30.05.2017

LAZARUS ARISEN

ARCHITECTURE / TOOLS / ATTRIBUTION

Group-IB reveals the unknown details of attacks from one of the most notorious APT groups: sophisticated espionage and APT techniques of the North Korean state-sponsored hackers

The North Korean hacker group named Lazarus has spied on the ideological enemies of the regime – state institutions and private corporations in the United States and South Korea – for years. Now Lazarus attacks banks and financial institutions around the world. Investigating not only the malicious code, but also the complex three-layer infrastructure of Lazarus, their encrypted channels and obfuscation tools, Group-IB reveals the previously unknown details of cyberattacks from one of the most notorious APT groups.

Download the full report >>>

There are two points of interest in the Potonggang district of Pyongyang – the National Defence Commission of the Democratic People's Republic of Korea (NDC) and the unfinished 105-storey Ryugyong Hotel. Both facilities are restricted for foreigners. The IPs identified in Group-IB's investigation refer to this area, we are unaware of other organisations or locations of interest and given the closed nature of the North Korean state cannot attribute further.

The Lazarus (aka DarkSeoul group) is allegedly controlled by Bureau 121, a division of th Reconnaissance General Bureau, a North Korean intelligence agency. Bureau 121 is responsible for conducting military cyber campaigns.

Lazarus is known to have specialized in DDoS attacks and corporate breaches targeting government, military, and aerospace institutions worldwide. Now that global economic pressure on North Korea has increased, Lazarus has shifted their focus to international financial organizations to conduct money thefts and espionage.

The most large-scale attack happened in February 2016, when hackers tried to steal about $1bln from the Central Bank of Bangladesh through SWIFT. Due to a mistake in the payment document, the attackers managed to steal only $81 million. In March 2017, FBI and NSA officials publicly confirmed for the first time that Pyongyang was likely behind the attack on the Bangladeshi Central Bank. Following this, new sanctions were immediately imposed on North Korea — local banks were disconnected from the SWIFT system.

In February 2017, several Polish banks were compromised.

Security researchers analysed the malware code, chiefly using this to attribute activity to Lazarus group. As tools are often reused by different groups, while helpful, malware analysis does not provide conclusive evidence of attribution.

Evolution of Lazarus

The major operations of the North Korean hacker group from 2009 to 2016

1

Troy operation

Period: 2009-2012
Target: cyber espionage agaist armed forces and governmental bodies of South Korea, sabotage.
Method: hacking websites, stealing information, DDoS-attacks.

2

DarkSeoul operation

Period: March 2013
Target: three broadcasting stations, a bank in South Korea.
Method: infecting with viruses, stealing and wiping information.

3

Attack on Sony Pictures

Period: November 2014
Target: Sony Pictures Entertainment (released the "Interview" movie, ridiculing the North Korean leader).
Method: infecting with malware, stealing and wiping data of the

4

Attack on the Centra Bank of Bangladesh

Period: 2016 year
Target: an attempt to steal $9
from the Central Bank of Bangl
Managed to steal only $81 milli
Method: a targeted attack on

company's employees, correspondence, copies of unreleased films.

system of interbank transfers S

Group-IB specialists have researched this group and now have evidence which identifies that North Korea is behind these attacks: We have detected and thoroughly analyzed multiple layers of C&C infrastructure used by Lazarus and have identified North Korean IP addresses from which the attacks were ultimately controlled. The following report is an outline of the criminal group's attack methodology for financial institutions, the malware employed and an overview of who they have planned to attack.

Through investigation of attacks on banks, we have proved that there is a strong connection between Lazarus and North Korea, while the analysis of IP addresses enables us to locate the attackers. We have detected and thoroughly analyzed the C&C infrastructure used by Lazarus. Our research shows how hackers gained access to the banks' information systems, what malware they used, and who their attempts were aimed at.

Dmitry Volkov
Head of Threat Intelligence Department, Co-founder Group-IB

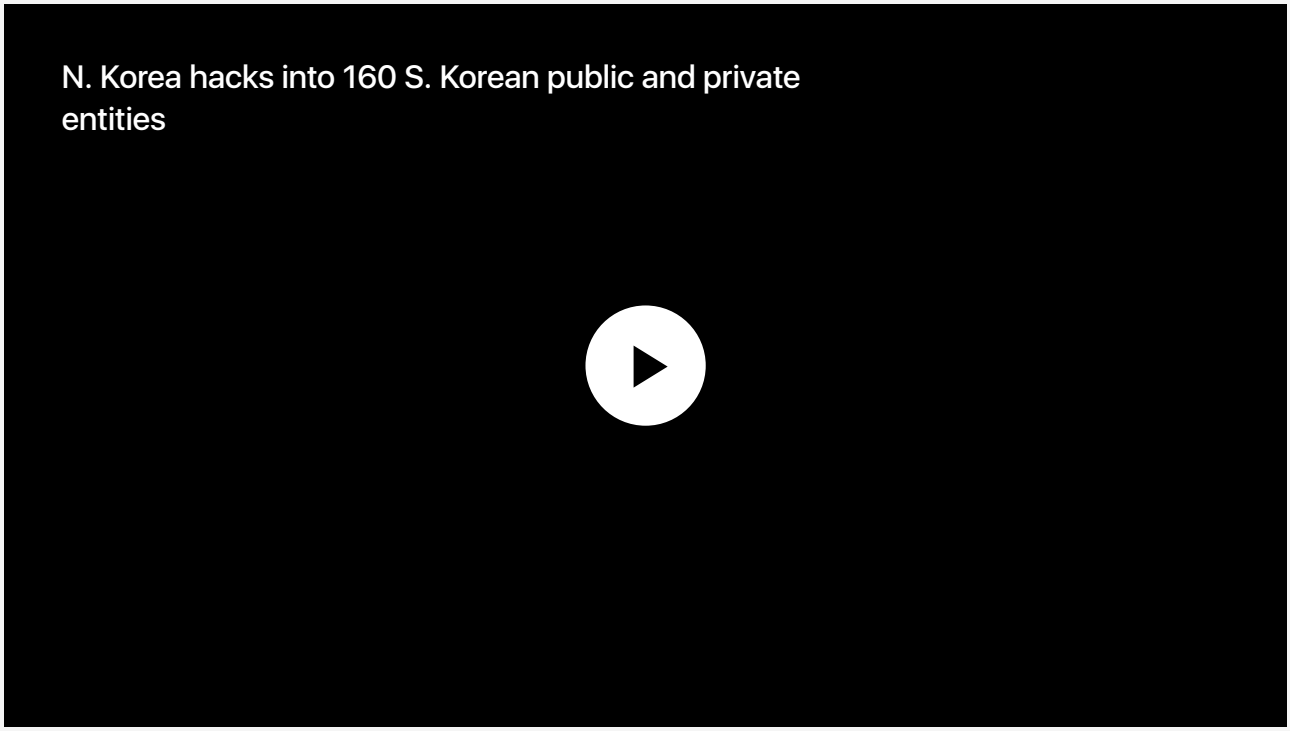
Attack Organizers: Involvement of North Korea

Due to analysis of Lazarus infrastructure, Group-IB specialists have detected that the attack was controlled from two IP addresses:

- 210.52.109.22 belongs to an autonomous system China Netcom. However, some sources indicate that the set of IPs 210.52.109.0/24 is assigned to North Korea.

- 175.45.178.222 refers to a North Korean Internet service provider. The Whois service indicates that this address is allocated to the Potonggang District, perhaps coincidentally, where Natinal Defence Commission is located — the highest military body in North Korea.

Through investigation of public information, we came across a TV report from a South Korean news agency Arirang News dated 2016.



In February 2016, the report said, North Korean hackers attacked two corporations:

1. SK Group is one of the largest conglomerates in South Korea.
2. The plot referred to the attack of North Korean hackers in February 2016 on two corporations: SK Group is one of the largest conglomerates in South Korea. Hanjin Group is the head company of Korean Airlines, its division produces under license combat helicopters and fighter jets.

On the screen behind the host, Group-IB specialists noticed two IP addresses 175.45.178.19 and 175.45.178.97, which had been used to control Ghost RAT malware. Both IP addresses are in the same set of IP addresses as an IP address 175.45.178.222 that was discovered by Group-IB specialists.

The South Korea's National Police Agency reportedly identified that the cyber- attack had been performed from the unfinished North Korean Ryugyong hotel. Group-IB could not confirm this location attribution.

Masquerading as Russian hackers

Starting in 2016, the Lazarus group tried to mask their activity by pretending to be Russian hackers:

- The Client_TrafficForwarder module includes debugging symbols and strings containing Russian words in descriptions of commands received by malware from the C&C server.

  It's worth noting that "Russian commands" received from the server are not typical for a Russian native speaker, and in the case of the «poluchit» (to receive) command the meaning of the word contradicts the action (to send) it is intended for.

Poluchit	Отправить на C&C сетевой адрес текущего сервера

- To protect their executables, hackers used Enigma Protector, a commercial product, which was created by a Russian software developer.

- Exploits for Flash and SilverLight were borrowed from the sets of exploits created by Russian-speaking hackers.

These masquerade techniques did originally mislead some researchers who conducted malware operational analysis.

KEY FINDINGS

Lazarus Infrastructure

Through analysis of Lazarus activity, Group-IB gained deep insight on a complex botnet infrastructure built by the hacker group to conduct their attacks. To mask malicious activity, the hackers used a three-layer architecture of compromised servers with SSL-encrypted channels established between them. In addition to encrypted traffic, data sent through SSL-channel was additionally encrypted. The attackers achieved anonymity by employing a

legitimate VPN client - SoftEther VPN. In some cases, they also used corporate web servers that were part of the attacked infrastructure.

Unique tools

To control infected machines, the hackers employed multi-module tools, attempting to complicate malware analysis. That said, they managed to conduct several successful attacks without employing 0-day exploits. Lazarus demonstrated a flexible approach to attacks by applying different hacking tools, which prevented their detection by endpoint security solutions.

Victims

The earliest indicator of attacks on financial institutions compromise detected by Group-IB is dated March 2016. This was directly after the Central Bank of Bangladesh incidet, which took place in February 2016, where attackers attempted to steal $1 billion USD. Only a spelling mistake in an online bank transfer instruction helped prevent them from stealing more than $81 million USD. Following this incident, the group modified its tactics and tools, adapting them to the changing environment and misleading researchers.

Through analysis of compromised networks, Group-IB identified IP addresses of universities in the US, Canada, Great Britain, India, Bulgaria, Poland, Turkey, pharmaceutical companies in Japan and China, as well as government subnets in various countries.

Emerging trend

A state-sponsored hacker group Lazarus managed to gain fraudulent access to the SWIFT network of attacked banks. This is believed to be a growing trend: state-sponsored hackers are demonstrating an increased interest in conducting attacks on financial institutions, which are considered a component of the national critical infrastructure in some countries. At the moment, only a few similar incidents have been detected. For example, in 2010-2013 the NSA reportedly penetrated the SWIFT banking network and monitored a number of Middle East banks. In late 2016, attacks on Ukrainian banks were conducted, allegedly as part of the BlackEnergy operation. However, researchers expect that the number of attacks on financial institutions by state-backed hackers may significantly increase in the future.

ATTACK PREPARATION AND IMPLEMENTATION

To conduct attacks, the criminals developed toolsets to control C&C servers and infected machines, built a three-layer C&C infrastructure, and compromised dozens of large web resources. A detailed technical analysis of the infrastructure is in the chapter "Preparing and conducting an attack" in the full version of the report.

1 Infection of web resources

To infiltrate systems of their interest, Lazarus conducted watering-hole attacks leveraging compromised resources often visited by their potential victims, such as websites of financial regulators and government agencies in several countries.

Some of these resources are listed below:

- **knf.gov.pl** — The Polish Financial Supervision Authority
- **cnvb.gob.mx** — National Banking and Securities Commission, Mexico
- **brou.com.uy** — Banco de la República Oriental del Uruguay, a state-owned bank in Uruguay

Through examination of a code on a web server with exploits, Group-IB specialists detected a list of 255 IP address ranges. That said, hackers infected only those users who visited the website from a computer within the specified IP range. Based on this list, researchers have compiled a map of the countries that were of interest to the attackers, which is presented below.

Based on this
researchers ha
compiled a ma
countries that
interest to the
attackers, whi
presented bel

2

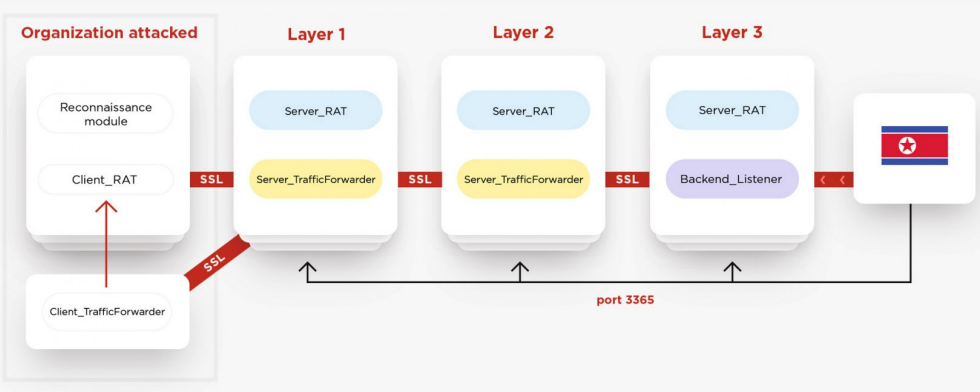
Establishment of C&C infrastructure:

Attackers created a 3-tier infrastructure that consisted of compromised servers, between which the hackers established SSL-encrypted channels. The network interaction with the attacked computer was carried out only from the Layer 1 server, which acted as a C&C server. In some cases, hackers placed the Layer 1 server inside the organization attacked in order to reduce the risk of detection. They gained access to these servers by brute forcing password for RDP.

3 Hackers used original set of tools

After trying to steal $ 1 billion from the Central Bank of Bangladesh in February 2016, hackers from Lazarus promptly changed their tactics and modified their unique set of tools.

Server_RAT	Used to manage windows-based server infrastructure
Server_Traffic Forwarder	Forwards traffic from one external server to another
Backend_ Listener	Establishes connection with servers with installed Server_RAT, gets commands directly from threat actor
Admin_Tool	Admin tool to send commands to infected computers
SWIFT toolbox	Used to work with SWIFT, consists of Alliance software Hook Files and SWIFT transactions Information Harvester



Through in-de
analysis of the
used by the at
Group-IB spec
identified the s
of communica
between node
the C&C infras

Server_RAT

Server_RAT was installed on all infrastructure levels to control the compromised infrastructure Server_RAT constantly listens on port 3365, to which attackers connected to control the server. To ensure the availability of the specified port, the malicious program added a special rule to the firewall that allowed incoming connections to this port. Infected computers performed an outgoing connection to the compromised server acting as proxy via port 443, which is usually open in corporate networks.

Based on analysis of the Server_RAT functionality, Group-IB specialists identified that Server_RAT responds to certain requests in a specific way. Keeping in mind that Server_RAT constantly keeps port 3365 open, we scanned the Internet for open ports 3365. Following this, we checked a list of detected servers to identify those servers where Server_RAT was installed. As a result, Group-IB specialists received a list of 74 IP addresses.

Server_TrafficForwarder

Server_TrafficForwarder was installed on the first and second server level — this module redirected traffic from one server to another.
In some cases, Server_TrafficForwarder was installed on servers inside the attacked organization. This approach allows the criminal to avoid detection of suspicious connections to the external network or bypass network connection restrictions with prohibited connections to the external network from specific computers/servers, which is often applied by companies to protect the most critical PCs, such as those of SWIFT operators.

After the start, Server_TrafficForwarder reads the contents of the key and certificate files from the root directory that will be used to create an SSL tunnel. That said, the file does not contain any information about the servers to which traffic should be transferred. At the first start, hackers manually specify the port to listen on as well as the address of the C&C server to which traffic is to be sent. In the event the port is not specified, the program listens on a random port and waits for incoming connections.

To verify communication with a compromised server, hackers check if the client is appropriate: they send the first network request; when a response is received from the client, they decrypt it and compare with a previously known response. In the event the responses are different, the connection is broken.

Backend_Listener

Backend_Listener is software installed by attackers on Layer 3 servers. The program performs communications with other servers, receives commands from the administrator and sends them in chain order to the end infected computer.
Backend_Listener listens on the two ports:

- port 8080, to which it accepts SSL connections from Layer 2 servers.
- port 9090, to which it receives requests from the control system, which Group-IB dubbed Admin_Tool.

To encrypt traffic, the wolfSSL open source library is used. After the application is launched, the private key and certificate files are loaded from the root directory. These files are used to encrypt traffic between the C&C server and connected clients.

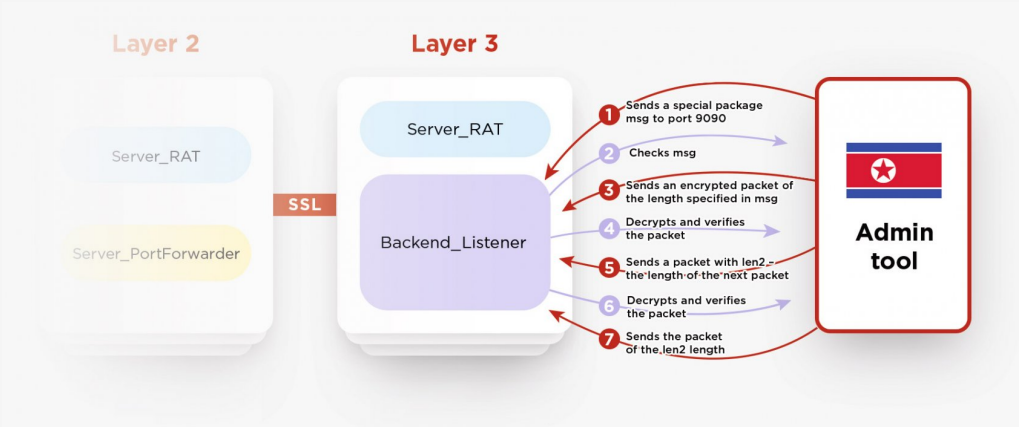
To defend against security solutions designed to "unpack" SSL encrypted traffic, Backend_Listener encrypts all data sent over an SSL channel using an additional reversible encryption algorithm and performs legitimacy tests.

To reverse-engineer the protocol of server communications with clients, Group-IB specialists have developed a client that successfully connects to both above-mentioned ports.

VPN

VPN: the attackers installed SoftEther VPN (http://softether.net/) service supported by University of Tsukuba, Japan on some servers to unsure additional level of anonymity. Lazarus have chosen this service for the following reasons:

- This legitimate application isn't detected by security solutions
- It establishes VPN connection via ICMP or DNS to avoid detection by network security solutions
- It contains Dynamic DNS function, which means that if a compromised system has a dynamic IP address, the attacker can always find it by DNS name connected to the VPN client
- This VPN client supports Windows, Linux, FreeBSD, Solaris, Mac OS X



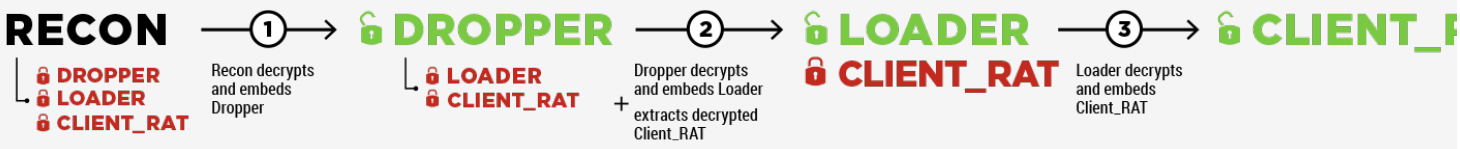
Tools to control infected PCs

In addition to multi-layer server structure, hackers developed a specialized toolset to perform remote control over infected PCs.

The group actively attempted to conceal their activity, complicating malware detection and analysis as much as possible. All tools consist of modules, which were delivered separately to target organizations only. To complicate malware investigation, criminals encrypted their tools.

Modular architecture of the victim's infection process provides both additional flexibility and anonymity throughout the cyber-attack. This scheme allows hackers to divide software development activity between teams, as well as to ensure the reuse of program code.

Recon	Recon is a backdoor that is initially installed on the target machine through successful execution of exploits. This module is used by hackers to perform initial reconnaissance to search for systems of interest.
Dropper	Dropper extracts and decrypts Loader, embeds it into the system and extracts Client_RAT.
Loader	Loader is used to decrypt the payload — Client_RAT or Client_ TrafficForwarder — and inject it into the legitimate process (for example, in lsass.exe).
Client_Traffic Forwarder	This module was installed on one of the PCs in the internal network of the attacked organization. It proxies traffic from C&C server to PCs in the local network of the attacked organization.
Client_RAT	The Client_RAT program provides full control over the target system: it allows you to analyze the system, download and execute files, transfer data from the infected computer to the C&C server.



RECOMMENDATIONS

Taking into consideration strengthening economic sanctions against North Korea, as well as the geopolitical tension in the region, we expect new wave of Lazarus attacks against global financial institutions. With that said, we strongly recommend the banks to learn more about targeted attacks' tactics and techniques, increase corporate cybersecurity awareness, and cooperate with the companies providing relevant Threat Intelligence.

Dmitry Volkov
Head of Threat Intelligence Department Co-founder Group-IB

1

Updates of software and operating systems

To prevent infection through execution of exploits, it is enough to update your Microsoft and Adobe software.The Lazarus group uses known and patched exploits, rather than leveraging 0day vulnerabilities. That's why, even usual software updates did not allow attackers to infiltrate corporate networks. Unfortunately, some of the attacked banks did not comply with this requirement.

2

Network traffic analysis

Even if the criminals have managed to obtain access to the corporate network, the attack can still be successfully prevented. After intrusion into the company's network hackers still need to find systems of their interest, and gain access to them. It takes days and even months sometimes, and this time should be used to detect the malicious activity.

Attackers use malicious programs that transfer data to the C&C server - Layer 1. Communications between the infected computer and the C&C server can be identified through network traffic analysis. All communications are encrypted, that is why you should use solutions that can detect network anomalies based on threat intelligence data.

3

Application whitelisting

Application whitelisting should be introduced into critical bank servers. This will prevent attackers from installing their remote control tools, monitoring financial transactions, and escalating privileges. It also helps to identify unauthorized attempts to run such malicious applications.

4

Checking indicators of compromise

The "Indicators of compromise" section contains current and historical intelligence data. With these indicators, you can check if your organization was, or is, under attack by Lazarus. The group uses legitimate compromised servers, that's why these indicators can give false positives. You will find a list of indicators in the full version of the report.

5

Professional response

And the most important thing: if you have detected trails of a targeted attack at any stage, you need to involve specialized companies for its analysis. Incorrect responses to the attack result in the attacker activity remaining partly undetected to enable criminals to achieve their goal — to steal money.

Full report

Download

ABOUT GROUP-IB

Group-IB is one of the global leaders in preventing and investigating high-tech crimes and online fraud. Since 2003, the company has been active in the field of computer forensics and information security, protecting the largest international companies against financial losses and reputational risks.

International honors

The company is recognized by Gartner as a threat intelligence vendor with strong cyber

security focus and the ability to provide leading insight to the Eastern European region and recommended by the Organization for Security and Co-operation in Europe (OSCE). In 2017 IDC Report named Group-IB the leader of the Russian Threat Intelligence Services Market. The company is a member of the World Economic Forum working group on cybersecurity.

Clients worldwide

Fortune 500 companies worldwide use Group-IB products and services. Group-IB clients include top-tier banks and financial institutions, FMCG brands and industrial corporations, oil and gas companies, software and hardware vendors, telecommunications service providers the US, Western Europe, the Middle East, Asia and Australia.

CyberCrimeCon2017

Annual conference organized by Group-IB aims to empower global threat intelligence exchange in one of the hottest spot on cybersecurity map. Be the first to discover key cybercrime trends and get a chance to interact with the global experts directly, both on and off stage. Learn more on 2017.group-ib.com

Receive insights on the latest cybercrime trends

originating from Russia and Emerging Markets

Email

SUBSCRIBE

Moscow
+7 495 98
info@grou

New York
+1 917 809
help@grou