Contents

[**Lazarus Group (G0032)** 2](#_Toc179363281)

[**I. Introduction** 2](#_Toc179363282)

[**III. Techniques** 3](#_Toc179363283)

[**IV. Procedures** 3](#_Toc179363284)

[**V. Summary** 5](#_Toc179363285)

[**References** 6](#_Toc179363286)

## **Lazarus Group (G0032)**

## **I. Introduction**

The Lazarus Group, also known as HIDDEN COBRA, Guardians of Peace, ZINC, and NICKEL ACADEMY, is a highly sophisticated and prolific North Korean state-sponsored cyber threat group. Active since at least 2009, Lazarus Group has gained notoriety for its diverse range of cyber operations, including espionage, sabotage, and financial theft. The group is known for its technical prowess, adaptability, and its alignment with North Korean state interests.

**II**. **Tactics**

Lazarus Group's tactical approach is characterized by

1. ***Diverse Targeting***

The group conducts operations against a wide range of sectors, including government, military, financial institutions, media, and entertainment.

1. ***Long-term Campaigns***

Lazarus often maintains a presence in compromised networks for extended periods, sometimes years.

1. ***Destructive Attacks***

Known for deploying wiper malware in high-profile sabotage operations.

1. ***Financial Motivation***

Conducts large-scale financial heists to generate revenue for the North Korean regime.

1. ***Continuous Evolution***

Regularly updates and diversifies its toolset to evade detection and improve capabilities.

## **III. Techniques**

Lazarus Group employs a wide array of sophisticated techniques

|  |  |
| --- | --- |
| **Techniques** | **Description** |
| Spear-phishing (T1566) | Use of meticulously crafted emails with malicious attachments (T1566.001).  Employment of fake job offers and recruitment campaigns (T1566.002). |
| Supply Chain Attacks (T1195) | Compromise of software vendors to distribute malware through legitimate channels. |
| Custom Malware Development | Use of an extensive arsenal of custom malware, including HOPLIGHT, FALLCHILL, and ELECTRICFISH. |
| Watering Hole Attacks (T1189) | Strategic compromise of websites to distribute malware or gather intelligence. |
| Living Off The Land (T1059) | Extensive use of legitimate system tools and scripting languages for malicious purposes. |
| Cryptocurrency Theft | Development of custom tools for targeting cryptocurrency exchanges and users. |
| Anti-forensics and Obfuscation | Employment of sophisticated techniques to hinder analysis and attribution efforts |

## **IV. Procedures**

Lazarus Group's typical attack chain follows this sequence:

***1. Initial Access***

a. Spear-phishing emails are sent to targeted individuals, often containing malicious documents or links.

b. In some cases, watering hole attacks or supply chain compromises are used for initial access.

***2. Execution and Persistence***

a. Upon successful compromise, Lazarus deploys custom loaders and backdoors.

b. Multiple persistence mechanisms are established, including the use of scheduled tasks, services, and registry modifications.

***3. Privilege Escalation and Lateral Movement***

a. The group leverages both public and private exploits to elevate privileges within the compromised network.

b. Lateral movement is achieved using stolen credentials and by exploiting network vulnerabilities.

***4. Command and Control***

a. Lazarus uses a variety of C2 mechanisms, including HTTP/HTTPS protocols and compromised legitimate websites.

b. Communication is often obfuscated to evade detection.

***5. Data Exfiltration or Destructive Actions***

a. Depending on the operation's goal, sensitive data is exfiltrated or destructive malware is deployed.

b. For financial operations, custom tools are used to manipulate banking systems or steal cryptocurrency.

***6. Covering Tracks***

a. Anti-forensic techniques are employed to complicate analysis and attribution.

b. In some cases, wiper malware is deployed to destroy evidence and cause disruption.

## **V. Summary**

The Lazarus Group is a formidable, and versatile, threat actor. Their reach covers a wide range of operations, they've hit from the Sony Pictures hack to the global WannaCry ransomware outbreak and so many cryptocurrency thefts. What makes Lazarus different from many other APT groups, is the variety of targets and tactics it chooses.

More intriguing is how Lazarus is able to act as both a high tech cyber espionage unit, and as a financially motivated cybercrime organization. According to North Korea's geopolitical conundrum, cyber operations are worn two hats: they gather intelligence on the outside world and also produce hard currency to evade international sanctions. The group can be considered to evolve technically not only in developing zero day exploits, creating custom malware for different platforms and quickly adapting to new technology like cryptocurrencies.

And Lazarus’s operations graft sharp, subtle techniques and attention grabbing tactics. The Sony Pictures hack is a perfect example of how they use psychological warfare and misdirection and how to make it a media spectacle and false flag it so as to complicate attribution efforts. Lazarus is a particularly unpleasant adversary to defend against because they are able to do both long term stealthy operations and loud, destructive attacks. As North Korea's need for both strategic intelligence and alternative revenue sources persists, the Lazarus Group is likely to remain a significant and evolving threat in the global cyber landscape, blurring the lines between state-sponsored cyber activities and cybercrime.

**References**

1. Symantec Threat Hunter Team. (2017). "Lazarus: WannaCry Ransomware Attack on the Healthcare Sector." <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wannacry-ransomware-attack>

2. MITRE ATT&CK. (2024). " Lazarus Group, G0032." <https://attack.mitre.org/groups/G0032/>