# FSI 2017 Cyber Threat Intelligence Report (Eng)

This is English translated version of the original report released at <http://www.fsec.or.kr/common/proc/fsec/bbs/21/fileDownLoad/1235.do>

Profiling threat groups targeting homeland

Campaign Rifle:

Andariel, the Maiden of Anguish

# Header

2016 February, Novetta in the association with security firms (KasperskyLab, Symantec, TrendMicro, JPCERT/CC etc) released the profiling report entitled “Operation Blockbuster: Unraveling the Long Thread of Sony Attack”. The Lazarus group that was identified as the actor of the attack by the report still remains active and Novetta’s research has helped in responding and preventing against the attacks by the Lazarus group worldwide. However there is certain limitation that the global security firms in intelligence gathering on the attacks happened inside of South Korean homeland, and it is lacking in the information regarding the attacks driven by the Lazarus group or smaller threat groups that are deemed to be a Lazarus member groups. In this regards, FSI conducted profiling of the IT infrastructure and characteristics of the working environment of the homeland and the attacks against them. The results are described in this report. However, some of the contents are not clearly confirmed, and the estimation of the circumstances is also included.

|  |
| --- |
| This report is based on technical facts and some assumptions. It may show different views depending on the method of analysis and can not be quoted as official position of Financial Security Institute. |

# 01. Summary

It is not easy to track attackers and authors while analysing incidents and malicious codes. Especially in the case of cyber terrorism which thoroughly hides itself while attacking. Therefore, analysts profile TTPs (Tactics, Techniques and Procedures) throughout the incidents for profiling the attackers (groups).

Such profiling result helps to understand attack scenario and concealing method when analysing new incident and malicious code. In addition, it predicts attack targets and purpose of the attack, checks the readiness against the attacks, prevents damage and enable preemptive response.

Financial Security Institute tracked the associations of multiple known incidents and malicious codes from 2015 to early 2017, and identified it as a series of actions by the same actor that we call as the campaign ‘Rifle’.

***Rifle***

The PDB \* path of the malware sample that was the starting point for profiling the threat group contained the string rifle as follows:  
\* Program database for debugging when developing programs using Visual Studio

E:\Data\My Projects\Troy Source Code\tcp1st\rifle\Release\rifle.pdb

It is common to use code names when publishing a threat group or an incident analysis report. This unique code name is given to analysis processes related to cyber terrorism (war), such as using code names to prepare confidential outflows in military operations or to give meaning to action names and clarify missions and commands. Likewise, major incidents in cyberspace refer to a single incident as an operation and a series of successive incidents as a campaign.

The behind of the rifle campaign was identified as an attack group associated with the Lazarus group that committed cyber terrorism such as the DDoS attack and system destruction. Financial Security Institute named Andariel as the attacking group that carried out the rifle campaign and tracked the major incidents (operations) occurred in homeland.

The operations in the Rifle campaign include financial, military, defense, large corporations, organisations against North Korea, and security companies. Started since 2014, attacks have begun to reveal the damage from early 2016 where the malware infections and information breach were confirmed by the investigations by Prosecutors, Police and Ministry of Defense. It has also been confirmed that small/medium enterprises and university research institutes have also been compromised to be used as C&C servers and multiple zero-day vulnerabilities and stolen code signing certificate were used in the attacks.

This report provides an overview of the operations performed by the Andariel Group, as well as how they were profiled, and the results of the association analysis. However, in some operations, the details are not known, and the situation has been identified based on malicious code samples collected from various routes.

## A. Lazarus Group

Lazarus Group is a representative threat group named by the global security industry and one of the threat groups that are estimated to have technical and organizational capabilities, presumably based on the government of a particular country. In particular, they are considered to be the actor of multiple cyber attacks against homeland including 7.7 DDoS attack in 2009, 3.4 DDoS attack in 2011, 3.20 cyber terror in 2013 (operation DARKSEOUL) that destructed computer network of financial institutes and media broadcasting companies, and attack against Sony Pictures Entertainment (Operation Blockbuster) in November 2014, and so on.

They are considered as a cyber attack organisation in North Korea as a result of investigation by the prosecutors and police of homeland, US FBI and others. In the [Operation Blockbuster report](http://operationblockbuster.com/) published by Novetta in 2016, through the outcome of TTP (especially malicious code) profiling, series of attacks were analysed as the attack by the same actor.  In addition, it is also suspected to have carried out the Company I's personal information breach occurred in 2016 and [WannaCry Ransomware outbreak that affected the worldwide 2017](https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group).

Recently, the attacks of the Lazarus group have changed, and the FSI has separated the tracking effort into several different groups related to Lazarus based on the attack target selection criteria and the malicious code profiling results. Among them, the groups that are active in their activities are Bluenoroff, an attack center for global financial companies, and Andariel, who has campaigned for a Rifle campaign in homeland. These groupings are based on technical facts but the analysis results may differ due to the amount of information collected or differences in interpretation.

## B. Bluenoroff Group

Symantec, Kaspersky Lab, BAE Systems and others, in response to attacks on global financial companies including SWIFT fraud in Bangladesh announced in February 2016 and watering hole attacks via the Polish financial agency homepage, pointed Lazarus group as the actor behind of the attacks.

In April 2017, [Kaspersky Lab analysed](https://securelist.com/files/2017/04/Lazarus_Under_The_Hood_PDF_final.pdf) the results of an attack on a global financial company and reported the analysis with the name of the new threat group Bluenoroff that links to the Lazarus group. [Group-IB also analysed](http://www.group-ib.com/lazarus.html) C&C It traced the composition and revealed its connection with North Korea.

They have mainly attacked overseas financial companies. However, in January of 2017, they started exploiting the weakness of the network separation solution of the financial company to infect malicious code on internal network PC. Recently, they used WebDAV Vulnerability (CVE-2017-7269) in an attempt to infiltrate financial companies internal server. There have also been attempts to leak important information after infiltration through spear phishing and WebShell for IT developer company.  
  
From April 2017, malicious code which is presumed to be Bluenoroff’s work was found from the attack using Hangul document. By profiling a series of circumstances and incidents in 2017, we estimate that it started customised attacks against homeland. It has been monitored that Bluenoroff are continuously expanding footholds of C&C servers by using WebDAV vulnerability which increases the tension of the threat. Accordingly FSI are strengthening its profiling and monitoring on this group.

## C. Andariel Group

While analysing a series of incidents and attack attempts occurred in homeland, we has identified new organisations that are related to Lazarus group. As a result of tracking their activities, we observed that, although there are certain similarities to the malicious codes used in DARKSEOUL, most of the malicious codes were new. Also they presented different malicious codes and attack pattern from the Bluenoroff group who attacked global and homeland financial companies using the vulnerability in network segregation solution.

Therefore we determined there are two different threat groups with different TTP are attacking different targets at the same time, since around 2014 likely due to being restructured from the Lazarus group, and named this threat group as Andariel.

***Andariel***

The name of Lazarus is the character of the game Diablo, which is made of Bible motif. Andariel also borrowed that name to show his connection to Lazarus as a character in Diablo.

Andariel and Bluenoroff have a common roots in Lazarus, but there is a difference in the target or purpose of attack. In particular, Bluenoroff focuses on global financial companies including some in South Korea, and Andariel focuses on attacks targeting companies and government agencies in South Korea using customised attack methods.

Recently, they are exploiting zero-day vulnerabilities in IT products installed in endpoint in the form of ActiveX or an agent, and are carrying out omnidirectional attacks including infiltrating into the software developers to find vulnerabilities.

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat Group** | **Lazarus** | **Bluenoroff** | **Andariel** |
| Attack target | Homeland government agencies, finance, broadcasting etc. | Homeland and global financial companies | Homeland financial companies Homeland small and medium-sized IT companies  Large corporations  Ministry of Defense and defense industry |
| Purpose | Social chaos | Economic benefit  (SWIFT, bitcoin, etc.) | Stealing confidential information and economic benefits |
| Major Activities | ~ Recently | 2015 ~ | 2014 ~ |
| Major Incidents | - 7.7 DDoS Attack  - 3.4 DDoS Attack - 3.20 Cyber Terror - Sony Pictures Entertainment USA - Personal information breach in Company I - WannaCry Ransomware | - SWIFT illegal transaction of central bank of Bangladesh - Compromise of the website of the Polish Financial Supervisory Service and watering hole attack - Attacks on network segregation environment of financial institutions | - Data breach in large corporations  - Infiltrate into Defense network  - Malware infection on ATM managed by Company VAN  - Malware distribution via financial companies union homepages |

# 02.  Campaign Rifle

## A. Identification of the campaign

In order to determine that the attacks that happened on different targets and in different time to be done by the same threat group, the association through digital forensics and malicious code analysis should be conducted. The same C&C server or malicious code may be used in other incidents, or a unique pattern may be found in malicious code used in multiple incidents.

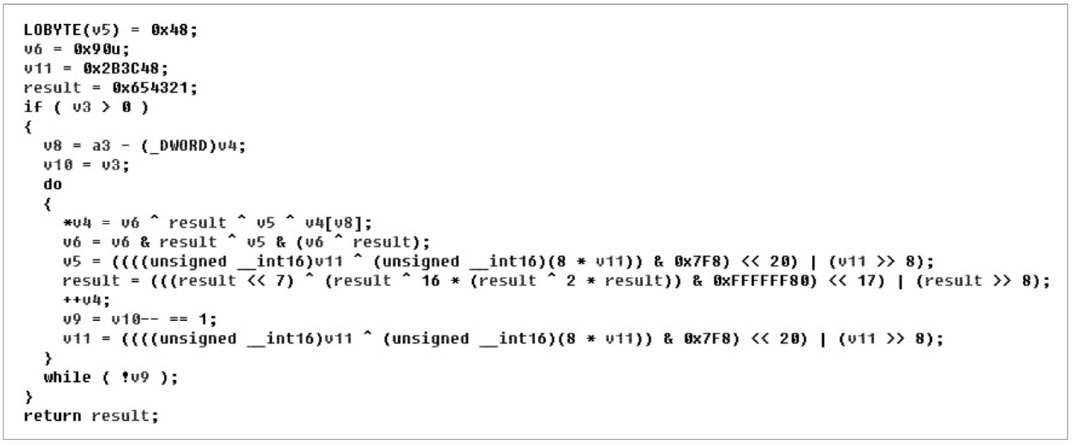
As described in the reason for naming the campaign as Rifle, we started tracking the series of attacks since we found the string "rifle" in PDB path of the malware that used the stolen code signing certificate from the company I (Operation INITROY) in February 2016.

E:\Data\My Projects\Troy Source Code\tcp1st\rifle\Release\rifle.pdb

The same PDB string and similar functions were found in malicious code used in ADEX spear phishing (XEDA operation) in 2015, and the same code pattern was confirmed in malicious code disguised as DRM module by Company “S” found in early 2016.

The same code pattern that was discovered through the static analysis of the malware was the code for transforming the obfuscated string. While the attackers often use the unique concealment technique to make the malware analysis difficult or to protect the data communication, they not only use the well known encryption algorithms but also use relatively light bit-operation or substitution method. Transform codes found are also based on XOR operations and are commonly identified in malicious code related to series of incidents that we will discuss below.

♦ XOR Transform: EE778BE503FDA770EE2F40E51EDFD595

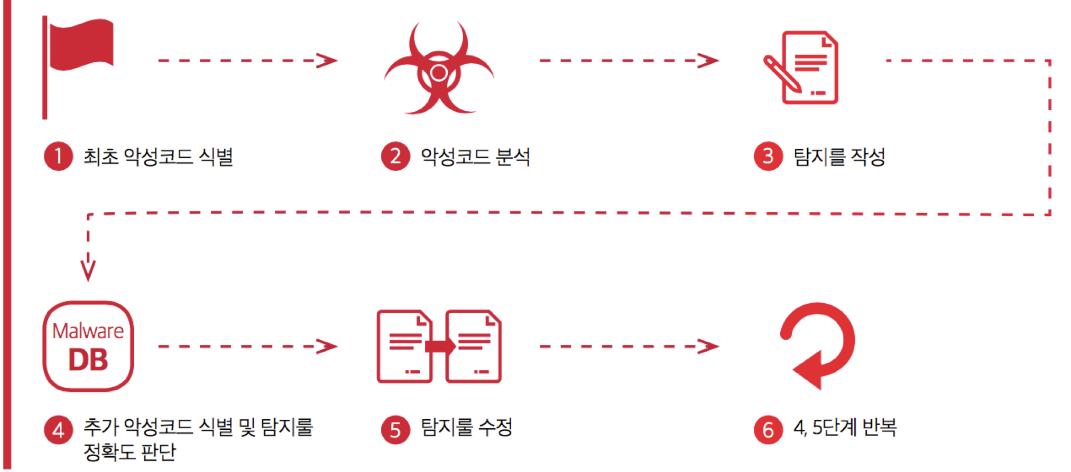


In order to identify such malicious codes, a method of extracting features of each malicious code and finding common points is used. Various techniques such as simple string extraction, API call count and sequence, and similarity calculation of partial hash are introduced. Recently, the concept of the cyber genome, which is a similar approach to the human genome project, has also appeared and is under study. In recent years, it is common to profile malicious code using YARA, a tool that supports binary and character pattern matching, along with classifications based on common malicious code features.

YARA analyzes the malicious code and generates a detection rule with a simple intrinsic grammar to find malicious code that conforms to the same detection policy. We can find similar malicious code using simple strings, specifying file offset, virtual memory address, regular expression, and entropy.

FSI perform malicious code-based profiling using the following procedure using YARA. 1) If the first malicious code is identified, 2) proceed to the detailed analysis and find the unique pattern of the malicious code and 3) create detection policies. Then, to determine the accuracy of the detection policies created and to identify similar malicious codes, 4) apply detection policies to malware databases and virus total intelligence services. Then, 5) after correcting the created detection policy 6) by repeating previous steps(step 4 and 5) it improves the accuracy of detection policies and continually finds similar malicious code.

♦  Malware profiling procedure



1. Identify the initial malware
2. Analyse malware
3. Creation detection rule
4. Additional malware identification and determine the accuracy of the detection rule
5. Amend detection rule
6. Repeat of the step 4 and 5

Meanwhile, there was a large scale port scanning activity on TCP port 3511 originated from the C&C server used by the malware that had used stolen code signing certificate from Company I. We also observed the INITROY C&C server sending the port scan attack on TCP port 3511 against dozens of financial companies in homeland. Afterwards, this port was confirmed to have been the vulnerable service port of the asset management solution by Company M hat was used to infiltrate into the target companies in Operation GHOSTRAT.

Thus, it is possible to analyze the association of a series of incidents based on the malicious code, the C&C server, and the vulnerability used by the attacker. In the case where the forensic image of the incidents was not secured, tFSI identified the campaign by mainly profiling the characteristics of the malicious code.

## B. Analysis of the operation

Malicious code profiling enabled us to track multiple operations (infiltration incidents), and in the course of analysing each operation, we found links between operations, such as using the same C&C server or vulnerabilities. Since the late 2015, we were able to confirm the involvement of Andariel in seven operations and the targets were financial service, Defense, IT solution developers in South Korea.

♦  Campaign Rifle Timeline

2013.03: DARKSEOUL

Destructive cyber terror against Broadcasting, Financial, ISP providers

2015.11: XEDA

Spear phishing against domestic/international Defense Industry

2016.02: INITROY

Infiltrated into the company "I" and stole the source code and code signing certificate

Related issue:

Malware used the stolen code sign certificate from "I company.

Malware used the application vulnerability in the DLP solution by company "N".

2016.05: GHOSTRAT

Stolen internal data from the domestic Telecommunication service, Defense related company. Used the customised well known RAT (GHOST RAT) and infiltrated by using the domestic security solution provider's solution vulnerability.

Relevant issue:

Malware disguised as DRM solution by the company "S" and used the solution vulnerability of the asset magagement solultion by the company "M"

2017.08: DESERTWOLF

Cyber terror aimed to steal the defense secrets. It used the Antivirus software's vulnerability and as a result the defense planning document was exfiltrated.

2016.09: BLACKSHEEP

Cyber terror related to Defense (detail is redacted)

2017.03: VANXATM

Ex-filtrate of the credit card information from ATM by hacking into the company "VAN". It used vulnerability in the Antivirus solution and the vulnerability in ATM update.

2017.05: MAYDAY

Attempted to infiltrate into the corporate network using the website where the specific company's employees often access by injecting the script that distributes malware through zero-day vulnerability.

### 1) DARKSEOUL

On the afternoon of March 20, 2013, a multifaceted network paralysis of major broadcasters, financial firms and ISP companies occurred simultaneously. It is reported that [about 48,000 systems](http://www.kisa.or.kr/uploadfile/201310/201310071957453995.pdf) have been damaged by this attack. The malicious code used in the attack destroyed the Master Boot Record and the Volume Boot Record, making the computer unbootable causing disturbance in public.

This attack is a case of APT that had been carefully prepared since at least 8 months before, with the following procedure.

(1)   [Foothold establishment in the internal network](http://concert.or.kr/issue/download.php?bo_table=qna&wr_id=4863&no=0): Attacker takes control of PC or server in target organization from at least 8 months before (June 28, 2012) and conducts continuous monitoring such as data theft and computer network vulnerability detection

(2)   Distribute malicious code: distributed malicious code at a specific point in time (2013.03.20 14:00) using Patch Management System (PMS) that manages PC software updates and operating system patches

(3)   Destruction of computing equipment: Damage of over 48,000 PCs, servers, ATMs in the network

##### DARKSEOUL TTP

|  |  |
| --- | --- |
| Tactics | System destruction (unable to boot due to MBR / VBR destruction) and irrecoverable |
| Techniques | Distribute malicious code at a specific point in time using PMS |
| Procedures | Establishing C&C server → Hacking of web server and distribution of malicious code using vulnerability → Malware infection of victim organisation internal PC → Collecting information of infected PC and distribution of additional malicious code for collecting information of the central server and database related port → Collecting central server and database related port information, and distributing additional malicious code for modifying update file of central management server → Modifying the PMS update file into a destructive malicious code → Distribute a destructive malicious code from PMS to victim computers |

DARKSEOUL is the cyber terror that caused the largest damage in the nation and is considered as the representative operation of the Lazarus Group. We have confirmed the recently discovered ANDARIEL’s transform modules were also used in DARKSEOUL operation, but the following attacks showed different malicious codes from the DARKSEOUL’s remote control & vulnerability attacking malware as well as presented different methods of attacks.

However, based on the fact that malicious codes with similar code patterns in DARKSEOUL are still found in overseas incidents, ANDARIEL is considered to be a group separated from Lazarus, and they appear to be using some of the existing modules developed by Lazarus in the past.

### 2) XEDA

In November 2015, there was a spear phishing attack targeting domestic and overseas defense industries participating in the Seoul International Aerospace & Defense Exhibition (ADEX). MS Office Excel document with malicious Macro embedded was attached to the email sent. Executing the macro by viewing the corresponding excel file resulted in malware infection.

The attached document in the email contained the content shared by a news media company who introduced the Seoul ADEX event. The method was to lure recipients to execute the attached file by disguising the email as a guiding message sent from the exhibition organizer. The excel file attached to the email was confirmed to contain a new type of backdoor at that time. When the malicious code is installed, it sends additional malware that can collect files and remotely control the victim. <http://www.etnews.com/20151123000356>

Content of the spear phishing

|  |
| --- |
| The ADEX 2015 joint operating headquarters in Seoul would like to advise you that we express our gratitude to all exhibitors who participated in ADEX 2015 held in Seoul from October 20 to 25.  Thanks to your active participation and encouragement, Seoul ADEX has been successfully held to its greatest success. Please find the attached list of participants of ADEX 2015 in Seoul for your reference. Thank you for your participation in this exhibition once again. If you do not see the image correctly due to the office version, you can set the macro function.  Thank you.  2015 Seoul Air Show results and visitor list.xls |

##### XEDA TTP

|  |  |
| --- | --- |
| Tactics | Gather information and gain control of attack target |
| Techniques | Send malicious code using MS Office macro function to spear phish |
| Procedures | Set attack target → Create social engineering e-mail and attachments → Create malicious code using macro function in Excel → Send e-mail |

Malicious code downloaded via macro contained the same "rifle" PDB string as the INITROY malicious code, and a very high similarity was observed in functions, registry usage, and file naming scheme. In addition, based on the fact that the malware distributing infrastructure for XEDA operation was used as C&C of INITROY operation, it is judged that it is executed by the same attacker.

### 3) INITROY

In February 2016, a case of malware distribution was confirmed to have used the stolen code signing certificate from the Company I. The investigation outcome of the Supreme Prosecutors' Office confirmed that the attacker compromised the demo server of Company I, then infected internal systems using a zero-day vulnerability in the DRM solution of Company N, then stole the [code signing certificate](http://www.spo.go.kr/_custom/spo/_common/board/download.jsp?attach_no=169641).

Code-signing

A program can be verified that it has not been tampered with in the distribution process, using a digital signature certificate proving that it was produced by a trusted company. In Windows environment, warning message is displayed during installation through validation of invalid digital signature.

The attack began in November 2015, and it is estimated that the code signing certificate was leaked between December 2015 and January 2016. In February 2016, the malicious code signed with this stolen code signing certificate was distributed resulting in 19 PCs from 10 organisations. The leaked certificate was discarded immediately and the vulnerability used for internal attack within the internal network of Company I was also patched.

##### INITROY TTP

|  |  |
| --- | --- |
| Tactics | Leakage of certificate (private key) and password for code signing  Product source code leak (estimated) |
| Techniques | Attack using zero-day vulnerability in DRM solution of Company N |
| Procedures | Computer server hacking → Installation of malicious code capable of steal internal data → Spreading  malware on employee PC → Ex-filtrating digital certificate that is stored in PC → Installing signed malware on a specific homepage operating server → Distributing the same malware to 10 organisation who accessed the homepage |

The distributed malware communicates with the C&C server and has the ability to steal information stored on the PC or install additional malicious code. As mentioned above, the PDB string of the malicious code was "rifle", and similarity with XEDA malicious code was confirmed.

### 4) GHOSTRAT

In May 2016, Cyber Security Bureau of National Police Agency confirmed that the large corporates internal confidential data were stolen by using Ghost RAT remote control malicious code as a result of computer network compromise and information leakage. (<http://www.police.go.kr/portal/bbs/view.do?nttId=18515&bbsId=B0000011&searchCnd=1&searchWrd=&section=&sdate=&edate=&useAt=&replyAt=&menuNo=200067&viewType=&delCode=0&option1=&option2=&option4=&option5=&deptId=&larCdOld=&midCdOld=&smCdOld=&pageUnit=100&pageIndex=2> ) The attack compromised two major corporate groups that were using the enterprise asset management solution by exploiting the vulnerability in file distribution and execution of the solution.

It was confirmed that the attacker had a long preparation time since July 2014, and even after establishing a foothold by gaining server and PC controls, it did not launch the immediate attack but concealed it while attempting to gain additional attack targets.

The attacker created a variety of malicious codes with functions such as remote control and monitoring, and gained controls over vulnerable servers such as SME, university research facilities and personal homepages and used them as malware C&C server.

##### GHOSTRAT TTP

|  |  |
| --- | --- |
| Tactics | Stealing data related to defense industry and telecommunication infrastructure |
| Techniques | Malicious code that exploits vulnerability of the asset management solution used by the target company  - Information of the pre-authorized vulnerable port for external access to PC - Exposed 'key (protocol) information' for operating the corresponding solution function |
| Procedures | Access through the legitimate path using vulnerability of the PC asset management system → Take over data by utilizing the normal file distribution & remote control function of the solution → Establish C&C server (SME, university research center, personal homepage, etc.) → Use of malware with remote control and monitoring capability |

##### GHOSTRAT OPERATION SUMMARY

We confirmed the trace of the large scale port scan activity from the INITROY operation C&C server against the vulnerable port of the asset management solution, and shared the same webshell with VANXATM and MAYDAY operation which we will discuss later on.

### 5) DESERTWOLF

In September 2016, it was acknowledged that the military data including wartime operational plans were leaked as a result of the malware infected computers including PC of the Minister of National Defense and PCs in the Internet connected network and internal network in the Ministry of Defense. The first confirmed penetration was August 2016 where the malware was distributed through PCs in the Internet connected network at the Ministry of Defense via hacked Antivirus relay server.

It was reported that the Antivirus solution provider was hacked in 2015 which the source code and the code signing certificate was stolen through the incident, and later the attacker used the zero-day vulnerability of the Antivirus solution. Internet connected network and internal network in the Ministry of Defense were meant to be two isolated networks however it was revealed that during the project of building central defense data centre server, for the operational convenience, the dual-homed server in both networks was set up which the attacker infiltrated the internal network through.

In addition, some of the IPs used in the attack are IP in Shenyang, China, and the similarity of the malicious codes used by known North Korean hackers attributed this attack to North Korea.

##### DESERTWOLF Operation Summary

(1)   North Korean hacker connect to Defense internal network through the Defense Internet connected network from IP address in Shenyang, China

(2)   Antivirus relay server at Ministry of Defense, Internet connected network and internal network were connected for 2 years, malware infected through Internet connected network

(3)   Leakage of military data from the internal network terminal

##### DESERTWOLF TTP

|  |  |
| --- | --- |
| Tactics | Military data leaked including wartime operational plans |
| Techniques | Distribution of malicious code through Antivirus relay server, total of 3,200 PCs  (2,500 PCs from internet connected network, 700 PCs from internal networks) |
| Procedures | Infiltrate into the Antivirus relay server → A large amount of malicious code penetrates into the Defense network → Ex-filtrated class 2 military secrets such as 'Operation Plan 5027' |

Although we have not officially confirmed the malware corresponding to the incident, we analysed the malware samples that are stringly believed to be related to the incident. The result is that the samples have same transform pattern and RAT malicious code pattern, and we also confirmed the malicious code used in keylogging was also used in the other operations. In addition, the zero-day vulnerability attack on the Antivirus server was also used in the subsequent VANXATM operation.

### 6) BLACKSHEEP

In August 2016, a distribution of malicious code was confirmed to be exploiting the update function of the web encryption solution by the Company I. In addition, from the same distribution server, the malicious code that exploits the vulnerability in DRM solution by Company N was also discovered. The two solutions relate to the INITROY operation that occurred in the early 2016, and this discovery backs the suspicion on the source code leakage through the INITROY operation. In addition to this, we also confirmed that the attack used [another zero-day vulnerability from the patched DRM solution by Company N](http://www.boannews.com/media/view.asp?idx=52522).

##### BLACKSHEEP TTP

|  |  |
| --- | --- |
| Tactics | Attacks against defense industry related companies (unable to confirm the damage) |
| Techniques | Malicious code that uses the update function of the ActiveX control in the web encryption solution by Company I (link to INITROY operation) |
| Procedures | (Suspect) source code and development documentation leakage during the INITORY operation → Analysis of the update procedure and verification method → Develop malicious code that passes the update verification procedure → Configure the distribution server with the update setting and logging → When accessed by the victim, automatically download malware |

### 7) VANXATM

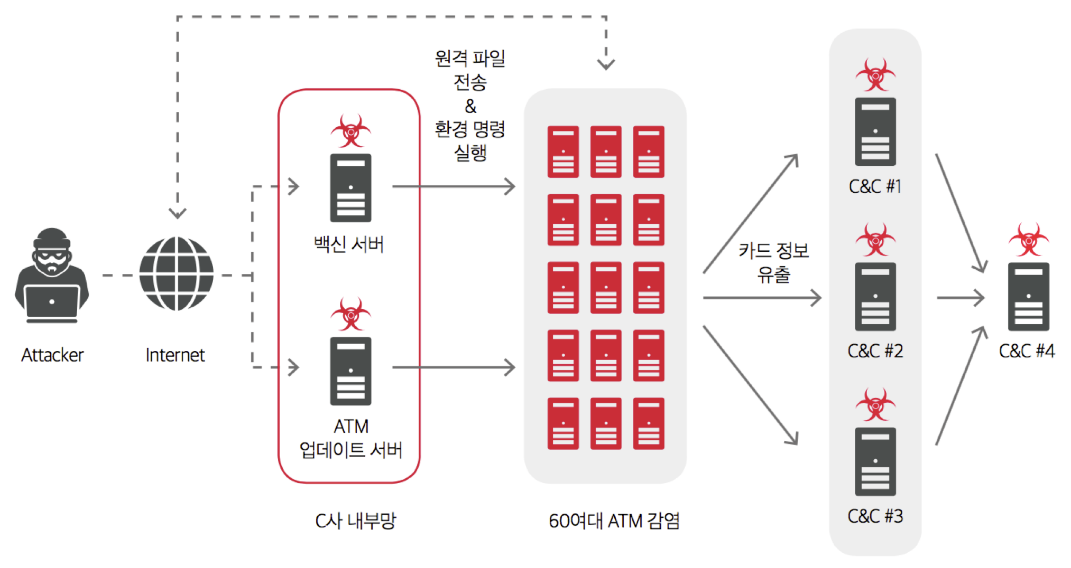
In March 2017, internal servers and ATM terminals were infected with malicious code through the compromise at the Company VAN, an electronic financial service third-party that provides CD operation and out-of-office ATM management services.

The attacker began a full scale attack in November 2016. Vulnerability in the Antivirus program was exploited to infect malicious code. It appears that the attacker created an account for the attack purpose who then remotely accessed and controlled, as well as obtained the administrator password that was stored in plaintext inside the Antivirus management server.

Using the remote managing function of the Antivirus management program, the attacker infected the ATM with malware (first round) and installed additional malware such as keylogger and backdoor.

Between February and March 2017, the attacker hacked into the update server and infected ATM with malicious code (second round). The attacker uploaded the malware into the hacked update server disguising as an update program. Due to the lack in the updated program validation, the disguised malware were downloaded and infected same model of ATM machines. As per the log from the infected ATM, it stored unnecessary information such as card number and valid period. We suspect the attacker have ex-filtrated this stored information from the second round of infection then sold at the dark web.

##### VANXATM Operation Flow



##### VANXATM TTP

|  |  |
| --- | --- |
| Tactics | Steal financial information and personal information from the ATM terminals |
| Techniques | Vulnerability of Antivirus Management Server to infect malicious code in ATM |
| Procedures | Attacks vulnerability of Antivirus Management Server → Gains VMS administrator privilege of the  Antvirus management server → Infects some ATMs with malware → Infects ATMs with additional malware and ex-filtrate stored information → Obtains privileged access to the update server → Upload malware disguised as update program → Infection of specific ATM model → Additional malware download → Ex-filtrate ATM operations log (including financial information) |

The same C&C server as the GHOSTRAT operation was used and attacks against the vulnerability of the Antivirus server used in the DESERTWOLF operation, the same key logger, and the RAT malware were found. In addition, there was an attempt to access the distribution server (using the ActiveX zero day vulnerability used) used in the BLACKSHEEP operation on the internal server, and the log was also confirmed to have downloaded a malware from the distribution server used in MAYDAY operation.

### 8) MAYDAY

In May 2017, a watering hole attack against employees of a financial company had occurred through the financial company’s union homepage. The attacker compromised the union homepage that was hosted externally through a web hosting service provider and distributed the malicious code using the zero-day vulnerability in the reporting solution by Company M. The distributed malicious code is the same type of malicious code as the other operations and all the web sites related to the incident confirmed so far appear to be using the same hosting company.

As the hosting company manages hundreds of union homepages including finance and public sector, it is suspected that it will affect not only finance but also other areas. At the same time, similar cases of distribution of malicious code using the same technique were confirmed in diplomatic and North Korea related sites, and the results of the analysis were released by the domestic security research group under the name of [GoldenAxe operation](https://www.wsj.com/articles/suspected-north-korean-hackers-try-tricky-new-tactic-1496142003).

##### MAYDAY TTP

|  |  |
| --- | --- |
| Tactics | Distributing malicious code to infiltrate internal networks |
| Techniques | Attempts to exploit malicious code targeting employees of certain organisations using ActiveX zero-day vulnerabilities |
| Procedures | Unions homepage hacking → Injection of malicious script and malicious code → Check if vulnerable ActiveX is installed when accessed by employees → Malicious code infection |

The attack on the homepages starts with uploading the webshell using the vulnerability of FCK editor, which is same as the webshell used in GHOSTRAT and VANXATM operations, also uses the same password.  
  
Some homepages only proceeded to the information gathering stage before distribution of malicious code, and only examined nine types of ActiveX controls on homepage user PC to see if they were installed. The distribution of malicious code using ActiveX vulnerability is one of various methods used by Andariel group including BLACKSHEEP operation to distribute malicious code. There is also a case where a new type of vulnerability was discovered again after the vulnerability was patched.  
  
We are unable to verify whether the attacker have vulnerabilities in all types of ActiveX program it examined of installation because we only have 1 type of ActiveX vulnerability attacking code so far.

The malicious code distributed using the vulnerability is a remote control malware that is a variation of the F.B.I. RAT whose source code is known to public. It is a remote control malware and a simple keylogger with the existing ANDARIEL code pattern.

## C. TTP Profiling

### 1) Tactics

The operations included in the rifle campaign are targeted at financial, IT, large corporations, defense industry, military, and other fields. However, the final goal is aimed at core infrastructures such as defense and finance.

Through detailed investigation on the target of the attack, the attacker performs thorough preparation such as understanding the IT infrastructure environment and personnel status of target organisation. With such information, the attacker finds and exploits the vulnerability or selects the name of the malware same as the known executable file of the software used by the victim organisation.

After the preliminary work is completed, after entering into the internal network, the attacker continuously infiltrates additional malware seeking key staff PCs and servers and attacking them. In the process, it collects and steals a large amount of internal information, analyzes the internal environment of the target in various angles, and ultimately carries out tasks such as ex-filtrating internal secrets and paralyzing work.

### 2) Techniques

The attacker used zero-day vulnerability in process of intrusion or internal propagation after the intrusion. In particular, the attacker exploited the vulnerability of ActiveX control solution which is widely used only in South Korea, and the zero-day vulnerability of enterprise software installed in many PCs in the form of agents. In order to find software vulnerabilities based on a great understanding of the operating environment of South Korean companies, IT companies may be selected as targets for exploiting vulnerabilities in related software.  
After successful penetration and getting the foothold established, it attacks internal network through reverse tunneling usually set from inside to outside. It is difficult to track the actual attacker's IP because of the use of VPN connections. However, there is often a case where the actual IP is exposed due to an error in the VPN software. It is common to install a RAT or backdoor developed by an attacker on the foothold system. In a Windows environment, it frequently uses an RDP connection after adding an account for attack (SQLAdmin, etc.).

##### Actual RDP access IP exposed through the VPN error

On the other hand, after securing the C&C server using WebShell or specific vulnerability, FTP program (FileZilla, etc.) is installed and data is taken from the infected PC. Then, the collected data is transferred to the secondary C&C, and the corresponding data is deleted from the primary C&C.

### 3) Procedures

Andariel group follow typical APT attack flow as they mainly conduct cyber terror. After initial penetration into the internal network, they thoroughly collect internal information and select useful information to ex-filtrate. However, in recent years, it has not been seen that the stage of the attack progressing into the level 5 “Destructive” due to the factors such as improved early detection capability and the change of agenda of the threat group, etc. But we can confirm they are continuously testing MBR destructive malware.

Attack Procedure

* Step 1: Information Gathering
* Collection of information about attack target (IP band, solution usage status, server type, internal employee status, etc.)
* Step 2: Infiltrate into internal network
* Infiltrate into the internal network using various vulnerabilities or social engineering techniques (spear phishing)
* Step 3: Gather internal information
* Infect malicious code for further attacks and communicate with C&C servers and identify information such as internal key assets
* Step 4: Data Theft
* Steal data including confidential internal documents and customer privacy and ex-filtrate to C&C server
* Step 5: Destruction (paralysis)
* Internal PC and server destruction

# 03. Malicious Code Profiling

## A. Rifle Transform

The Andariel group use their own special functions for specific string conversion (encoding / decoding). The following decoding functions were used in most attacks performed by Andariel with their naming modules corresponding to the characteristics of each function. The result decoded by each function can also be used as an input value of another decoding function. For example, a string decoded by an SUBS transform may be entered into an XOR transform to produce the final string.

### 1) XOR Transform

XOR transforms are used for both decoding and encoding using XOR operations. Encoded strings can be decoded and converted to plain text characters, and the infected PC information is encoded and transmitted to the C&C server.  
Characteristically, a total of four initial key values are used. The following is the result of converting the function to pseudo code using IDA.

XOR Transform: EE778BE503FDA770EE2F40E51EDFD595

The following is an XOR transform function ported to C language. The program can be used to encode / decode strings in malicious code.

XOR transformed functions ported to C language

In an operation occurred in the approximate point in time, the same XOR key value was reused. Therefore, the XOR key value is also the important profiling element. The list of XOR key values found so far is as follows (except 1 byte key value).

XOR transform key value per operation

Use of the same XOR key value (left : GHOSTRAT, right : DESERTWOLF)

Along with the unique XOR key value first appearing in each operation, the key value used in the previous operation was also reused. The following is an operation-to-operation relationship diagram based on the XOR key value used. Some GHOSTRAT key values were reused in VANXATM and DESERTWOLF, and DESERTWOLF-specific key values not used in GHOSTRAT were reused in VANXATM and BLACKSHEEP operations, respectively.

XOR key value association analysis by operation

### 2) FE Transform

The FE transform has a similar code pattern to the XOR transform, but there are some differences in bit operations.

FE Transform: E2982D47C354779415539BC305037427

From left, FE transforms found in GHOSTRAT, DESERTWOLF and MAYDAY

### 3) S Transform

S Transform: EE778BE503FDA770EE2F40E51EDFD595

S transform is used to extract a string excluding "S ^" from a string starting with "S ^" as shown below. As shown in the figure, the string following "S ^" is a WinAPI to be used in malicious code or other necessary strings (path for additional file to generate, additional malicious file name, etc.).

S Transform: EE778BE503FDA770EE2F40E51EDFD595

Looking at the S transform in Pseudocode, we get the remaining strings except the first two characters for the string starting with "S ^".

### 4) SUBS Transform

The SUBS transform uses the Substitution Table stored in it to replace it with a specific character, and then uses the Shift and OR operations to generate the final character string. The figure below shows the code part that passes the decoded string to the SUBS transform function.

Multiple Transform Invocations: 00F850A82B366A2E4E0C312D1D7A1266

The transferred string is converted to a primary decoded string through the SUBS transform function shown in the figure below, which is then passed to the XOR transform function and converted into the final plaintext string.

SUBS Transform: 00F850A82B366A2E4E0C312D1D7A1266

The SUBS transform function can be ported into Python to quickly decode encoded strings used in malware. In the code below, the subsTable is a character substitution table used by the function at the time of decoding, and is found in all malicious codes that use the SUBS transform, it can be used in gathering similar malicious codes.

SUBS transforms ported to Python

String substitution table

If we look at the operation of the SUBS transform function, the string that comes in as the initial input value (eg 978FF5eqF2YM0l + 4) is the inner coordinate of the decoded character substitution table (data type: WORD). The first character 9 is decimal 57 (0x39) and the data type of the substitution table is word (2 bytes), which means the 114th value in the above Python script substitution table. That is, 0x3D. Through this process, the final decoded character string is generated through the SAR, SHL, and OR operations several times using the value extracted from the substitution table. The final result is shown in the figure below, and if the value is entered into the XOR transform, the final plaintext gets generated.

SUBS Transform Operation Process

## B. RAT Server Module

### 1) Type A

RAT Server Type A Operation Screenshot

GUI-based RAT server module that allows file transfer and execution of commands against the infected agent. "Current path\log\agent.log", "Current path\log\{RAT Agent ID}.log" records the operation log and the result of command executed in the agent, respectively. RAT server Type A is connected by RAT client type A. In the server module, by default, system commands can be executed against the connected clients.

You can also transfer and run the files you want from the server to the client via the "upload" command.

Example log file

### 2) Type B

Client Type B is connected to RAT Server Type B, and unlike Type A, GUI interface is not supported. It reads the "conf.ini" file of the execution path and operates by giving commands to the agent. This is the method that desired commands are given and then the results of the command execution are sent back.

|  |
| --- |
| Admin] => Infected PC Identifier  USER = {command}    [Administrator]  USER = {command} |

## C. RAT Client Module

### 1) Type A

This is a client module connected with RAT server Type A. When infected, it transmits information to the server in the form of “computername\*\*\*\*\*username”

Generate infected PC information  
  
The agent uses mutex \* to prevent duplicate execution, and it copies itself in the startup program path so that the agent can operate even when the infected PC is rebooted.  
  
Creates mutex

If the agent operates normally, it tries to access port 443 with hard-coded C&C IP. It is presumed that the well-known 443 port is used instead of random port in the purpose of evade firewall. After executing the command that is received from the server, the result is sent to the server and stored as a file in the local temporary path.

\* Mutex (MUTual EXclusion): Object that is not shared among threads

Saving result after executing command

### 2) Type B

This is an agent connected with RAT server Type B. Like Type A, it connects to hard-coded C&C IP. Each agent is distinguished by "computername\_username".

Generating a RAT Client Identifier

The agent consists of 10 commands in the form of switch case and receives the command code remotely so that only the specified command is executed.

|  |  |
| --- | --- |
| Command | Function |
| ‘P’ (0x50) | Check the process list |
| ‘F’ (0x46) | Command execution |
| ‘G’ (0x47) | Check communication availability |
| ‘J’ (0x4A) | Write file |
| ‘H’ (0x48) | Library Loading |
| ‘I’ (0x49) | Library Unloading |
| ‘<’ (0x3C) | Check infected PC Drive Information |
| ‘=’ (0x3D) | Check File Retrieval |
| ‘B’ (0x42) | Process execution |
| ‘C’ (0x43) | Process execution |
| ‘D’ (0x44) | Search File |
| ‘E’ (0x45) | File Write |
| ‘>’ (0x3E) | File Contents Search Result Transfer |
| ‘@’ (0x40) | File Download |

### 3) Type C

Although the communication with the server cannot be analyzed in detail without having the server program of the RAT client Type C, some communication methods can be confirmed through the Type C code. The commands and functions received from the server are as follows.

|  |  |
| --- | --- |
| Command | Function |
| 0x8 | Create and execute additional malware |
| 0x1C | Sleep for certain time as commanded by the server |
| 0xA | Transmit specific file contents to the server |
| 0xF | Inject specific value into memory |
| 0xB | Create file |
| 0x1F | Execute file |
| 0x1E | Create file |
| 0x21 | Mark if infected |

C & C commands and functions

## D. Vulnerability exploit tool

A number of cases of vulnerability attacks against software used only in South Korea were identified during the initial attack on the target or the lateral attack after the infiltration. Some operations appear to have attacked software development company for the purpose of searching for vulnerabilities. In addition, after the vulnerability of a specific software is patched, another vulnerability is found to be used. This shows they are actively discovering and utilising software vulnerabilities.

The vulnerabilities used in the attacks are all patched at this time of writing and are not covered in detail here. The attacker creates a program to attack a vulnerability, exploits it remotely or directly after entering an internal network, and in case of ActiveX vulnerability, it compromises the distribution server then use it for a watering hole attack. Bluenoroff is known to use exploit kits mainly, but in the case of Andariel, it often uses vulnerabilities in ActiveX control or vulnerabilities in the enterprise security solutions (Antivirus, DRM, DLP, etc.) that are only used in South Korea .

### 1) Vulnerability exploit tool #1

It is a tool for attacking remote command execution vulnerability of Antivirus management server and agent. It has functions such as sending and receiving files and executing commands.

Antivirus vulnerability exploit tool

### 2) Vulnerability exploit tool #2

This is malicious code that exploits vulnerability in an asset management solution by Company M. It scans a server using vulnerable ports of the solution, selects an attack target, and performs a remote code execution attack using the corresponding tool.

Asset Management Solution Vulnerability Attack Tool

### 3) Vulnerability exploit tool #3

Below is part of the malicious script discovered in May 2017 that distributed Rifle family malware through vulnerability in the end-user and enterprise environment. In order to attack only certain corporate employees, Andariel is distributing malicious code using a watermarking technique as follows. The "$ prefix1" variable is set with IP belonging to specific company and it is set to prevent malicious actions when the user is coming from non-specified IP.

Attack targeted specific IP range

If a victim is an employee of specific organisation, malware is served through a zero-day vulnerability and executed.

ActiveX vulnerability exploit code

### 4) Vulnerability exploit tool #4

Vulnerability exploit tool #4 was found at a time close to when vulnerability exploit tool #3 was found. Below is a malicious script that identifies a total of nine ActiveX installations. It is difficult to confirm whether the vulnerability exists on those as the exploit codes were not found yet. The Financial Security Institute is close-monitoring of similar attacks that may occur in the future.

Identify whether a particular ActiveX control is installed

### 5) Vulnerability exploit tool #5

The following is a part of a script that distributed malicious code using the ActiveX vulnerability in November, 2016, and it is similar to the distributed malware code of vulnerability attack tool # 3. At the time, Andariel also used watering hole techniques to spread malicious code to attack only specific corporate employees.  
  
ActiveX vulnerability exploit code

## E. Known RAT

In addition to its own RAT, Andariel also modified the RAT program released on the Internet and used it to attack such as Aryan, Xtreme RAT, Ghost RAT, and F.B.I RAT. In addition, dozens of RAT source code downloaded by attackers are expected to continue to be used in future attacks. In the Ghost RAT, programs with Korean language expressions that are not used in South Korea such as “문자렬 (strings)" and “통보문현시(present notification)”.

Publicly available RAT source code downloaded by Andariel

Below is the RAT used by Andariel for actual attacks.

Xtreme RAT

Ghost RAT

Trochillus RAT

F.B.I RAT

## F. Keylogger

Keylogger captures the current time, window title, clipboard contents and keyboard keystroke events, then encrypts it through XOR transform, and records the collected contents to file. The log file name is hard-coded in encrypted form in the keylogger code as shown in the figure below, and the plain text file name can be obtained by decoding the binary data value (cipher text) generated after Base64 decoding using the SUBS transform. This log file is created under C:\Windows\System32 and stores the collected information.

Process of decrypting encrypted string

* Cypertext
* Base64 decoding
* SUBS transform
* Plaintext

String conversion outcome in each step

|  |  |
| --- | --- |
| 1 Cypertext | +pckL8P0F20agR24oMw= |
| 2 Base64 decoded | \ xfa \ x97$/ \ xc3 \ xf4 \ x17m \ x1a \ x81 \ x1d \ xb8 \ xa0 \ xcc |
| 3 Plaintext (using SUBS Transform) | FMSV123897.log |

The keylogger encrypts the key value entered by the victim using the XOR transform, and encodes the generated binary data value with the Base64 algorithm to generate the final cipher text.

Key-in value encryption process

* Collect keystroke values
* XOR Transform
* Base64 Encoding
* Cypertext

In order to decrypt the encrypted value stored in the log file into the plaintext, the process of generating the ciphertext is performed in reverse order. Deciphering the ciphertext with the Base64 algorithm and XOR transforming can be used to obtain the collected plaintext.

Below is the keylogger found in other operations and is made with relatively simple code. It saves the plaintext without encoding the captured keylog data.

Simple keylogger without encoding process

G. Webshell

Several types of WebShell programs were found in university labs and small/medium enterprise homepages that were used as C&C servers. Among these, "404 Not Found Shell V" web shell which disguised as 404 error page was also found in GHOSTRAT, VANXATM and MAYDAY operation. Webshells from these operations used same password.

Password input screen in 404 Not Found Shell

404 Not Found Shell

# 04 Association analysis

Based on the results of TTP and malicious code profiling, we can see the relationship between operations. As mentioned in some of the operations, the use of the same C&C server and the use of malicious code containing the same transforms have been confirmed, and based on these associations, we can determine these are the same actor’s campaign.

Commonly used in all operations, Andariel’s unique transform for string conversion is found. The comparison table for each operation's use of transform module is as follows.

Comparison table for using Transform module by operation

The same C&C server was used in different operations (INITROY-XEDA-GHOSTRAT, BLACKSHEEP-DESERTWOLF, GHOSTRAT-VANXATM). In the DESERTWOLF and VANXATM operations, the same keylogger program and XOR key were found in the same transform. In GHOSTRAT, VANXATM and MAYDAY operation, the same WebShell program with the same user password was found.

The C&C server used in INITROY operation was traced to have launched a large-scale port scan prior to attacking the asset management solution vulnerability used in the GHOSTRAT operation to select the target.

Among the vulnerabilities used in the attack, INITROY used the code signing certificate stolen from Company I and attacked the Company I using the vulnerability in Company N’s information leakage prevention solution. In BLACKSHEEP operation, exploits against another vulnerabilities in solutions of Company I and Company N were found in the same distribution server. In addition, a record of attempted access to the BLACKSHEEP distribution server was found from the compromised internal server of the VANXATM operation.

Campaign Rifle Relation Map

# 05 Recent Trends

In the past, the Andaleri group aimed primarily at cyber terrorism, such as stealing or destroying the key asset inside the target organisations, but recently it also actively engages in cyber crime activities for foreign currency earning, such as hacking an ATM to steal card information and then selling it at the underground market, or directly withdrawing money or making a payment and making malware that hack gambling programs.

## A. Gambling Program Hacking Malware

Recent detection on the malware that performs the hacking function of the online poker game suggests the Andariel group is  focusing on foreign currency earning by the looking at the.

Among the recent malicious codes observed, the sample initially uploaded at Virustotal with the file name of ProcessClean.exe uses XOR Transform and SUBS Transform. When executed, it appears as it installs a program called “Process Clean”, but in the background, it installs the malware that hack the online poker game.

Process Clean

The malicious code checks whether the specific game program is installed as follows. If it is installed, additional malicious code is generated and executed, and it is suspected that the malicious code performs the function of viewing the hand of the victim user.

Suspected online gambling program hack : 09A365BCA304D011E519978375EFE9B0

## B. Working with Bluenoroff and Code Update

Recently, it seems that Andariel and Bluenoroff group are cooperating in the attacks against South Korean financial institutes.

with domestic financial institutions. Until 2016, the Bluenoroff group did not carry out any special attack against the South Korea, but from 2017 attacks by Bluenoroff group are often discovered. It was also observed that Andariel and Bluenoroff carried out attack against the same corporate target. Lately, Bluenoroff has been utilising its own malicious codes that uses vulnerability in Hangul documents. These observation suggests two groups are currently focusing on attack targets in South Korea.

Also Andariel group has recently updated its unique character conversion function. Recent malicious codes believed to be belonging to Andariel group show XOR Transform with modified codes, and FSI are preparing the future attacks with the detection rules against the modified codes.

New Rifle Transform (found May 2017)

# 06 conclusion

News regarding the spread of malicious code and incidents are reported daily, and attackers are continuously attacking in various ways. APT groups like Andariel and Bluenoroff are continuing attacks to find unknown vulnerabilities or to establish the foothold,  bases and creating and testing malicious codes to infiltrate into corporations and government agencies to steal secrets.

The recent attacks are primarily aimed at economic gains, and the financial sector which is one of the key infrastructure that can cause chaos throughout the society at the time of an outbreak, is meant to be the target of all attack groups. Particularly the attacks of Andariel and Bluenoroff groups, which are the members of Lazarus group who are actively engaged in attacks including the financial sector at homeland and abroad, should be regarded as always in progress. Recent observation on the coopration of two groups in attack against the same financial institute and the various attack attempts monitored supports the fact they are continuously preparing and attempting the attacks on financial sector.

Although the financial sector are considered to be more difficult to attack than other sectors because of the tendency of the strong security controls, it is advised to thoroughly prepare from the basics.

It requires thorough security control management at the perimeter that connects internal network to Internet, such as Firewall access policy and response to the phishing emails. Also, it is necessary to continuously check the non-business web sites, which are frequently accessed by internal staff and can be exploited by watering hole attacks, so as to periodically eliminate security blind spots.

The Financial Security Institute track and analyse various threat groups including Andariel, Bluenoroff and Lazarus, and build database of the characteristic attack methods, malicious code patterns, and vulnerabilities used by each threat group.

We hope the past incidents and malicious code association analysis presented in this report based on the accumulated data would help security monitoring and control, predict the upcoming attacks, or assist efficient incident investigation. In addition, we expect it is possible to collaboratively respond to additional attacks through sharing information with financial institutions and related organizations.

Financial Security Institute will continue its efforts to prevent the spread of such damages and hopes that this report will be of great help in responding to financial threats.

# IOC

Malicious code hash

\* Please refer the [original document](http://www.fsec.or.kr/common/proc/fsec/bbs/21/fileDownLoad/1235.do) for the list of hashes.

Profiling threat groups targeting homeland  
  
Issued on July, 2017 Publisher: Heo Chang-Eon Publisher: Financial Security Institute

Site 132, Sujeong-ku, Yongin-si, Gyeonggi-do TEL: 02-3495-9000

The contents of this document are forbidden to be reproduced without the written consent of the Financial Services Authority. The information contained in this document is subject to change without notice.

* [Header](#FSI2017CyberThreatIntelligenceReport(En)
* [01. Summary](#FSI2017CyberThreatIntelligenceReport(En)
  + [A. Lazarus Group](#FSI2017CyberThreatIntelligenceReport(En)
  + [B. Bluenoroff Group](#FSI2017CyberThreatIntelligenceReport(En)
  + [C. Andariel Group](#FSI2017CyberThreatIntelligenceReport(En)
* [02.  Campaign Rifle](#FSI2017CyberThreatIntelligenceReport(En)
  + [A. Identification of the campaign](#FSI2017CyberThreatIntelligenceReport(En)
  + [B. Analysis of the operation](#FSI2017CyberThreatIntelligenceReport(En)
    - [1) DARKSEOUL](#FSI2017CyberThreatIntelligenceReport(En)
      * [DARKSEOUL TTP](#FSI2017CyberThreatIntelligenceReport(En)
    - [2) XEDA](#FSI2017CyberThreatIntelligenceReport(En)
      * [XEDA TTP](#FSI2017CyberThreatIntelligenceReport(En)
    - [3) INITROY](#FSI2017CyberThreatIntelligenceReport(En)
      * [INITROY TTP](#FSI2017CyberThreatIntelligenceReport(En)
    - [4) GHOSTRAT](#FSI2017CyberThreatIntelligenceReport(En)
      * [GHOSTRAT TTP](#FSI2017CyberThreatIntelligenceReport(En)
      * [GHOSTRAT OPERATION SUMMARY](#FSI2017CyberThreatIntelligenceReport(En)
    - [5) DESERTWOLF](#FSI2017CyberThreatIntelligenceReport(En)
      * [DESERTWOLF Operation Summary](#FSI2017CyberThreatIntelligenceReport(En)
      * [DESERTWOLF TTP](#FSI2017CyberThreatIntelligenceReport(En)
    - [6) BLACKSHEEP](#FSI2017CyberThreatIntelligenceReport(En)
      * [BLACKSHEEP TTP](#FSI2017CyberThreatIntelligenceReport(En)
    - [7) VANXATM](#FSI2017CyberThreatIntelligenceReport(En)
      * [VANXATM Operation Flow](#FSI2017CyberThreatIntelligenceReport(En)
      * [VANXATM TTP](#FSI2017CyberThreatIntelligenceReport(En)
    - [8) MAYDAY](#FSI2017CyberThreatIntelligenceReport(En)
      * [MAYDAY TTP](#FSI2017CyberThreatIntelligenceReport(En)
  + [C. TTP Profiling](#FSI2017CyberThreatIntelligenceReport(En)
    - [1) Tactics](#FSI2017CyberThreatIntelligenceReport(En)
    - [2) Techniques](#FSI2017CyberThreatIntelligenceReport(En)
      * [Actual RDP access IP exposed through the VPN error](#FSI2017CyberThreatIntelligenceReport(En)
    - [3) Procedures](#FSI2017CyberThreatIntelligenceReport(En)
* [03. Malicious Code Profiling](#FSI2017CyberThreatIntelligenceReport(En)
  + [A. Rifle Transform](#FSI2017CyberThreatIntelligenceReport(En)
    - [1) XOR Transform](#FSI2017CyberThreatIntelligenceReport(En)
    - [2) FE Transform](#FSI2017CyberThreatIntelligenceReport(En)
    - [3) S Transform](#FSI2017CyberThreatIntelligenceReport(En)
    - [4) SUBS Transform](#FSI2017CyberThreatIntelligenceReport(En)
  + [B. RAT Server Module](#FSI2017CyberThreatIntelligenceReport(En)
    - [1) Type A](#FSI2017CyberThreatIntelligenceReport(En)
    - [2) Type B](#FSI2017CyberThreatIntelligenceReport(En)
  + [C. RAT Client Module](#FSI2017CyberThreatIntelligenceReport(En)
    - [1) Type A](#FSI2017CyberThreatIntelligenceReport(En)
    - [2) Type B](#FSI2017CyberThreatIntelligenceReport(En)
    - [3) Type C](#FSI2017CyberThreatIntelligenceReport(En)
  + [D. Vulnerability exploit tool](#FSI2017CyberThreatIntelligenceReport(En)
    - [1) Vulnerability exploit tool #1](#FSI2017CyberThreatIntelligenceReport(En)
    - [2) Vulnerability exploit tool #2](#FSI2017CyberThreatIntelligenceReport(En)
    - [3) Vulnerability exploit tool #3](#FSI2017CyberThreatIntelligenceReport(En)
    - [4) Vulnerability exploit tool #4](#FSI2017CyberThreatIntelligenceReport(En)
    - [5) Vulnerability exploit tool #5](#FSI2017CyberThreatIntelligenceReport(En)
  + [E. Known RAT](#FSI2017CyberThreatIntelligenceReport(En)
  + [F. Keylogger](#FSI2017CyberThreatIntelligenceReport(En)
* [04 Association analysis](#FSI2017CyberThreatIntelligenceReport(En)
* [05 Recent Trends](#FSI2017CyberThreatIntelligenceReport(En)
  + [A. Gambling Program Hacking Malware](#FSI2017CyberThreatIntelligenceReport(En)
  + [B. Working with Bluenoroff and Code Update](#FSI2017CyberThreatIntelligenceReport(En)
* [06 conclusion](#FSI2017CyberThreatIntelligenceReport(En)
* [IOC](#FSI2017CyberThreatIntelligenceReport(En)
  + [Reports to integrate](#FSI2017CyberThreatIntelligenceReport(En)

## Reports to integrate

* .