Lazarus APT Group (APT38) - Brandefense

Published: 2022-08-15 · Archived: 2026-04-05 17:55:32 UTC

> **Download IoC, YARA and SIGMA Rules**

This post analyzes Lazarus APT group findings that can be used by people who work in the information technology departments, part of the cyber security team, or have gained competence in areas such as security researchers and system administrators. The following topics are included and shared:

- Group's Mission and Vision
- Group's Country of Origin and Known Aliases
- Targeted Countries and Industries
- Activities/Operations/Cyber Attacks by Year (Historical Background)
- Cyber Attack Lifecycles and MITRE ATT&CK TTPs
- Group's Toolset and Related Malware
- Indicator of Compromises
- YARA and Sigma Rules
- Recommendations/Mitigations

Group's Mission and Vision

In general, the motivations of apt groups are mostly based on ideological reasons, and they are state-supported.

The Lazarus Group has strong links to North Korea. The United States Federal Bureau of Investigation says that the Lazarus Group is a North Korean "state-sponsored hacking organization".

The known main goals of this group :

- Extortion of Money
- Information Theft
- Sabotage
- Espionage

Group's Country of Origin and Known Aliases (Names)

Lazarus Group is one of the most sophisticated North Korean APTs that has been active since 2009.

Also known by other monikers such as **Guardians of Peace** or **Whois Team**. The names **HIDDEN** and **COBRA** are generally used by the United States intelligence community to refer to the malicious cyber activities of the North Korean government. Also, the name Zinc is used by Microsoft.

Lazarus's Aliases:

- Andariel,

- Appleworm,
- APT-C-26,
- APT38,
- Bluenoroff,
- Bureau 121,
- COVELLITE,
- Dark Seoul,
- GOP,
- Group 77,
- Guardian of Peace,
- Hastati Group,
- HIDDEN COBRA,
- Labyrinth
- Chollima,
- Lazarus,
- NewRomantic Cyber Army Team,
- NICKEL ACADEMY,
- Operation AppleJesus,
- Operation DarkSeoul,
- Operation GhostSecret,
- Operation Troy,
- Silent Chollima,
- Subgroup: Andariel,
- Subgroup: Bluenoroff,
- Unit 121,
- Whois Hacking Team,
- WHOis Team,
- ZINC

Targeted Countries and Industries

The Lazarus APT Group targets;

- Banks,
- Defense Industries,
- Software Business,
- Pharmaceutical Companies,
- Cryptocurrency Platforms,
- Manufacturing and,
- Electrical Industries.

Malware known to belong to this group has been spotted in 18 countries worldwide. The list of the countries are below;

- Brazil
- China,
- India,
- Indonesia,
- Iran,
- Iraq,
- Malaysia,
- Mexico,
- Poland,
- Russia,
- Saudi Arabia,
- South Korea,
- Taiwan,
- Thailand,
- Turkey,
- USA,
- Vietnam.

Operations by Year (Historic Background)

North Korean group definitions are known to have significant overlap and some security researchers report all North Korean state-sponsored cyber activity under the name Lazarus Group instead of tracking clusters or subgroups.

2009 – Operation Troy

This attack utilized the Mydoom and Dozer malware to launch a large-scale, but quite unsophisticated, DDoS attack against US and South Korean websites. The volley of attacks struck about three dozen websites and placed the text “Memory of Independence Day” in the master boot record (MBR).

2014 – Sony Breach

The Lazarus Group attacks culminated on November 24, 2014. On that day, a Reddit post appeared stating that Sony Pictures had been hacked via unknown means; the perpetrators identified themselves as the “Guardians of Peace.” Large amounts of data were stolen and slowly leaked in the days following the attack. An interview with someone claiming to be part of the group stated that they had been stealing Sony’s data for over a year. The hackers were able to access previously unreleased films, emails, and personal information about 4,000 employees.

2016 – Bangladesh Bank Heist

Bangladesh Bank cyber heist was a theft that took place in February 2016. Thirty-five fraudulent instructions were issued by security hackers via the SWIFT network to illegally transfer nearly $1B from the Federal Reserve Bank of New York account belonging to Bangladesh Bank. Five of the thirty-five fraudulent instructions were successful in transferring $101M, with $20M traced to Sri Lanka and $81M to the Philippines. The Federal

Reserve Bank of New York blocked the remaining thirty transactions, amounting to $850M, due to suspicions raised by a misspelled instruction. Cybersecurity experts claimed that the North Korea-based Lazarus Group was behind the attack.

2017 – WannaCry Ransomware Attack

The WannaCry attack was a massive ransomware cyber attack that hit institutions across the globe ranging all the way from the NHS in Britain to Boeing and even to Universities in China on the 12th of May, 2017.

The attack lasted 7 hours and 19 minutes. Europol estimates it affected nearly 200,000 computers in 150 countries, primarily affecting Russia, India, Ukraine, and Taiwan. This was one of the first attacks to spread via a cryptoworm.

The US Department of Justice and British authorities later attributed the WannaCry attack to the North Korean hackers the Lazarus group.

2020 – Pharmaceutical Company Attacks

Due to the ongoing COVID-19 pandemic, pharmaceutical companies became major targets for the Lazarus Group. Using spear-phishing techniques, Lazarus Group members posed as health officials and contacted pharmaceutical company employees with malicious links. It is thought that multiple major pharma organizations were targeted, but the only one that has been confirmed was the Anglo-Swedish-owned AstraZeneca.

According to a report by Reuters, a wide range of employees were targeted, including many involved in COVID-19 vaccine research.

2022 – Crypto Stealer Malware Attack

Lazarus group targets cryptocurrency companies with trojanized malicious Windows and macOS applications. Those apps are used to steal private keys and exploit security vulnerabilities to fraudulent cryptocurrency transactions. Cyber security authorities linked Lazarus to Ronin’s $625M worth of Ethereum and USDC theft. North Korean hackers have stolen at least $1.7B in cryptocurrency in the past few years.

Almost 200 malicious cryptocurrency apps related to these attacks on the Google Play Store were discovered. Most of these applications advertised themselves as mining services in order to entice users to download them.

Cyber Attack Lifecycle and TTPs

When cyber threat actors strategize a way to infiltrate an organization’s network, they follow a series of stages that comprise the cyber attack lifecycle. Here is an example of Lazarus APT’s related WannaCry ransomware attack lifecycle;

MITRE ATT&CK is an open knowledge base of threat actors’ techniques, tactics, and procedures. By observing the attacks that occur in the real world, the behavior of threat actors is systematically categorized.

MITRE ATT&CK aims to determine the risks against the actions that the threat actors can take in line with their targets and make the necessary improvements and plans.
The following MITRE ATT&CK Threat Matrix has been created to provide information on the techniques, tactics, and procedures used by Lazarus APT.

> For more details about the group, MITRE ATT&CK link

Group's Toolset and Related Malware

Lazarus uses specialized toolsets to control their victims. The group tries to hide their activity and complicate malware detection and analysis. Lazarus's infection process provides additional flexibility and anonymity throughout the cyber attacks. Here are some tools and related malware from Lazarus APT;

Tools Used for Lateral Movement:

- **AdFind:** Command line tool to collect information from Active Directory
- **SMBMap:** Tool to list accessible shared SMB resources and access those files
- **Responder-Windows :** Tool to lead clients with spoof LLMNR, NBT-NS, and WPAD
- **Mimikatz:** Dumping in-memory credentials using mimikatz is a popular attack method and a common tool.

Tools Used for Stealing Sensitive Data:

- **Xenrmor Email Password Recovery Pro:** Tool to extract credentials from email clients and services
- **XenArmor Browser Password Recovery Pro:** Tool to extract credentials from web browsers

Tools for Process Listing and Network Packet Capture

- **TightVNC Viewer:** VNC client
- **ProcDump:** Common Microsoft tool to get a process memory dump
- **tcpdump:** Packet capturing tool

- AppleJeus
- BADCALL
- Bankshot
- BLINDINGCAN
- Cryptoistic
- Dtrack
- KEYMARBLE
- KiloAlfa
- SierraAlfa
- ThreatNeedle
- Torisma
- WannaCry

Recommendations and Mitigations

After the encountered cases have been examined, it shows that the group mostly uses phishing attacks and known security vulnerabilities to gain initial access to their victims. Therefore, precautions should be taken by considering attack vectors used by the Lazarus APT may carry out.

Important recommendations that should be implemented to protect valuable assets and minimize the risk of compromises caused by security vulnerabilities and misconfigurations are shared below.

- An integrated cyber defense platform should be used that shares threat data from email, web, cloud applications, and infrastructure.
- Make sure that multi-factor authentication is enabled for all accounts using your network.
- Internet dependency should be minimized for all critical systems, and control system devices should not be connected directly to the Internet.
- All unused legacy applications should be removed from all machines on the network to avoid abuse.
- Critical networks, such as control system networks behind firewalls, must be isolated from the external network.
- Secure methods such as VPN should be used if remote access is required.
- Unused system accounts should be removed, disabled, or renamed.
- To avoid being affected by known security vulnerabilities, updates that patch the vulnerabilities should be applied as soon as possible.
- Policies that require the use of strong passwords should be implemented.
- Organizations should keep backups of important data, systems, and configurations.
- The restoring capacity should be tested. Ensure that the restore capabilities support the needs of the business.
- Institution/Organization personnel should be trained to understand cybersecurity principles and not engage in behavior that could compromise network security.

> **Download IoC, YARA and SIGMA Rules**

Source: https://brandefense.io/blog/apt-groups/lazarus-apt-group-apt38/