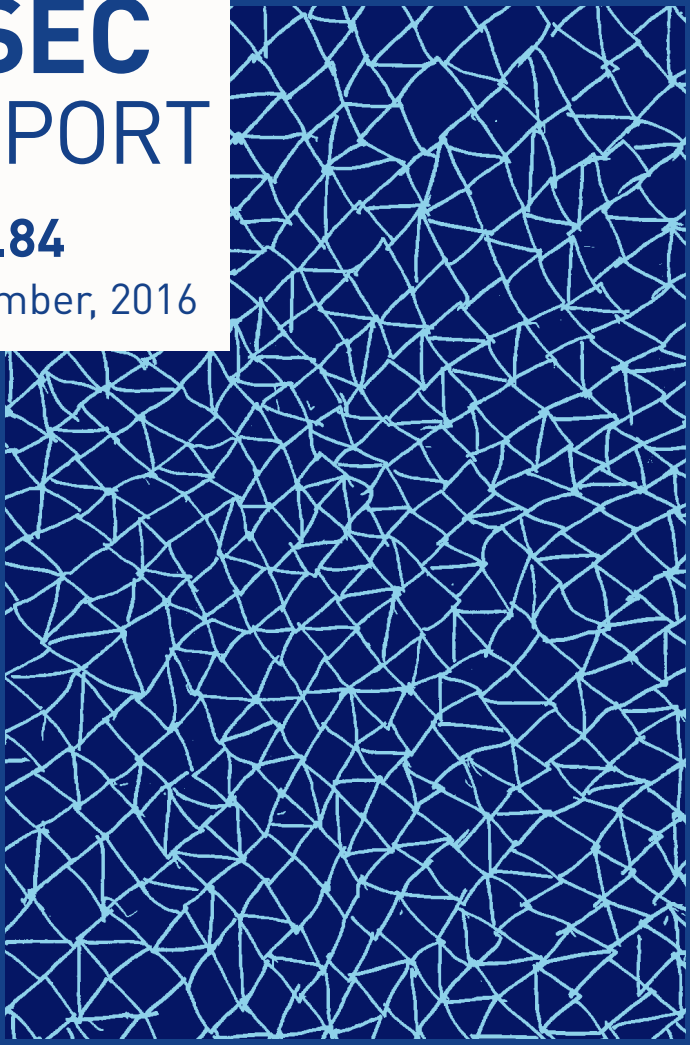
Security Trend

ASEC REPORT

VOL.84

December, 2016



AhnLab

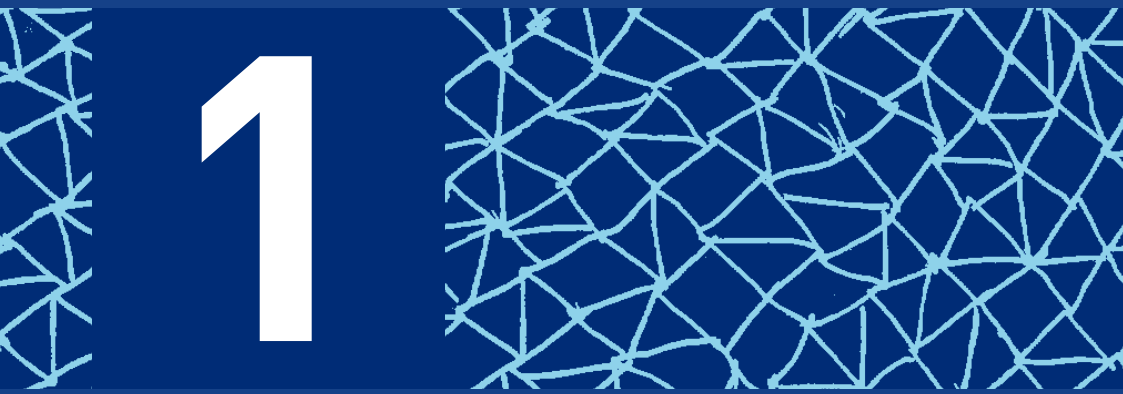
ASEC REPORT

VOL.84 December, 2016

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 2016

Table of Contents



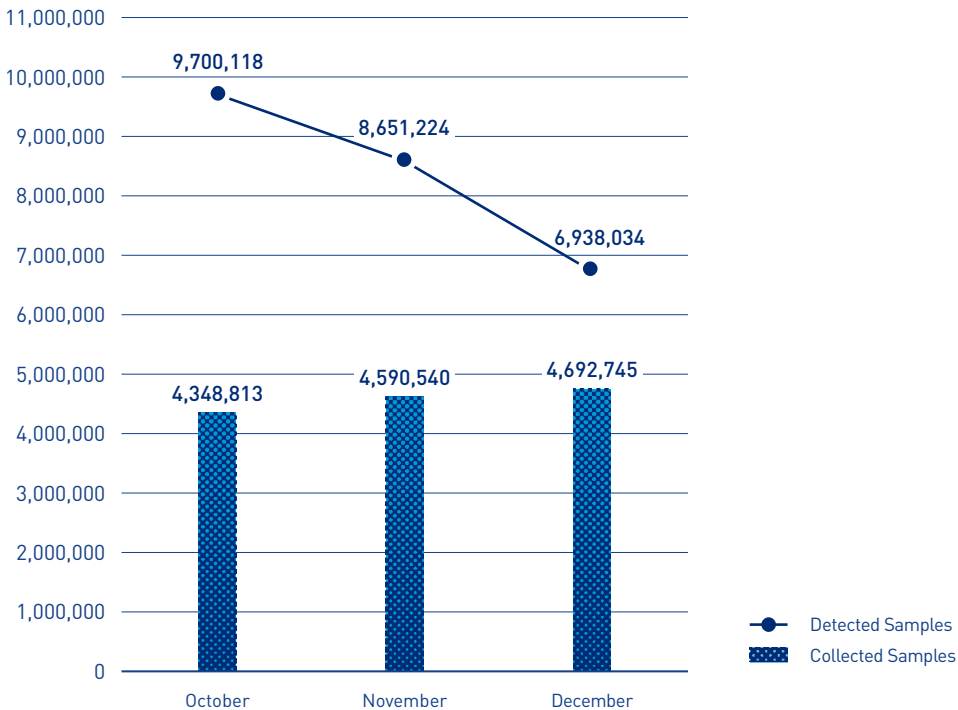
1

SECURITY STATISTICS

SECURITY STATISTICS

01
Malware Statistics

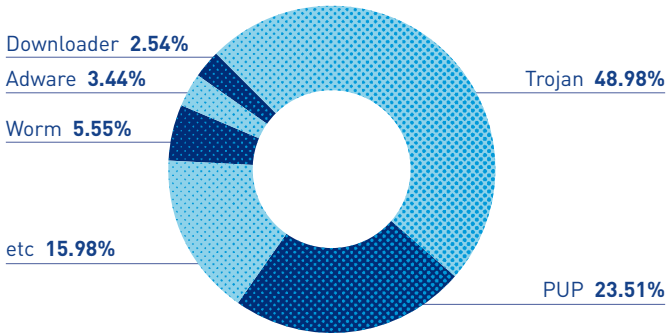
According to the ASEC (AhnLab Security Emergency Response Center), 6,938,034 malware were detected in December 2016. The number of detected malware decreased by 1,713,190 from 8,651,224 detected in the previous month as shown in Figure 1-1. A total of 4,692,745 malware samples were collected in December.



[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 2016. It appears that Trojan was the most distributed malware with 48.98% of the total. It was followed by PUP(Potentially Unwanted Program, 23.51%) and Worm (5.55%).



[Figure 1-2] Proportion of Malware Type in December 2016

Table 1-1 shows the Top 10 malware threats in December categorized by alias. Worm/Win32. IRCBot was the most frequently detected malware (317,192), followed by Trojan/Win32.Starter (277,706).

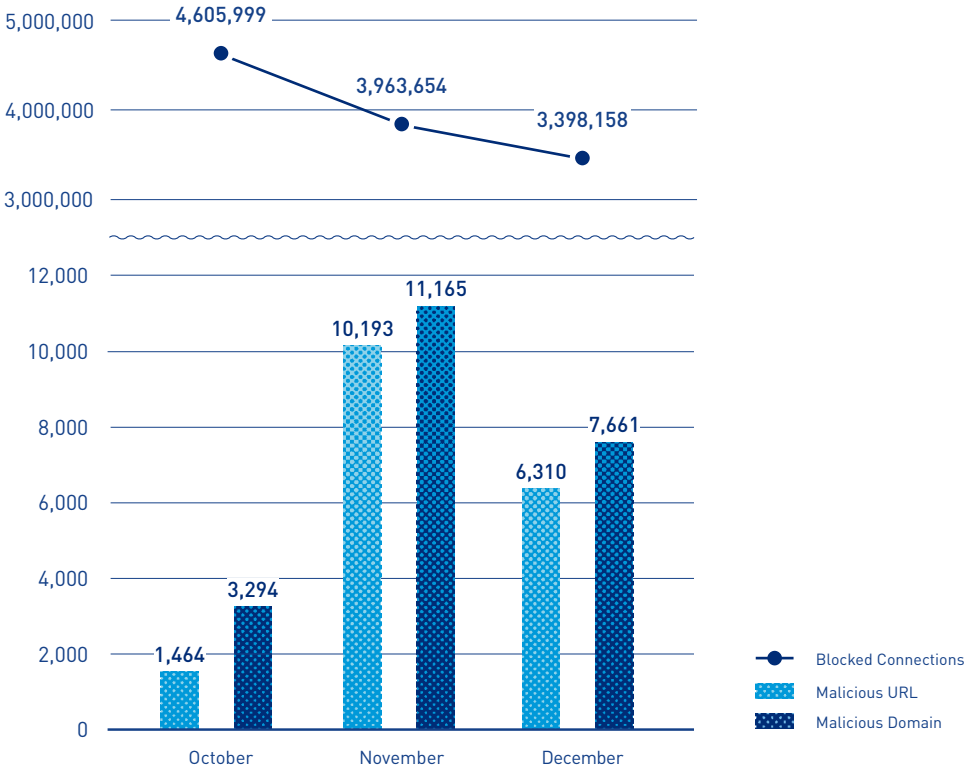
[Table 1-1] Top 10 Malware Threats in December 2016 (by Alias)

Rank	Alias from AhnLab	No. of detections
1	Worm/Win32.IRCBot	317,192
2	Trojan/Win32.Starter	277,706
3	Trojan/Win32.Banki	159,981
4	Malware/Win32.Generic	154,620
5	Unwanted/Win32.HackTool	115,199
6	Trojan/Win32.Cerber	104,462
7	Trojan/Win32.Downloader	91,232
8	Trojan/Win32.Agent	80,939
9	Trojan/Win32.Nitol	74,782
10	Trojan/Win32.Neshta	69,072

SECURITY STATISTICS

02
Web Security Statistics

In December 2016, a total of 6,310 domains and 7,661 URLs were comprised and used to distribute malware. In addition, 3,398,158 malicious domains and URLs were blocked.



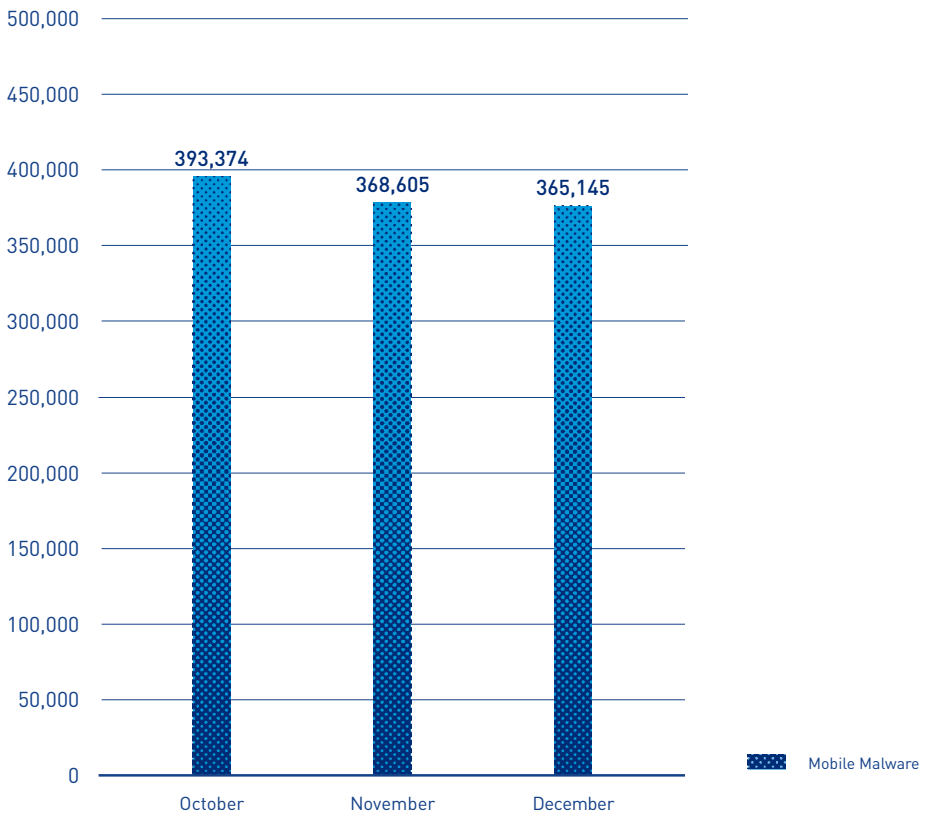
[Figure 1-3] Blocked Malicious Domains/URLs in December 2016

* "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 2016, 365,145 mobile malware were detected as shown in Figure 1-4.

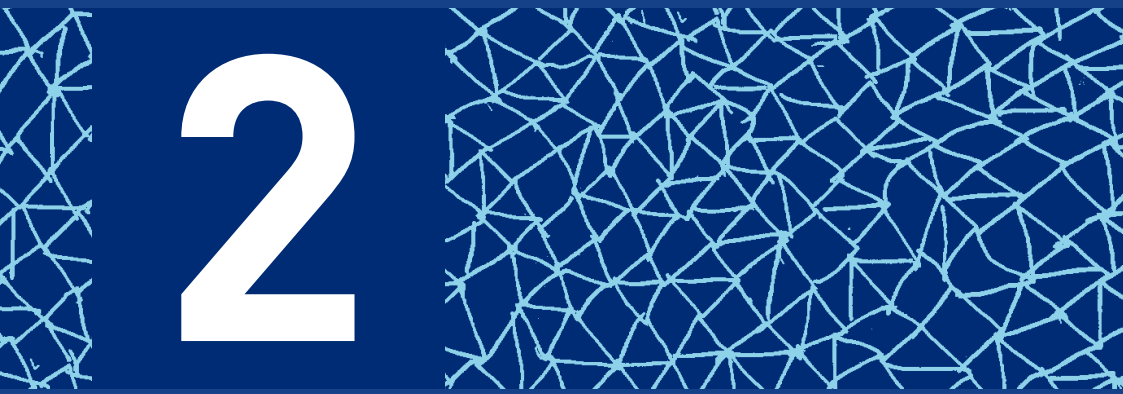


[Figure 1-4] Mobile Malware Trend

Table 1-2 shows the top 10 mobile malware detected in December 2016. Android-PUP/SmsPay was the most distributed malware with 57,515 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	57,515
2	Android-PUP/Baogifter	34,831
3	Android-PUP/Shedun	31,098
4	Android-Trojan/SmsSpy	25,744
5	Android-PUP/SmsReg	18,214
6	Android-PUP/Agent	18,192
7	Android-Trojan/Jimo	15,891
8	Android-Trojan/SmsSend	14,143
9	Android-Trojan/Agent	12,704
10	Android-Trojan/Slocker	12,050



2

SECURITY ISSUE

Ransomware Targets Online Bargain Hunters

SECURITY ISSUE

Ransomware Targets Online Bargain Hunters

Late last November, a spate of spam email messages targeting shoppers during "Black Friday" and "Cyber Monday" was discovered.

These latest spam emails are disguised as official email from Amazon, the famous online shopping Web site. The fake email, bearing the subject "Your Amazon.com order has dispatched (sic)" even contains detailed shipping and refund/exchange information.

Figure 2-1 | Email disguised as a message from a shopping site

The email includes a compressed file, which contains a JavaScript (JS) file as shown in Figure 2-2.

Figure 2-2 | Compressed JavaScript file contained in the attachment

The JS file, which is the ransomware downloader, is obfuscated to make analysis and recognition difficult.

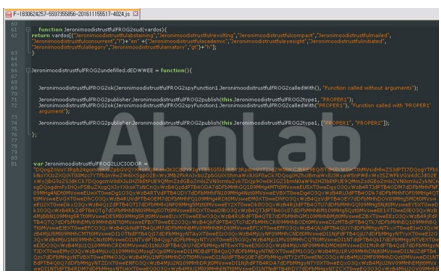


Figure 2-3 | Ransomware downloader in obfuscated JavaScript form

Double-clicking on the malicious JS file opens a connection to the URLs listed in Table 2-1 and downloads the ransomware.

Table 2-1 | URLs access by the malicious JS

hxxp://minoritycounselor.com/7845gf?ocDCoWDVHY=ocDCoWDVHY
hxxp://muzica-evenimente.ro/7845gf?ocDCoWDVHY=ocDCoWDVHY
hxxp://mediclo.pl/7845gf?ocDCoWDVHY=ocDCoWDVHY
hxxp://teazexebec.com/7845gf?ocDCoWDVHY=ocDCoWDVHY
hxxp://chewysissy.net/7845gf?ocDCoWDVHY=ocDCoWDVHY

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

<Aliases identified by V3 products>
JS/Obfus.S166 (2016.11.10.03)
BinImage/Ransom (2016.12.01.06)

With more shoppers looking for deals on online shopping sites, malicious email purporting to be sent by well-known Web sites are being spotted with increasing frequency. These emails lure users into clicking them with subjects such as "payment", "return" and "receipt".

To prevent being harmed by these malicious messages, users should avoid opening email from unknown origins or running suspicious attachments. Vigilant users should also develop the habit of closely monitoring not only the sender's name but the email address as well.

3

IN-DEPTH ANALYSIS

GoldenEye Ransomware Encrypts Files and MBR

IN-DEPTH ANALYSIS

GoldenEye Ransomware Encrypts Files and MBR

The so-called GoldenEye ransomware has been discovered, which encrypts both files as well as the master boot record (MBR). GoldenEye is a variant of Petya and Mischa ransomware that were discovered last March and May respectively. Whereas Petya only encrypts the MBR while Mischa selectively encrypts either files or the MBR, the recently-discovered GoldenEye targets both files and the MBR. Petya, Mischa and GoldeEye are all known to have been created by Janus Syndicate, which draws its name from the crime organization featured in the James Bond film "Golden Eye".

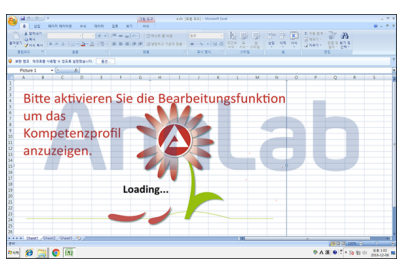


Figure 3-1 | Excel file containing the malicious macro

GoldenEye, which targets German-language users, is being distributed via spam email disguised as a fake resume. The email contains a PDF file and an Excel file containing a malicious macro. Opening the Excel file displays a message in German stating that the macro file cannot be used as shown in Figure 3-1. When the user enables the macro function, the malicious macro is executed and the ransomware attack commences. The macro creates the files listed below, then runs them.

Table 3-1 | Locations of the files created by the malicious macro

C:\Users\[user account]\AppData\Local\Temp\radA3ACA.exe
C:\Users\[user account]\AppData\Roaming\{db864363-a5b3-4623-a8cf-fa919cd7b079}\java.exe

Figure 3-2 | Malicious macro contained in the Excel flie

Once executed, the files first generate a ransom message. The message informs the user of the ransomware infection as shown in Figure 3-3, instructing the user to download the Tor browser in order to make the ransom payment.

Figure 3-3 | Pay-up warning dialogue of GoldenEye

File encryption begins once the ransom note has been generated; once complete, eight random characters are added to the extensions of affected flies as shown in Figure 3-4.

Figure 3-4 | File extensions added after encryption

Unlike more run-of-the-mill ransomware, however, GoldenEye does not stop at encrypting files. Once the first stage of encryption is complete, the ransomware makes modifications to the C:\ path, assumed to be part of the preparation process for MBR encryption.

When the user reboots the system, instead of the regular Windows logo a screen indicating that CHKDSK, a program used to repair errors on the hard disk, is shown to be running as displayed in Figure 3-5. However, this is in fact a bogus program created by GoldenEye. While it appears that the hard disk drive is being repaired, the ransomware is encrypting the MBR that contains booting and disk partition information.

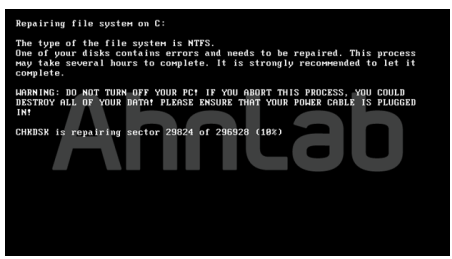


Figure 3-5 | MBR encryption underway

Once the MBR encryption is complete, the depiction of a skull appears on the desktop as shown in Figure 3-6. This is another feature shared in common with Petya and Mischa. However, while Petya uses an image in red and white and Mischa a skull in green and yellow, GoldenEye, as befitting its name, uses a yellow and gold color scheme.

Figure 3-6 | GoldenEye's skull image

Once the image appears, pressing any key displays the same message contained in the previously-generated TXT file.

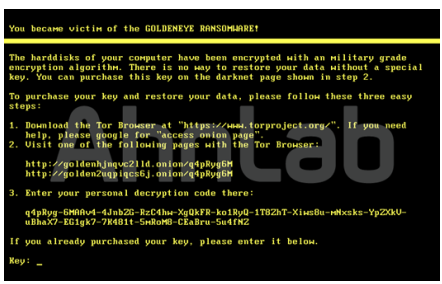
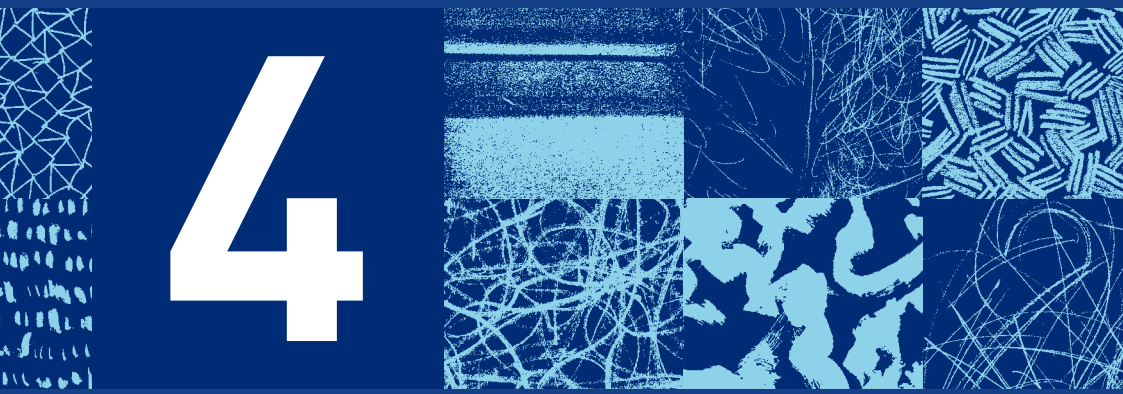


Figure 3-7 | Pay-up warning dialogue displayed after MBR encryption

The relevant aliases identified by V3 products, AhnLab's anti-virus program, for the GoldenEye ransomware are as below:

<Aliases identified by V3 products>
Trojan/Win32.Agent (2016.12.07.05)
W97M/Petya (2016.12.08.00)
W97M/Petya (2016.12.09.00)

Unlike the similar Petya, which only encrypted the MBR, and Mischa, which either encrypts files or the MBR, GoldenEye can wreak considerable more havoc by attacking both files and the MBR. The preferred vector for GoldenEye are spam email messages. These email bear subjects such as "payment" or "receipt" in order to lure users into clicking email that appear to be related to business or online transactions. Email from suspicious senders should not be opened in order to prevent infections from email-delivered ransomware.



2016 ANNUAL REPORT

01
The Top 5 Security Threats that Engulfed 2016

1. Ransomware, the Threat That Locked Up the Whole World

The different types of ransomware increased abruptly in 2016, causing enormous damage worldwide. According to ASEC (AhnLab's Security Emergency-response Center), at the beginning of the year, ransomware-related security breaches reported only 15% of the total cases, but became 60% of the total by the end of November. Ransomware threat evolved through a repeated process that involved different kinds of changes, and even periods of inactivity.

TeslaCrypt, which was notorious in 2015, announced they were shutting down their activities. Also, CryptXXX, which caused massive damage in Korea, has been quiet since last July. On the other hand, Locky, which spread via spam, and CERBER, with its ransom notes and sophisticated websites, are being constantly upgraded. Also, new types of ransomware that encrypts MBRs (Master Boot Records) to interfere with the use of the PC itself, have also appeared.

This year in particular, the so-called Ransomware-as-a-Service (RaaS), ransomware services that produce and disseminate ransomware for profit, have started to pick up steam and accelerate the diffusion of ransomware throughout the world. Although most ransomware is programmed in English, there is also ransomware that supports different languages, such as TeslaCrypt, CryptXXX, Locky, CERBER, and others.

Dissemination and infection methods are being diversified constantly. Attaching files to spam, drive-by downloads, malvertising, Remote Desktop Protocol

(RDP), and combining social engineering techniques are becoming more advanced.

2. Targeted Attacks, Cost-efficient with No Boundaries

Targeted attacks have increased significantly over the past few years due to their cost-efficiency. These attacks are generally directed at normal companies with political or financial purposes.

The security incident of the US Department of Homeland Security's personnel information in February, 2016, is widely suspected to have been the work of Russia. The security breach on the NSA by the Shadow Brokers organization last August is also linked with international spy act.

Targeted attacks directed at individuals usually have political purposes: Targeted attacks were mostly directed at politicians or social activists who oppose the ruling parties in countries such as Hong Kong, Myanmar, Syria, the UAE, and Kazakhstan.

The traditional cyberattacks on companies involves stealing customers' personal information. This year, two large-scale personal information attacks were carried out on Yahoo and Dropbox. Also, the business email scam, a conventional e-mail falsification scam, caused tremendous damage to companies in North America and Europe, and is still ongoing. According to FBI reports, there were around 7,000 cases of email falsification in the US, resulting in losses of $7,400,000.

3. The Preemptive Attack of IoT Malware

As Internet of Things (IoT) technologies advance, so do IoT-related threats. IoT devices use embedded Linux systems, which are lightweight in terms of usability and feature low power consumption. The reality is that Operation Systems used by user terminals are not easy to manage, and security is often overlooked, particularly by small manufacturers. Attackers have not missed this point.

In September, 2016, record-breaking DDoS attacks were carried out against security blog Krebs on Security and the hosting company OVH. A US Internet hosting service provider, Dyn, was also the target of DDoS attacks. This attacks took advantage of connection problems

on websites such as Twitter, The New York Times, Airbnb, PayPal, Netflix, SoundCloud, and others. It was confirmed that both attacks utilized the IoT malware, Mirai. Various IoT devices were exploited in this attack and, just this year, more than 10,000 IoT malware were discovered after the source code of some malware was released to the public.

Recently, IoT terminal manufacturers have started to pay close attention to security problems. However, it is not easy to constantly monitor IoT devices once purchased and installed. Assuming they will be used for 5 years after installation, attacks using IoT devices can occur any time during the operation period.

4. Survival of the Exploit Kit: Fierce Attacks on Vulnerabilities

The Exploit Kit (EK) is a tool that distributes large quantities of malware programs that target vulnerabilities. This tool is becoming more and more active as the ransomware black market grows. There has also been fierce competition between Exploit Kit developers.

Angler EK and Nuclear EK, which were the most distributed ransomware programs in the first half of last year, suddenly disappeared, and the activity of Neutrino EK, which inherited the position of Angler EK, also decreased in the second half of the year. On the other hand, Sundown EK and Magnitude are still constantly active.

The Exploit Kit's multilevel redirection technique is mainly used to distribute different kinds of malware (including ransomware) in malvertising attacks. The distribution of both downloaders with different script formats and Exploit Kit-based ransomware is constantly occurring. People have even discovered malware that uses Window's Powershell.

Also, as the use of the Exploit Kits increases, distinct vulnerability attacks have grown stronger, including those that exploit the vulnerabilities of Internet Explorer, Flash, and Java. Particularly, there has been an increase in the distribution of malware that exploits the vulnerabilities of Encapsulated PostScript (EPS), which is related to document files, and Open Type Font. It was also

discovered that AtomBombing, a code injection technique that exploits design flaws in the Windows OS, affects all versions of Windows.

5. Rooting App Rooted in Mobile Environments

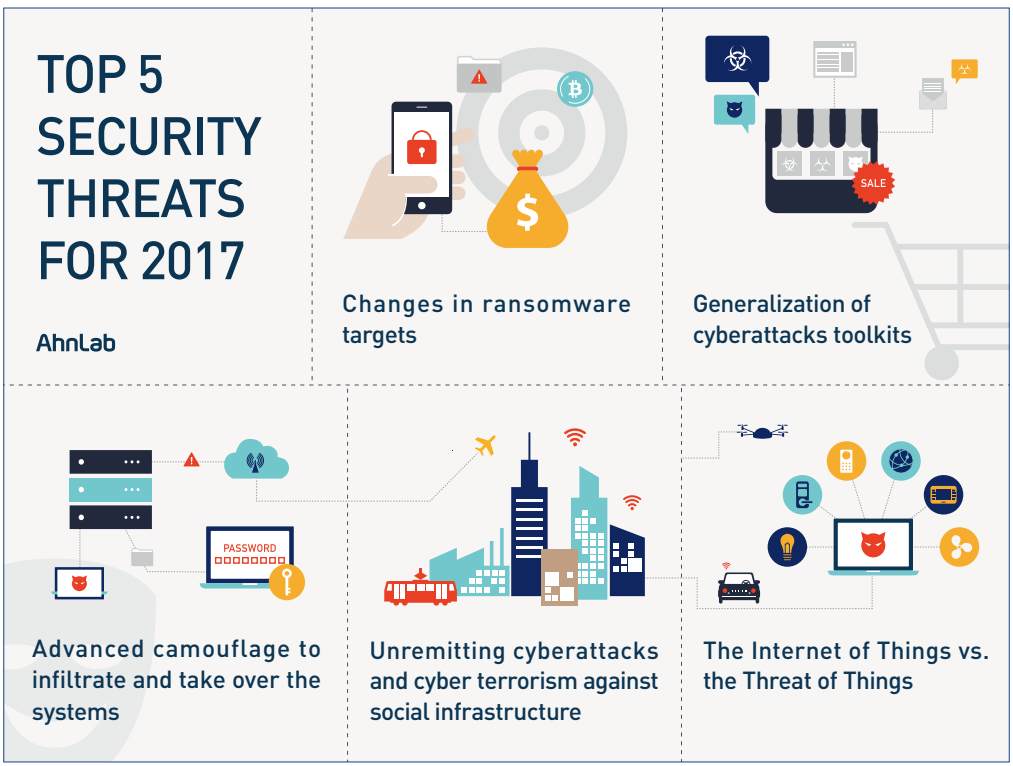
In 2016, a number of malicious apps that root Android-based smartphones were discovered. Particularly, from July to October this year, the number of rooting apps collected by AhnLab increased by 30% compared to the first half of 2016. This shows that the number of malicious apps are constantly increasing.

Generally, malicious apps secretly install other apps or bypass the detection and removal functions of a smartphone's antivirus software and use root privileges to perform malicious acts, such as taking personal information or displaying ads. In the last first half of the year, the most common malicious apps were those that use root privileges to show ads or secretly install other apps. In the second half of the year, rooting apps that steal financial information have started to appear. It was confirmed that malicious apps made in China mostly try to acquire root privileges to earn profits by displaying ads or installing apps.

Rooting apps exploit Android OS vulnerabilities to acquire privileges over smartphones. Godless, which is a malicious app discovered in the first half of the year, exploited various vulnerabilities in Android OS v5.1 (Lollipop) and lower to acquire root privileges.

As malicious apps that exploit Android OS vulnerabilities increase, Google is also taking various steps to bolster Android's security. Ever since discovering the Stage Fright vulnerability in 2015, monthly security updates for Android OS have been made available, and the update order of smartphone manufacturers is made public. This year Android OS v7.0 (Nougat) was announced. It cannot be booted after system modulation attempts via rooting. The problem is that there are some cases in which security updates are not supplied, depending on the smartphone manufacturer or production year of the terminal. Therefore, users of smartphones with outdated OS versions should pay special attention to security.

02
The Top 5 Security Threats that Will Sweep Over 2017



1. Changes in ransomware targets

Ransomware that spread widely over the past year has become a useful criminal tool for gaining money from an attacker's point of view. For corporates in particular, there have been cases of ransom payments being made since corporates felt risk of interrupting business or losing important data, such as customer information. With the creation and

distribution of Ransomware as a Service (RaaS), ransomware has become a market unto itself with both consumers and suppliers.

Ransomware threats are expected to increase in frequency and range of attacks this year. With the goal being to acquire money, it is only natural that attackers will target places where money flows. So far now, phishing and pharming scam have mainly took lead financial cybercrimes, but now ransomware is expected to become a mainstream of financial cybercrimes. Also, ransomware has combined with spear phishing and other cybercrime campaigns that target foreign trade transactions and companies.

2. Generalization of cyberattacks toolkits

Not so long ago, it was considered that cyberattacks were committed by IT experts and hackers or hacking groups. Nowadays, however, it is possible to generate malware or launch cyberattacks without any IT knowledges and skills since it has become easier to find malware tool kits and a variety of cyberattack services such as RaaS (Ransomware as a Service) and spam mail delivery services not only from the he cyber black market but also via public internet. The generalization of cyberattacks is expected to be exploited for more crimes; it becomes more difficult to specify and investigate who is behind the cybercrimes.

Attackers will continue to use drive-by download method that malware is automatically installed when visiting a website or viewing an e-mail message. Also, attackers will enhance attack techniques, such as exploiting software security vulnerabilities more actively against users who do not apply software security patches. In order to prevent these exploit-based attacks, corporate security managers should regularly check websites and pay extra attention to attacks via web shells.

3. Advanced camouflage to infiltrate and take over the systems

Until 2010, most hackings against corporates were committed to steal confidential business data or customer information. Recently, however, the purpose of cyberattacks against corporates has shifted to attempts to infiltrate and take control of corporate internal infrastructure.

These types of attacks combine with multiple techniques to penetrate companies and organizations successfully.

The attackers acquire system account by collecting information from employees within the company and then escalate their access to the corporate infrastructure by exploiting infected systems. They then repeat to search and collect various accounts until they finally obtain the privileges to take control the entire systems.

When attackers successfully take over the systems, they are able to use the company's infrastructure as an attack base for large-scale attack: they can distribute malware disguised as normal programs required for accessing the company's services, which users must download and install on their personal computers. These infected computers also can be used for attacks against other corporate systems; that is why this type of attacks are not likely to be discontinued this year.

4. Unremitting cyberattacks and cyber terrorism against social infrastructure

The political and economic conflicts over the world will be more intensified this year; ideological conflicts between nations will be deepen. Also, cyber terrorism that targets foreign organizations will not halt.

Along with online services used by citizens, the latest cyberattacks target nearly every type of company and organization regardless of service type or size. It is presumed that there are primarily terrorist organizations or hostile countries behind the most cyber terrorism, such as attacks on social infrastructures. Motivations for these types of attacks can also be found in religious, ideological, and political conflicts, in addition to monetary motives. If attacks against social infrastructures succeed, it can maximize the effects of propaganda by causing social confusion and fear. Since it is never easy to resolve religious and political conflicts, thus these types of attacks continue to increase.

Most systems in social infrastructures are separated from network and are not directly connected to the external Internet. However, if there is even one system connected to the Internet or there is any point connecting the Internet and the internal network, it is not completely

free from security threats. No matter how the systems are protected, the most vulnerable point is always the human; there can be an employee who violates security policies by mistake or other reasons, simply because of inconvenience. Attackers have always keep that it mind and continue targeting human error using various methods to exploit these kinds of vulnerabilities.

5. Internet of Things vs. Threat of Things

The development and proliferation of Internet of Things (IoT) technologies will be accelerated this year; so the IoT security threats do. Due to the lack of IoT device manufacturers' security awareness, the IoT devices with security vulnerabilities continue to be sold. The attackers will never miss the chance; malware target IoT devices will rapidly increase this year.

Last year in the United States, there was a large-scale DDoS attack launched via IoT devices that had been infected with Mirai malware. Once IoT devices are sold or installed, they are used as-is for many years, and thus it is difficult to manage security status. In addition, most IoT device manufacturers can't afford to address security problems due to the lack of funds or technologies. Meanwhile, it is difficult to raise the prices for security enhancement considering the low power and low cost are the main factor for users.

Therefore, it is necessary to foster co-operation between security companies, government agencies, and manufacturers to prevent security threats related to the fast-growing IoT device market. In addition, as various countries rush to develop IoT technology and products competitively, it is difficult to solve a wide range of security threats caused by IoT devices through current regulations. It is imperative to establish a minimum inspection system for IoT devices and to prepare practical guidelines for strengthening security measures through multinational cooperation between governments, industry associations, and manufacturers worldwide.

AhnLab

ASEC REPORT

VOL.84
December, 2016

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

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

©AhnLab, Inc. All rights reserved.