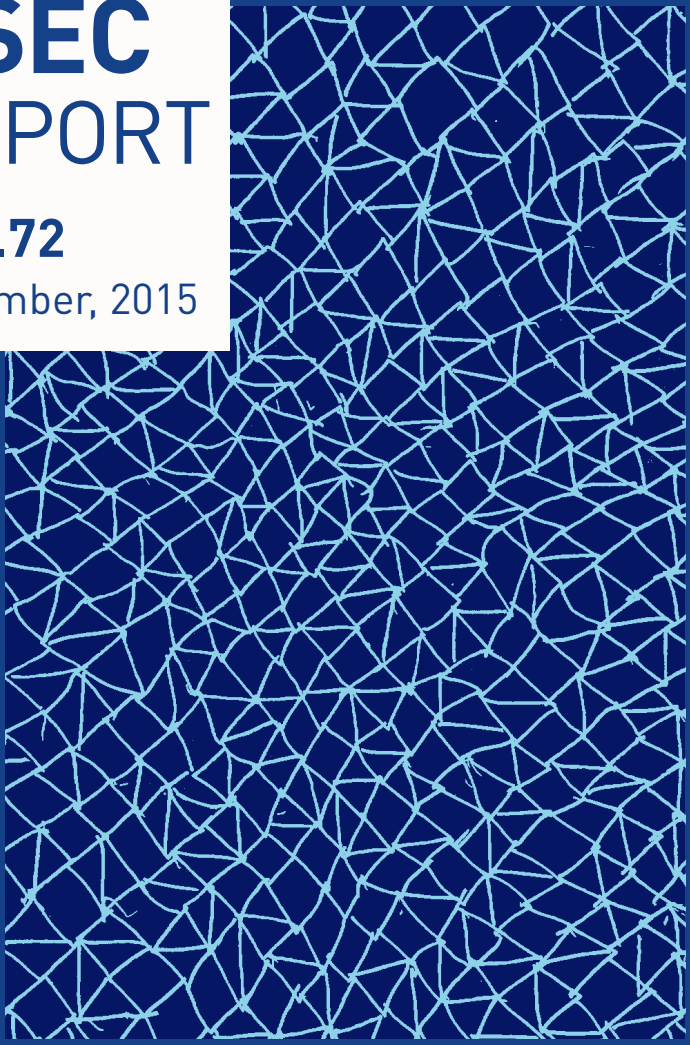
Security Trend

ASEC REPORT

VOL.72

December, 2015



AhnLab

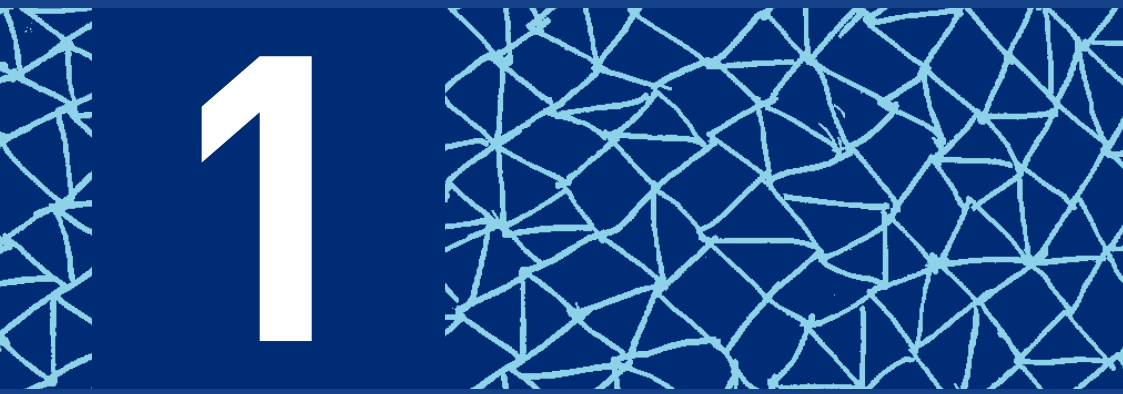
ASEC REPORT

VOL.72 December, 2015

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 December 2015

Table of Contents



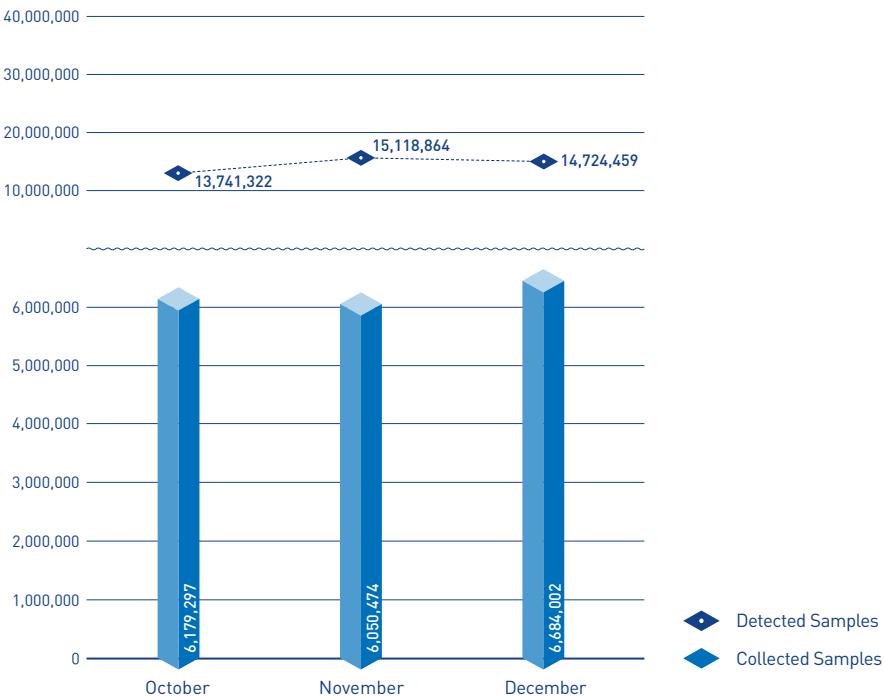
1

SECURITY STATISTICS

SECURITY STATISTICS

01
Malware Statistics

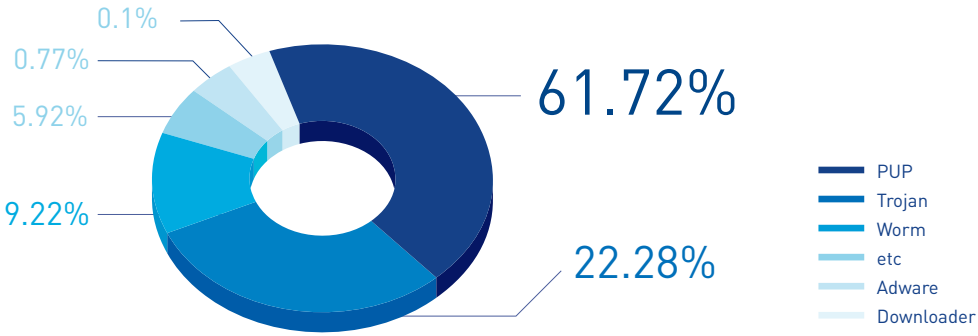
According to the ASEC (AhnLab Security Emergency Response Center), 14,724,459 malware were detected in December 2015. The number of detected malware decreased by 394,405 from 15,118,864 detected in the previous month as shown in Figure 1-1. A total of 6,684,002 malware samples were collected in December.



[Figure 1-1] Malware Trend

* "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 December 2015. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 61.72% of the total. It was followed by Trojan (22.28%) and Worm (9.22%).



[Figure 1-2] Proportion of Malware Type in December 2015

Table 1-1 shows the Top 10 malware threats in December categorized by alias. Trojan/SWF.Agent was the most frequently detected malware (196,608), followed by Trojan/Win32.Starter (191,120).

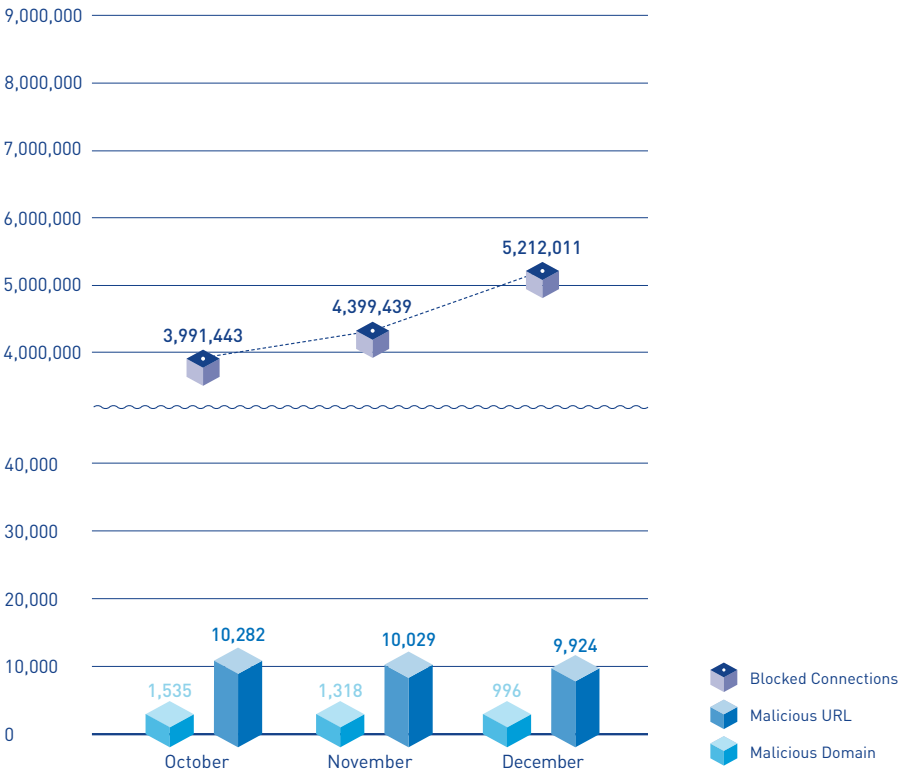
[Table 1-1] Top 10 Malware Threats in December 2015 (by Alias)

Rank	Alias from AhnLab	No. of detections
1	Trojan/SWF.Agent	196,608
2	Trojan/Win32.Starter	191,120
3	Malware/Win32.Generic	141,225
4	Trojan/Win32.Agent	117,330
5	Trojan/Win32.Gen	85,034
6	Trojan/Win32.Neshta	84,827
7	Unwanted/Win32.Exploit	71,726
8	HackTool/Win32.Crack	68,159
9	Unwanted/Win32.HackTool	67,421
10	Trojan/Win32.Teslacrypt	65,017

SECURITY STATISTICS

02
Web Security Statistics

In December 2015, a total of 996 domains and 9,924 URLs were comprised and used to distribute malware. In addition, 5,212,011 malicious domains and URLs were blocked.



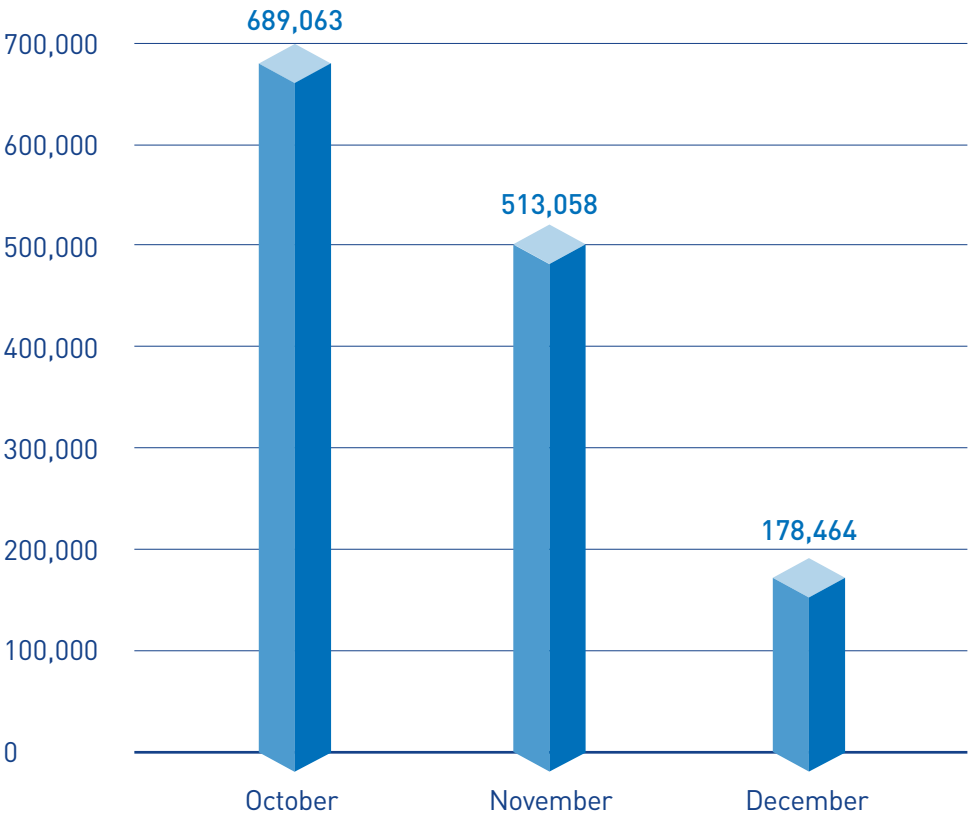
[Figure 1-3] Blocked Malicious Domains/URLs in December 2015

* "Blocked Connections" refers to the number of blocked connections from PCs and other systems to the malicious website by AhnLab products deployed by our customers.

SECURITY STATISTICS

03 Mobile Malware Statistics

In December 2015, 178,464 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 detected in December 2015. Android-PUP/SmsPay was the most distributed malware with 25,847 of the total.

[Table 1-2] Top 10 Mobile Malware Threats in December (by alias)

Rank	Alias from AhnLab	No. of detections
1	Android-PUP/SmsPay	25,847
2	Android-Trojan/FakeInst	25,382
3	Android-PUP/Noico	23,665
4	Android-PUP/SmsReg	22,146
5	Android-Trojan/Opfake	7,331
6	Android-Trojan/SMSAgent	6,888
7	Android-PUP/Dowgin	5,378
8	Android-Trojan/SmsSend	4,769
9	Android-Trojan/Slocker	3,933
10	Android-Trojan/SmsSpy	3,493

2

SECURITY ISSUE

SECURITY ISSUE

01 Localized Ransomware Circulated: Offline and Chimera

Ransomware exploded across the world in 2015. These malware are becoming more technologically advanced, and have recently shown signs of becoming "localized." While the messages contained in existing ransomware demanding payment were mostly written in English, ransomware using languages other than English have been increasingly discovered these days. CryptoLocker checks the IP range of the infected PC and outputs a message in the local language. For example, two new ransomware using local language are "Offline," written in Russian, and "Chimera," targeting users in the European region.

1. Offline Ransomware

The ransomware "Offline" uses the RSA algorithm, similar to more typical types of ransomware. However, instead of encrypting the files on the infected system by receiving a key from the C&C server, Offline generates a random key based on the infected system's information and the data in the targeted files, encrypting the files on the system in several stages. The targeted files, in other words, become encrypted without the need to communicate with a C&C server and receive a key, hence the name of the ransomware, "Offline."

Users need to exercise caution, as Offline is being most commonly distributed in the form of compressed RAR files attached to emails.

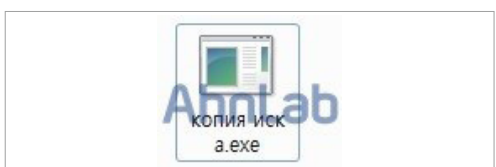


Figure 2-1 | File containing the ransomware Offline (after uncompressing the RAR file)

Figure 2-1 is an .exe file from uncompressing an RAR file; executing this file creates the following files and writes

them to the startup registry.

Table 2-1 | Files generated
C:\Program Files\1C\копия иска.exe (self-replication) %TEMP%\1C\копия иска.exe (self-replication)

Table 2-2 | Writing to registry (startup programs)
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\pr - C:\Program Files\1C\копия иска.exe

Then, the file stores a randomly-generated ID and time of infection, and issues a "GET" request to the URL as shown below:

Table 2-3 | Additional files generated, connection made to the URL
C:\Program Files\1C\[random file name]
www.res********a.co.uk/********/in**all/in**.**p

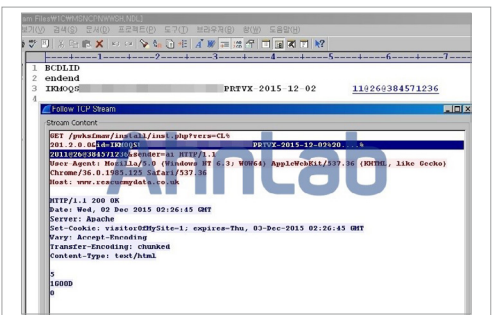


Figure 2-2 | Files generated (top) / connected to URL (bottom)

Once the encryption process is complete, an image file with a message in Russian as shown in Figure 2-3 is set as the desktop screen image. The message states, "Your files have been encrypted, and will be destroyed (unable to be decrypted) if an email is not sent to the indicated address in 72 hours." This message is another notable difference with other ransomware messages that generally provide a Bitcoin address and tell the user that "a recovery tool will be provided once the payment is verified."

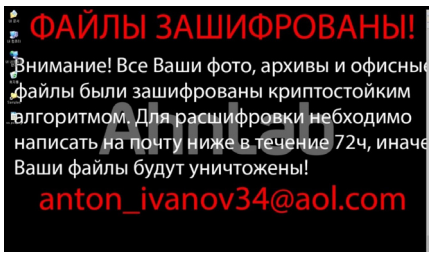


Figure 2-3 | Desktop image (message indicating infection)

2. Chimera Ransomware

Germany and other European nations have been witnessing the spread of a ransomware named "Chimera." When first discovered in September of 2015, infections were only reported in Germany and not deemed serious. However, the ransomware has been spreading recently, even issuing a call for co-conspirators.

Like other types of ransomware, Chimera generates an HTML page directing the user to an address for making the Bitcoin payment after the files in the infected system have been encrypted. However, a

notable feature is a threat to publish the affected files online if a payment is not made. Despite its claim, no actual feature enabling the distribution of encrypted files was found.

Figure 2-4 | Chimera ransomware

Chimera targets a wide variety of file extensions for encryption. Even files needed for operating Windows, such as boot.ini and system.ini, are encrypted.

Table 2-4 | File extensions targeted for encryption

*.jpg, *.jpeg, *.vmx, *.txt, *.xml, *.xsl, *.vbs, *.ini, *.conf, *.config, *.msg, *.key, *.htm, *.html, .class, .java,.cs, .asp, *.aspx, *.php, *.jsp, *.bak, *.dat, *.pst, *.eml, *.sql, *.js, *.jar, *.py, *.db, *.bay, *.png, *.bmp, *.gif, *.zip, .rar, *.bin, *.ptx, *.wav, *.ram, *.mkv, *.doc, *.docx, *.rtf, *.xls, *.xlsx, *.ppt, *.pptx, *.pdf, *swf, etc.

Once an infection takes place, the encrypted files are given the extension ".crypt." Some operating systems generate an alert that states, "Files required for running Windows have been altered with an unknown version. Restore with original files to maintain system stability."

Checking the source code for the HTML page that informs the user of the infection shows the following message from the ransomware's creators inviting "affiliates."

Figure 2-5 | Message from Chimera's creators seeking co-conspirators

The message tells anyone interested to use BitMessage, a P2P encrypted mailing system, apparently an attempt to avoid tracking.

While Chimera is being distributed through compromised web site recently, spam mail infections are still occurring requiring extra vigilance by users.

The relevant aliases from V3 products, AhnLab's anti-virus program, are as below:

<Aliases from V3 products>

Trojan/Win32.MDA (2015.12.01.04)

Trojan/Win32.Chimera (2015.11.10.07)

SECURITY ISSUE

02 Malware Targets Chinese Online Game Users

The growth of the online game market has been accompanied by a continuous onslaught of malware. With the Chinese online game market growing, malware targeting users of Chinese online games are proliferating. A recently-discovered malware was first spread via a Chinese gambling site. When the infection takes place, the malware uses an ordinary utility program to change the start page of major browsers to a certain portal site, as shown in Figure 2-6.

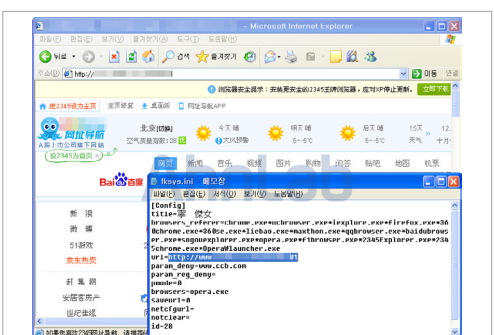


Figure 2-6 | The altered start page and the utility's settings file

Once the utility's setting file has been modified as shown in Figure 2-6, the browser takes the user to another start page instead of the web site designated by the user, creating an inconvenience.

The malware then issues a "GET" request to the C&C's IP address and extracts the OS information, MAC address, computer name and other information pertaining to the infected PC.

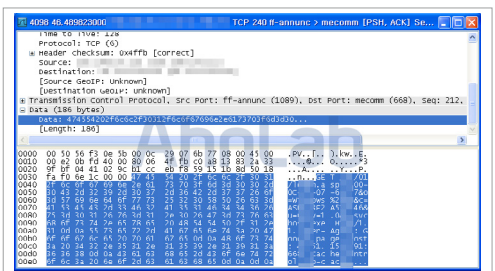


Figure 2-7 | User information being transmitted

Next, .txt files containing the download paths of additional malware are received periodically from the C&C server. Blocking the IPs in the .txt file is futile, since the additional download paths can

always be altered by getting new .txt files.

Table 2-5 | Paths for additional malware

svchost.exe||http://1.**.**.239:777/IE-32.exe
DNF.exe||http://42.**.***.191:668/down/DNF.exe
LolClient.exe||http://42.**.***.191:668/down/LolClient.exe
crossfire.exe||http://42.**.***.191:668/down/crossfire.exe
cstrike-online.exe||http://42.**.***.191:668/down/cstrike-online.exe
MapleStory.exe||http://42.**.***.191:668/down/MapleStory.exe
Game.exe||http://42.**.***.191:668/down/Game.exe
wow.exe||http://42.**.***.191:668/down/wow.exe
wow-64.exe||http://42.**.***.191:668/down/wow-64.exe
...
mir2.dat||http://42.**.***.191:668/down/7.exe
mir1.dat||http://42.**.***.191:668/down/7.exe
iexplore.exe||http://42.**.***.191:668/down/iexplore.exe

The file names listed in Table 2-5 are facsimiles of the run files of the most popular online games in China, and includes a number of games developed in Korea. The malware uses this list to check whether the process running matches with the first field value in the .txt files; when a match is found, the normal process is terminated and a malware bearing the same file name is executed. This appears to be an attempt to run the malware that is tailored to the job of stealing the account information from that particular game.

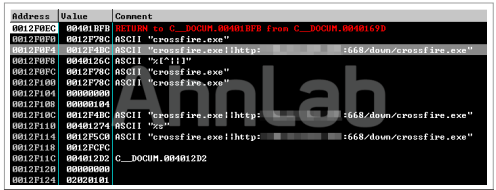


Figure 2-8 | Additional malware generated after comparing the with game's process name

The malware thus generated attempts to extract the account information of that particular game it was designed to target, and commonly connects to a C&C server to await the attacker's instructions.

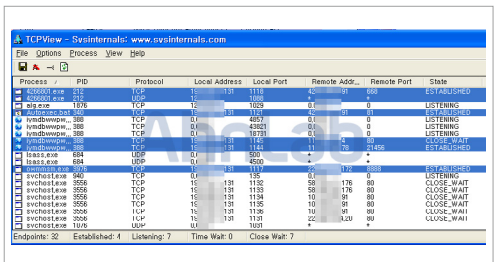


Figure 2-9 | Connection made to C&C server

Online games are attractive targets for attackers, since game items can easily be traded online and there is a large market for these digital goods. To prevent damages caused by malware targeting online games, users should make sure antivirus programs are kept up to date. Illegal programs related to games should be avoided, since there is a high likelihood that such files are related to malware.

The relevant aliases from V3 products, AhnLab's anti-virus program, are as below:

<Aliases from V3 products>

Malware/Win32.Generic (2015.12.03.00)
Backdoor/Win32.Farfli (2015.12.02.02)
Adware/Win32.Agent.R169696 (2015.12.03.01)
Dropper/Win32.Crypter (2015.11.24.05)

3

IN-DEPTH ANALYSIS

Crafty LNK Malware Continues to Circulate

IN-DEPTH ANALYSIS

Crafty LNK Malware Continues to Circulate

AhnLab has previously provided a review of LNK malware through an ASEC Report. With LNK malware continuously appearing, this article offers an in-depth analysis of this malware.

Once an LNK malware is executing, a normal Windows file, mshta.exe, is used to access a certain Web site, ultimately creating a malicious VBS script in the path "%TEMP%SysErrCheck.vbs".

Most types of malware display an ordinary document or output to the user as a disguise to prevent detection. LNK malware also receive a normal document file after running the malicious VBS to reassure the user. These documents are extracted from PCs that are already infected and used for subsequent attacks.

Along with the normal document file, the malicious VBS also downloads a suspicious image file. Figure 3-1 shows the malicious code contained in the image.

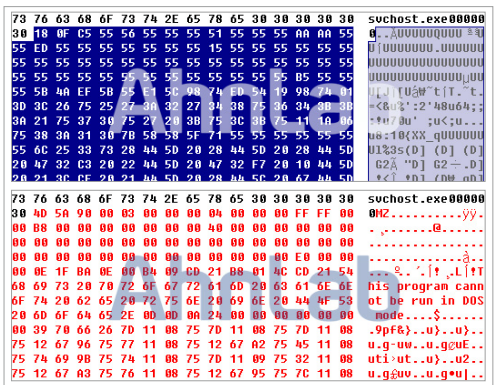


Figure 3-1 | Malicious code contained in the image file, before decoding (top) / after decoding (bottom)

The malicious code is decoded by moving to a certain location in the VBS file and carrying out an XOR operation to 0x55, creating and then running the file. The malware is merely a downloader for getting and running additional malware, and functions as shown in Table 3-1.

Table 3-1 | Downloader actions

1. Communicate with http://CNC server address/ update2014.php to verify server status.

2. Download malware encoded in http://CNC server address /download2014.htm
3. Leave a record on the server by making a request in the following URLs, based on the results of step 2:
3-1. When download is successful, access http://CNC server address /DownLoadSuccess.php
3-2. When additional downloads fail, access http://CNC server address /DownLoadFail.php
3-3. When download is made but PE recovery fails, access http://CNC server address /ExeFail.php

Files received from download2014.htm are encoded, which are decoded using base 64 and XOR'ed to 0x19, restoring them back to PE format.

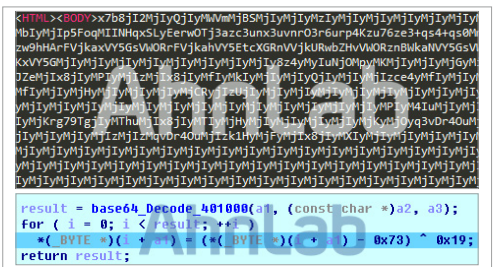
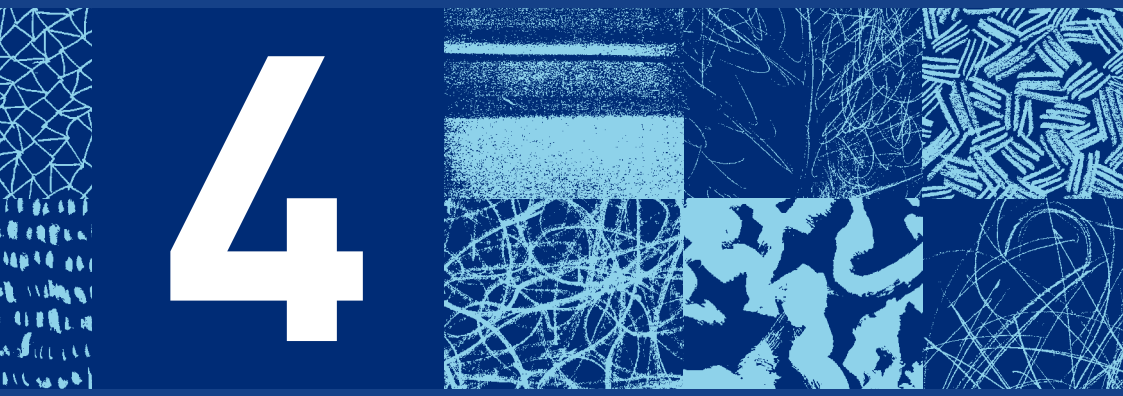


Figure 3-2 | Decoding the additional downloaded malware

The new malware that has been thus downloaded are saved to "%Temp%[random number]_res.tmp," with the time information of the file changed and moved to startup programs and run when Windows is restarted. The malware functions as a backdoor collecting computer information and downloading, uploading and running additional files, taking over the user's computer. To prevent infections from such malware, the user should take caution not to run attachments from unknown sources, carry out periodic and thorough system checks, and keep anti-virus software up to date.

The relevant aliases from V3 products, AhnLab's anti-virus program, are as below:

<Aliases from V3 products>
LNK/Downloader (2015.12.03.08)
VBS/Downloader (2015.12.03.08)
Trojan/Win32.Lnkdoor (2015.12.05.00)



2015 ANNUAL REPORT

01
The Top 5 Security Threats that Swept 2015

1. The Awakened Ransomware

Ransomware became a hot topic throughout the global information security field. Seeing the trend's explosive rise in areas such as North America and Europe, ransomware quickly expanded to South Korea with the massive spread of the Korean-language CryptoLocker, which hacked a well-known community site in April 2015 as its starting point.

From a technical perspective, previous ransomware mostly encrypted text files (doc, ppt, etc.) or image files (jpeg, for example); whereas as of recently, encryption has now expanded to target roughly 140 filename extensions including executable files (exe). In addition, the methods of encryption have advanced and ransomware have emerged that now make it impossible to operate a PC through locking the screen.

The "localization" of ransomware has also appeared. Ransomware such as BitCrypt and CoinValut in North America and Europe, and TrolDesh in Russia, Turkey and the East European Bloc, have caused considerable damage. Meanwhile, in Asia such as South Korea, there was a high infection frequency rate due to CryptoLocker, CryptoWall, TaslaCrypt and Nabucur.

2. It's All About Making 'Money': The Constant Threat to Financial Data

In 2015, malware that stalk financial data intensified their hunt as ever. Targeting over 1,000 banks and companies around the world, the notorious Dyre malware made the South Korean financial industry nervous by putting South Korean banks on its target list in the beginning of 2015. Recently, a trend of more evolved malware has appeared that steals data from the latest applications and browsers such as Windows 10 and Edge browser. The Banki malware, which steals data by luring

users through pharming sites, continues to rage on by altering its distribution method in the latter half of 2015.

Banks are not the only targets of malware attacks aiming to steal financial data. Entering 2015, POS malware that steal debit and credit card information through POS (Point of Sales) Systems started to increase. Some of the noticeable POS malware that appeared in 2015 include Cherry Picker and ModPos. Especially after the large-scale data breach of debit and credit cards at a major American retail chain store at the end of 2013, there has been a continuous stream of large and small POS security breaches throughout the world.

3. A Fierce Attack of Web Exploit Toolkit

After countless security threats involving ransomware that hit 2015, we then had the Web Exploit Toolkit. They revealed their presence with a much more sophisticated method of attack than before.

As an attack tool that preys upon numerous vulnerabilities and infects a user's PC with malware, Web Exploit Toolkits are used by attackers to easily create and spread malware. The most notorious Web Exploit Toolkit that ravaged 2015 was the Angler Toolkit.

When attackers use a Web Exploit Toolkit to spread malware, he or she uses content management systems or blogging tools to make it difficult to track its spread. It has also used the 'Malvertising' technique, a method which distributes malware by using advertising sites that create dynamic content. In addition, the Web ExploitKit has become a more serious threat through even more elaborate efforts to divert detection by anti-virus program.

4. Adware, its Extension into the Mobile Environment

Adware, which has irritated many online users with its excessive exposure of advertisements, has moved into the mobile environment.

The number of mobile adware discovered in 2015 increased by roughly 2.5 times. Mobile adware has gone beyond irritating smartphone users with its collection of personal data, excessive advertising, and app switching, and is now inflicting damages through malicious behavior. In addition, new mobile adware disguise as popular apps or obtain root privileges to prevent themselves being deleted by smartphone users.

Other mobile security threats are either similar to last year or show a slightly reduced trend in South Korea. After mobile banking malware showed a rising trend of more than doubling every year since 2012, it maintained a similar number to last year; Smishing, a method of spreading mobile malware, showed a downward trend in the second half of 2015. This can be seen as the result of user security education and proactive efforts to block Smishing by South Korea's National Police Agency, KISA (Korea Internet & Security Agency), government agencies, security vendors, and mobile carriers as well as the private sector.

5. Internet Routers, IoT: The Rising Threat of "Connecting"

From the beginning of 2015 and continuing from 2014, hacking attacks continuously were discovered that targeted the vulnerabilities of shared wired and wireless connections of well-known router manufacturers. Exploiting the vulnerabilities in shared connections by acquiring administrative privileges, the danger is high that there will be simultaneous attacks on mobile devices and PCs that share connections.

The security threat to devices connected to a network is not only limited to shared connections but the range of attack has expanded to the Internet of Things (IoT). Recently, various personal wearable devices have increased such as the personal usage of IoT devices, but so has the amount of concerns regarding their security. The typical IoT devices such as the IP Camera, NAS (Network Attached Storage), and CCTV have operating systems similar to general computers, which attackers know very well and can easily access to. While these devices are constantly connected to a network, we are still currently in a state where we lack appropriate security measures. To securely use devices that are constantly in a "connected" status such as Internet routers and IoT devices, the individual users' efforts are crucial such as frequently changing administrative passwords and maintaining firmware updates from manufacturers.

02
The Top 5 Security Threats that Will Dominate 2016

1. Continual Advancement of Ransomware

The threat of ransomware is expected to grow more unruly in 2016. Continual evolution is expected with the expansion of ransomware's encryption targets, and the addition of functions that interfere with user's operations such as the freezing of screens. In particular, as security vendors including AhnLab enhance their ransomware response technologies, it is expected that advanced ransomware will either bypass detection or hamper these security products.

The possibility of mobile ransomware expanding its harm throughout the world is also high. The number of ransomware targeting the Android mobile operating system increased more than 12-fold in a single year from 2,220 cases in 2014 to 27, 845 cases in 2015. In 2016, it appears that ransomware variants will continue to increase. As of yet, most mobile ransomware has targeted English-language users and have been produced using English. However, it is just a matter of time before mobile ransomware in different languages will emerge that inflicts tremendous harm on smart phone users, just as PC ransomware had.

2. Cyber Terrors to National Infrastructure on the Rise

The Paris Terror Attacks at the end of 2015 shocked the world. As with religious and political tensions, international conflicts have also taken place in the cyber world. While past terrorist activities were limited to physical damages, terrorism has already deeply infiltrated the cyber environment with ideological propagation and information collection through the internet, wiretapping/ blackmailing of hostile countries and data theft, etc.

In regards to terrorism's goal of creating fear in the general public, it is not

possible to rule out the possibility of APTs (Advanced Persistent Threats) that target national infrastructure.

Of course, these infrastructure facilities are tightly protected with numerous security systems and operate in a closed network environment. As a principle, most do not connect directly with the internet and thus, the probability of being exposed to threats is relatively low. Still, incidents of cyber attacks on national infrastructure have continued to occur, including the infection of the Stuxnet worm at the Bushehr Nuclear Power Plant in Iran, a data leak of nuclear power plants in Japan, and the recent data breach into the control system of a New York dam in the U.S.

As the international situation rapidly changes according to political conflicts and the long-term effects of the global recession, the importance of security for national infrastructure is even further emphasized.

3. Vulnerability Exploitations Will Be Intensified

In 2016, attacks that take advantage of software (hereinafter "SW") vulnerabilities will become even more rampant.

Microsoft announced that aside from its most recent version, technical supports and updates for previous versions of their Internet Explorer (hereinafter "IE") web browser would end as of January 12, 2016. Thus, even if new vulnerabilities are discovered in older IE versions, new patches will not be offered after January 12, and thus, attacks aimed at these vulnerabilities are expected to increase.

Last year, a large number of vulnerabilities were also discovered in text editing programs and other programs used by many people. Because these attacks that take advantage of vulnerabilities in popular SW can easily avoid the suspicion of users, it's clear that this will be the main attack method in the future. Beyond the simple report of vulnerabilities, specific damage caused by attacks that exploit these vulnerabilities are expected to occur in 2016.

In addition, specific vulnerabilities, including the VENOM (Virtualized Environment Neglected Operations Manipulation) vulnerability, which may occur in the virtual environment system, have been discovered in 2015 that execute the arbitrary code in a virtualization solution. Recently, as many corporations inspect their adoption of cloud and virtual infrastructure, it is likely that security

threats to these environments will become more specific.

4. The Realization of Threats that Will Surround IoT, Smart Home Systems

With the rapid pace of development in IT technology and devices, the scope of cyber threats has now expanded vastly beyond the PC. As more IoT devices that function and perform as well as computers continue to emerge in quick succession and as the number of devices that connect to the internet continue to rise, new cyber threats are projected to increase commensurately.

Security threats need to be urgently considered for Smart Home technology, which has developed heating control and household power control systems, including wireless routers often seen in most homes. Aside from this, it is anticipated that threats to drones and "Connected Cars", which is also known as smart cars that is equipped with Internet access and also with a wireless network, will soon become a reality, the validation and verification legislation of which is being negotiated in full swing among nations.

5. Emerging Threats to New Financial Environments

As financial data and systems are always a prime target for cyber threats, the level of threats worsens as the financial environment becomes increasingly online. In South Korea, it is projected that the security threats will lay siege to specialized internet banks as they are introduced at the beginning of 2016.

In addition, great concerns have been raised regarding the threat to mobile transactions through the use of smartphones. Recently, the use of smartphones for mobile transactions such as mobile banking and shopping has rapidly been increasing. Over the past few years, there have been frequent occurrences of damages through the theft of financial data by mobile malware such as micropayment fraud and the Bankun malware. Because pharming attacks aimed at smartphone users are on the rise, there is a need for greater security in mobile financial transactions.

AhnLab

ASEC REPORT

VOL.72
December, 2015

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