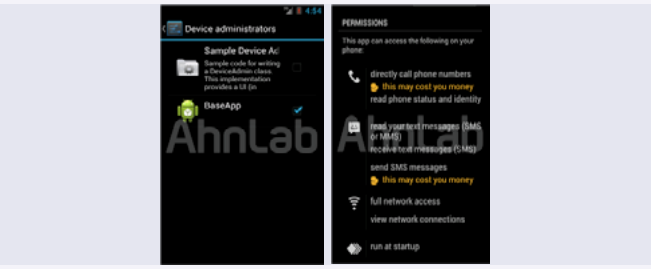


Figure 1-16 | Device administration registration and privilege acquisition

or USSD (Unstructured Supplementary Services Data) requests, or sends out SMS and application lists.

```
static
{
  commands.add("#intercept_sms_start");
  commands.add("#intercept_sms_stop");
  commands.add("#ussd");
  commands.add("#listen_sms_start");
  commands.add("#listen_sms_stop");
  commands.add("#check");
  commands.add("#grab_apps");
  commands.add("#send_sms");
  commands.add("#control_number");
}
```

Figure 1-17 | C&C commands

V3 Mobile detects the corresponding malicious application as shown below.

<Malicious code names in V3 Mobile product>

-Android-Backdoor/Torec.128C34

SECURITY TREND

01. Security Statistics

Microsoft Security Updates- February 2014

Microsoft released security bulletins for February 2014 with 7 security updates (4 critical, 3 important). One of the important updates is for the vulnerability of .NET Framework, which is used by attackers to compromise websites to obtain privileges. Thus, it is necessary to install these patches for safe use.

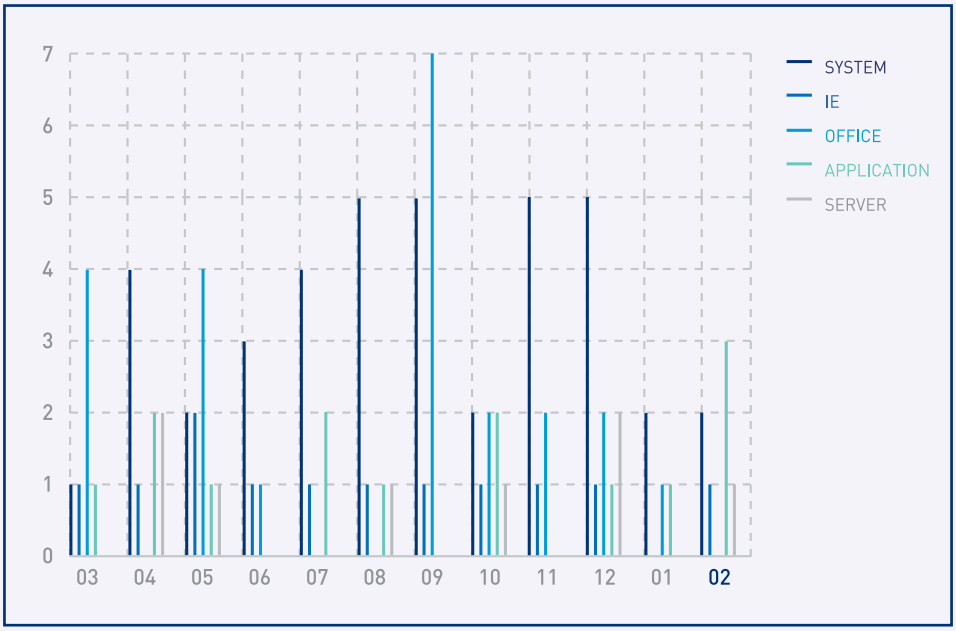


Figure 2-1 | MS Security Updates for each attack target

Critical	
MS14-010	052 Internet Explorer Cumulative Security Update
MS14-011	Vulnerabilities in VBScript scripting engine could allow remote code execution.
MS14-007	Vulnerabilities in Direct2D could allow remote code execution.
MS14-008	Vulnerabilities in MS Forefront Protection for Exchange could allow remote code execution.
Important	
MS14-009	Vulnerabilities in .NET Framework allow privilege elevation.
MS14-005	Vulnerabilities in Microsoft XML core service could allow information exposure.
MS14-006	Vulnerabilities in IPv6 could allow denial of service.

Table 2-1 | MS Security Updates for February 2014

SECURITY TREND

02. Security Issues

Apple's Critical Security Updates for iOS, SSL/TLS Vulnerability

Apple released the OS X Mavericks v10.9.2 security update on February 25, 2014. What is important about this security update is that it patches the "Gotofail" security vulnerability in SSL/TLS (Secure Sockets Layer / Transport Layer Security) encryption codes. The Gotofail security vulnerability in the SSLVerifySigned ServerKeyExchange function can be exploited to start Man in the Middle Attacks (MITM).

For example, when a user connects his laptop computer or portable devices to a network of cafeteria or other public place and uses Safari via SSL/TLS protocols, an attacker can steal any transmitted data. Installation of Apple security updates is strongly recommended since the Gotofail security vulnerability leaves users susceptible to critical security threats.

iOS devices should be immediately updated to the 7.0.6 version, other older devices need to be updated to the iOS 6.1.6 version, and OS X must be updated to the 10.9.2 version. To minimize exposure to potential eavesdropping or account hijacking, Chrome or FireFox can be used instead of Safari.

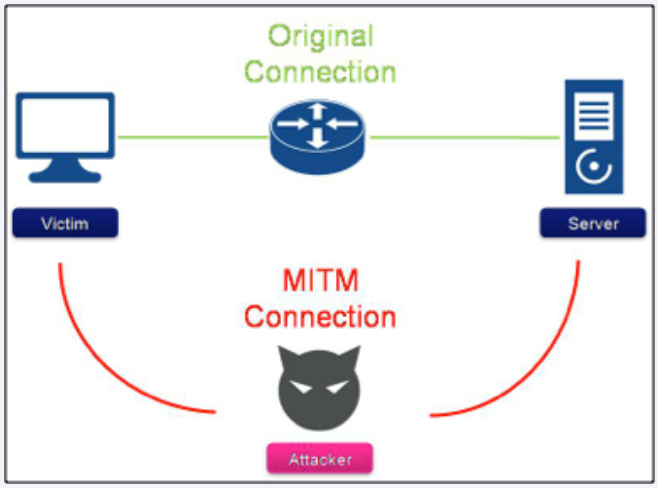


Figure 2-2 | MITM conceptual diagram

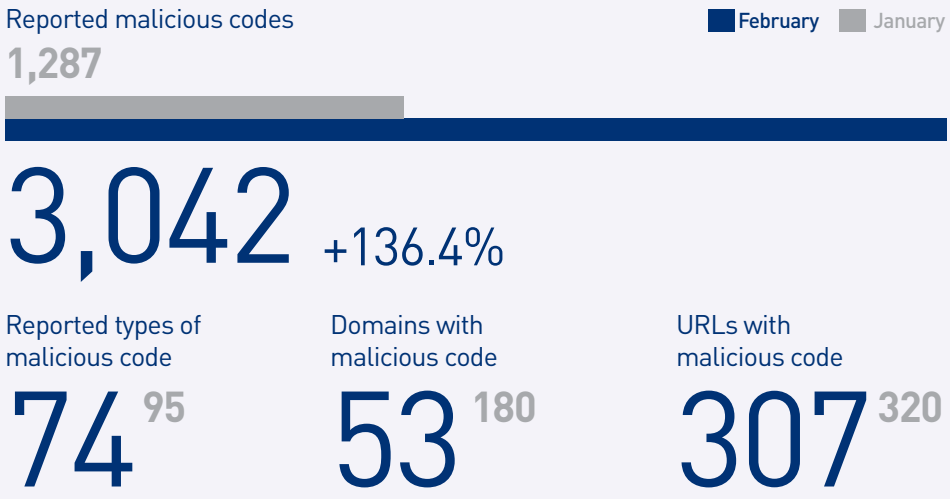
WEB SECUTIRY TREND

01. Web Security Statistics

Website malware trend

SiteGuard (AhnLab's web browser security service) blocked 3,042 websites that distributed malware in February 2014. There were 74 types of malware, 53 domains and 307 URLs that distributed malware were found. Compared to the previous month, the number of malware report, and the number of domains and URLs that distributed malware slightly decreased.

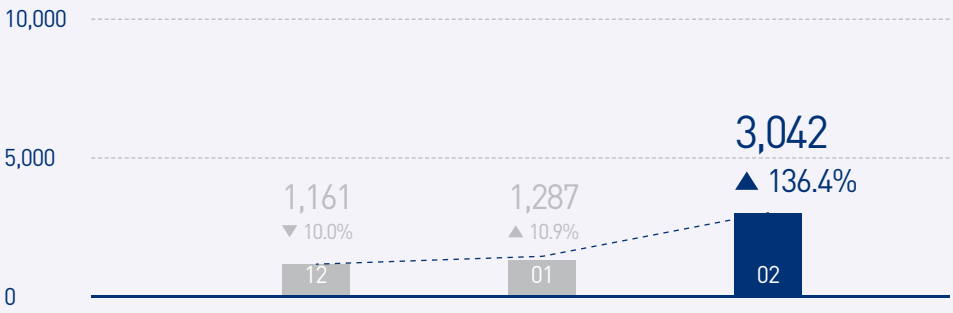
Table 3-1 | Website security trends for February 2014



Monthly change in malware detections

As of February 2014, the number of malware reports is 3,042 that is a 236% increase from the 1, 287 reported in the previous month.

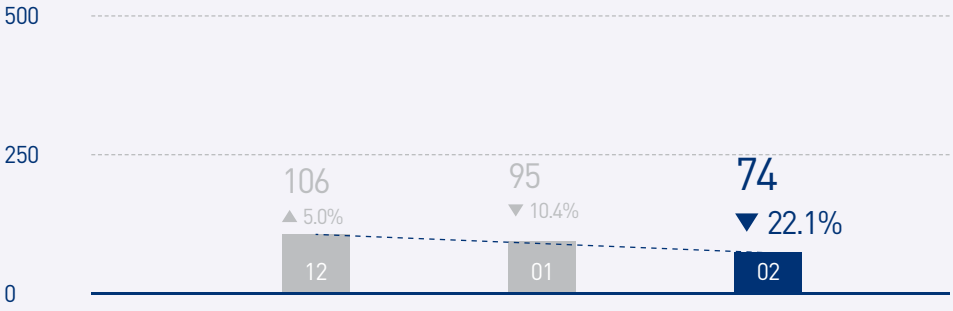
Figure 3-1 | Monthly change in malware detections



Monthly change in the number of reported malware types

The number of reported types of malware decreased to 74, 78% of 95 reported in the previous month.

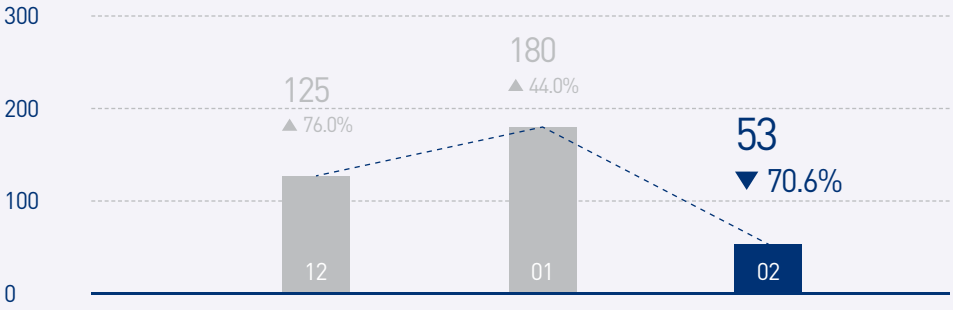
Figure 3-2 | Monthly change in the number of reported malware types



Monthly change in domains that distributed malware

The number of reported domains that distributed malware decreased to 53, which is 29% of 180 reported in the previous month.

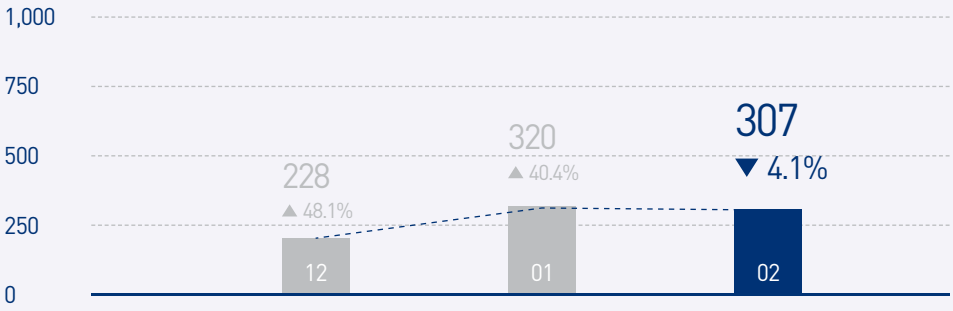
Figure 3-3 | Monthly change in domains that distributed malware



Monthly change in URLs that distributed malware

307 URLs that distributed malware were reported, which is 96% decreased from 320 reported in the previous month.

Figure 3-4 | Monthly change in URLs that distributed malware



Top distributed types of malware

Trojan was the top distributed type of malware with 1,356 (44.6%) reports, followed by Appcare with 1,259 (41.4%) reported.

Type	Report	Percentage
TROJAN	1,356	44.6%
APPCARE	1,259	41.4%
SPYWARE	84	2.8%
ADWARE	50	1.6%
DROPPER	12	0.4%
Win32/VIRUT	6	0.2%
DOWNLOADER	5	0.1%
ETC	270	8.9%
	3,042	100.0 %

Table 3-2 | Top distributed types of malware

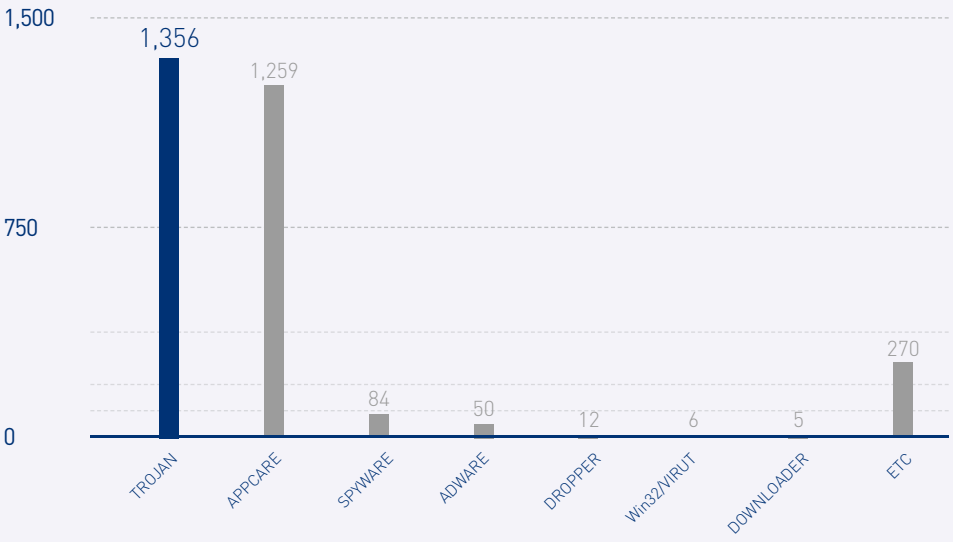


Figure 3-5 | Top distributed types of malware

Top 10 distributed malware

Win-AppCare/Exploit.233472 was the most distributed malware with 1,258 (44.8%) reports, and 6 malware, including Win-Trojan/Exploit.233472, newly emerged in the Top 10 list.

Ranking	↑↓	Malicious Code	Reports	Percentage
1	NEW	Win-AppCare/Exploit.233472	1,258	44.8%
2	NEW	Win-Trojan/Exploit.233472	548	19.5%
3	▼1	Win-Trojan/Downloader.950152	347	12.4%
4	▼3	Trojan/Win32.Agent	259	9.2%
5	NEW	PUP/Downloader.414184	217	7.7%
6	▼1	Spyware/Win32.Gajai	84	3%
7	NEW	Win32/Induc	29	1%
8	NEW	Adware/Win32.ProcessClean	23	0.8%
9	▼2	Win-Trojan/Downloader.12800.LU	22	0.8%
10	NEW	Trojan/ Win32.Buzus	21	0.8%
		TOTAL	2,808	100.0 %

Table 3-3 | Top 10 distributed malware (By Malicious Code Name)

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