Executive Summary

Lazarus Group, a state-sponsored North Korean advanced persistent threat (APT), has executed high-impact cyber campaigns over the last decade. Their operations, including the 2014 Sony Pictures hack[2] and the 2017 WannaCry ransomware attack, are characterized by geopolitical motives and a need to bypass economic sanctions through cybercrime. This report outlines the group's tactics, techniques, and procedures (TTPs), provides actionable indicators of compromise (IOCs), and offers recommendations for detection, mitigation, and strategic defense. Organizations in finance, defense, critical infrastructure, and cryptocurrency sectors must understand and proactively defend against Lazarus Group operations to reduce potential damage.

Key Takeaways:

- Lazarus is attributed to North Korea's Reconnaissance General Bureau (RGB).[4]
- Campaigns target financial systems, defense, healthcare, and media.
- Uses phishing, supply chain intrusions, and custom malware.
- This report provides a complete guide to detect and defend against known tactics.

Threat Actor Goals and Objectives

Lazarus Group operates under the direction of North Korea's RGB, aiming to achieve two strategic objectives: cyber espionage to advance military and political goals, and financial theft to support the regime and evade sanctions. [4] Their operations display flexibility and focus, evolving to exploit the most vulnerable sectors for maximum disruption or gain.

Target Sectors:

- Cryptocurrency exchanges (for financial theft) [1]
- Defense contractors (espionage) [7]
- Financial institutions (SWIFT fraud, digital heists) [1]
- Media and political institutions (sabotage and influence) [2]

These goals make Lazarus a dual-threat actor: a geopolitical espionage unit and a financially motivated crime syndicate.

Threat Actor Profile and TTPs

Lazarus Group, also tracked as HIDDEN COBRA or Zinc, has been attributed to North Korean interests since at least 2009.[4] Its campaigns span espionage, data destruction, and financially motivated crime. Their operations typically begin with phishing or fake job lures, followed by deployment of custom malware. They rapidly adapt to tooling to evade detection.

Notable Campaigns:

Operation Dream Job (2020–2023): Lazarus targeted defense and aerospace sectors by posing as recruiters offering fake job opportunities. Victims received malicious documents or links leading to malware installation. This campaign notably affected companies like Lockheed Martin and Boeing.[7]

Sony Pictures Hack (2014): Using destructive malware, Lazarus infiltrated Sony's network, stealing and leaking confidential data, including unreleased films and employee information. The attack was attributed to Lazarus by the FBI.[2]

SWIFT Banking Heists (2015–2016): Lazarus exploited vulnerabilities in the SWIFT banking system to steal $81 million from the Bangladesh Bank. They used malware to issue fraudulent transactions and cover their tracks.[1]

Cryptocurrency Exchange Attacks (2022–2024): Lazarus has been linked to several high-profile cryptocurrency thefts, including a $625 million heist from the Ronin Network in 2022 and a $1.4 billion theft from Bybit in 2024.[1]

Tactics, Techniques, and Procedures (MITRE ATT&CK-Aligned):

Initial Access: Lazarus frequently uses spear phishing emails with malicious attachments (T1566.001)[10] or fake job offers (Operation Dream Job). Known to exploit CVEs in Microsoft Office.

Execution & Persistence: Deploys tools such as *NukeSped*, *Manuscrypt*, and *RATANKBA* using techniques like DLL side-loading and Windows scripting (T1059)[5].

Privilege Escalation & Lateral Movement: Uses valid accounts (T1078), SMB shares (T1021.002), and exploits vulnerable software.

Command & Control (C2): Operates over HTTPS and uses compromised infrastructure and social platforms for communication (T1071.001).

Exfiltration & Impact: Compresses data before exfiltration (T1560) and has deployed wiper malware and ransomware in multiple campaigns (T1486).

Current Situation

Lazarus Group remains one of the most closely tracked APTs in the world due to its technical adaptability and broad target profile. In response, both government and industry have shifted from reactive investigation to proactive threat modeling, detection engineering, and adversary emulation.

Government Response

The U.S. Treasury's Office of Foreign Assets Control (OFAC) has issued sanctions against individuals, infrastructure, and cryptocurrency wallets linked to Lazarus Group[1]. Following the $625 million Ronin Bridge hack in 2022, the U.S. formally attributed the intrusion to Lazarus and sanctioned the Tornado Cash mixer used to launder the stolen assets[1]. These financial sanctions mark a shift in how nation-state cybercrime is countered—treating cryptocurrency abuse as a geopolitical issue rather than a criminal anomaly.

Joint technical advisories from the Cybersecurity and Infrastructure Security Agency (CISA), FBI, and NSA have detailed Lazarus's evolving TTPs[3]. These alerts include actionable IOCs, ATT&CK mappings, and mitigation strategies, with specific focus on targeting within healthcare, cryptocurrency, and defense sectors. The timeliness of these reports has improved defenders' ability to adapt detection rules and incident response workflows.

International cooperation through Europol, Interpol, and national CERTs has enabled partial takedowns of Lazarus infrastructure. However, decentralized and bulletproof hosting limits the scope and longevity of these efforts, highlighting the need for internal resilience rather than external takedown dependence.

Security Research and Enterprise Response

Leading cybersecurity firms—such as Mandiant, Kaspersky, and ESET—have played a key role in analyzing Lazarus's malware families (e.g., *NukeSped*, *DeathNote*, *Bookcode*) and sharing detection logic[5,6,7]. These technical reports have been essential for translating threat intelligence into deployable signatures and YARA/Sigma rules.

Security operations teams increasingly incorporate Lazarus TTPs into red and purple team exercises using MITRE ATT&CK and simulation frameworks like Atomic Red Team[4]. This hands-on testing approach has helped organizations identify visibility gaps in EDR/NDR coverage, especially around stealthy scripting and post-exploitation behavior.

Open-source and commercial threat intel platforms—such as VirusTotal, Abuse.ch, and Anomali—have become critical tools for maintaining situational awareness. Real-time IOC sharing enables defenders to track Lazarus infrastructure shifts and campaign evolutions with more agility than static blocklists.

Together, these efforts have improved global visibility of Lazarus Group's campaigns. However, meaningful defense still hinges on how well organizations ingest, interpret, and operationalize this intelligence in their own environments.

Detection and Detection Engineering

Detecting Lazarus Group activity requires more than static indicators — it demands layered visibility across endpoints, networks, and behavioral baselines. While the group's tools evolve, their campaigns often exhibit repeatable characteristics that defenders can detect using a mix of known signatures and behavioral analytics.

Intrusion prevention systems (IPS) and next-generation firewalls remain foundational for perimeter detection. They can be configured to block or alert on known Lazarus infrastructure using published IPs and domains, especially those released in joint advisories from CISA and commercial threat intelligence feeds[3]. However, this approach has limited shelf life: Lazarus frequently rotates infrastructure and blends into legitimate traffic.

Hashes of known Lazarus malware — including tools like *NukeSped*, *RATANKBA*, and *DeathNote* — can be used in EDR platforms and forensic triage to flag binaries during scanning or memory analysis. These static IOCs help confirm infections after initial compromise, especially when paired with a log correlation across host and network telemetry[5,6].

To move beyond reactive detection, many defenders rely on **YARA and Sigma rules**, which detect Lazarus activity based on string patterns, file structures, and event behaviors. YARA is the most effective in scanning files or memory for malware signatures, while Sigma is designed for use in SIEM platforms to flag suspicious log patterns[9].

YARA rules, by contrast, are more granular and used in malware analysis pipelines. For example, a lightweight YARA rule to flag Lazarus's *NukeSped* variant may include hardcoded strings or cryptographic patterns unique to that malware family[9].

Together, these tools allow security teams to proactively detect Lazarus Group operations — not only when signatures are known, but also when behaviors match a broader threat profile. Detection engineering is most effective when IOCs are backed by structured threat intelligence and tuned to the specific environment they protect.

Mitigation and Remediation Steps

To effectively defend against the Lazarus Group, organizations must implement layered, behavior-focused mitigation strategies mapped to real adversary techniques.

One of the most critical areas is email and document hygiene. Lazarus frequently gains initial access via spear phishing attachments (T1566.001) [10]. Organizations should block or sandbox common payloads such as Office documents with embedded macros, scripts, and executable file types. Disabling macros from untrusted sources and preventing unsigned script execution can significantly reduce exposure.

Endpoint Detection and Response (EDR) solutions should be tuned to monitor for Living Off the Land Binaries (LOLBins), custom interpreters, and obfuscated scripting, all of which Lazarus uses to evade detection. These techniques align with T1059 (Command and Scripting Interpreter) and T1218 (Signed Binary Proxy Execution) [4]. EDR platforms should alert anomalous parent-child process chains, scripting launched from non-standard directories, and system tools abused for persistence.

Lateral movement can be mitigated by enforcing strict SMB (T1021.002) restrictions and applying robust internal segmentation. Authentication attempts and lateral movement via valid accounts (T1078) should trigger alerts if they originate from untrusted network zones or privileged accounts. MITRE recommends using multi-factor authentication and limiting the use of administrative credentials to prevent unauthorized escalation[4].

In cases of confirmed intrusion, incident response teams should isolate affected systems, preserve forensic artifacts (e.g., registry keys, memory images), and conduct structured triage. Lazarus often establishes persistence via scheduled tasks, registry autoruns, or malware embedded in system services. Removing these mechanisms and rotating credentials, especially for privileged accounts, is essential to re-establish trust.

Proactive defense strategies must include red and purple team exercises modeled on Lazarus campaigns, including Operation Dream Job. These simulations test not just detection, but lateral movement visibility and response coordination. Organizations should also subscribe to curated threat intelligence feeds that track North Korean APT groups and Lazarus-specific IOC updates[4].

Call to Action

Lazarus Group is not a hypothetical threat. It is an active, state-sponsored adversary with a decade-long history of successful intrusions, financial theft, and cyber sabotage. Waiting for compromise is no longer a viable strategy. Organizations must act with intention, treating Lazarus like the persistent threat it is.

The priority is operationalizing detection. Security teams should deploy this report's YARA and Sigma rules to ensure coverage of known malware signatures and behavioral indicators[9]. These rules should be reviewed and tuned for the organization's specific threat landscape, particularly in sectors like finance, defense, or crypto, where Lazarus has demonstrated repeat interest.

Defensive posture also hinges on user-level hardening. Targeted spear phishing remains a primary vector of compromise for Lazarus campaigns, especially those posing as job recruiters. Security awareness training should emphasize spear phishing recognition and test user resilience through simulated lures. At the same time, mail gateways must be configured to block dangerous attachments and scripts that bypass standard protections[10].

Threat hunts and tabletop exercises grounded in Lazarus TTPs—such as those observed in Operation Dream Job or the SWIFT heists—should be integrated into security testing. These scenarios expose blind spots in detection logic and give incident response teams a chance to rehearse containment strategies before an actual breach occurs.

Finally, organizations should update their incident response playbooks to include procedures for malware families, C2 infrastructure, and lateral movement techniques associated with Lazarus. Playbooks should be validated during drills, with cross-functional participation from IT, legal, and executive stakeholders.

To begin this process, security engineering teams should be assigned to ingest and triage IOCs. Existing detections must be reviewed against known Lazarus techniques, and coverage gaps should be closed with high-priority configuration changes. Network segmentation and backup resilience should be audited, ensuring that in the event of compromise, systems can be contained, restored, and recovered quickly.

The threat from Lazarus is not going away—but with deliberate action, it can be outpaced

Appendix

Appendix A: Indicators of Compromise (IOCs)

File Hashes:

- c6323a40d1aa5b7fe95951609fb2b524 – NukeSped variant
- cf8c0999c148d764667b1a269c28bdcb – RATANKBA sample
- 37973e29576db8a438250a156977ccdf – DeathNote malware
- 778942b891c4e2f3866c6a3c09bf74f4 – Bookcode malware
- 1315027e1c536d488fe63ea0a528b52d – Manuscrypt sample
- b0e795853b655682483105e353b9cd54 – NukeSped variant
- e0dd4afb965771f8347549fd93423985 – RATANKBA sample
- 875b0cbad25e04a255b13f86ba361b58453b6f3c5cc11aca2db573c656e64e24 – APT38 malware
- 10370f821ef2d769bcb287b3f5ab081c4949a97891a25a23688e8c553bd393df – Lazarus malware

IP Addresses:

- 222.112.127.9 – Used in phishing campaigns targeting South Korea
- 23.237.32.34 – Lazarus C2 infrastructure
- 146.185.26.150 – Network activity tied to Lazarus
- 146.4.21.94 – Hosted QuiteRAT malware
- 23.81.246.131 – Naver phishing infrastructure
- 172.93.201.253 – Resolved from Lazarus domain
- 45.147.231.213 – Known C2 infrastructure

Domains:

- navercorpservice.com – Used in phishing campaigns

- www.devguardmap.org – Associated with Lazarus C2

Registry Keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin – Disables UAC prompts
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WmiApSrv\Start – Persistence via service abuse
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\ – Persistence on reboot

Mutexes:

- _desktop45678fo2 – Associated with MATA malware infections

Email Indicators:

- peterstewart0326@gmail.com – Used to register attacker-controlled cloud accounts
- X-Originating-IP: 222.112.127.9 – Sender IP in phishing email headers

---

Appendix B: MITRE ATT&CK Techniques Used by Lazarus Group

Tactic	Technique ID	Technique/Sub-technique Name
Account Discovery	T1087.002	Domain Account
Access Token Manipulation	T1134.002	Create Process with Token
Account Manipulation	T1098	Account Manipulation
Acquire Infrastructure	T1583.001	Domains
Application Layer Protocol	T1071.001	Web Protocols
Archive Collected Data	T1560.001	Archive via Utility
Boot or Logon Autostart	T1547.001	Registry Run Keys / Startup Folder
Brute Force	T1110	Brute Force

Lazarus Group: A Persistent Cyber Threat with Global Reach

Tactic	Technique ID	Technique/Sub-technique Name
Command & Scripting (VB)	T1059.005	Visual Basic
Command & Scripting (PS)	T1059.001	PowerShell
Command & Scripting (CMD)	T1059.003	Windows Command Shell
Compromise Infrastructure	T1584.001	Domains
Compromise Infrastructure	T1584.004	Server
Data from Local System	T1005	Data from Local System
Debugger Evasion	T1622	Debugger Evasion
Develop Capabilities	T1587.002	Code Signing Certificates
Develop Capabilities	T1587.001	Malware
Encrypted Channel	T1573.001	Symmetric Cryptography
Establish Accounts	T1585.001	Social Media Accounts
Establish Accounts	T1585.002	Email Accounts
Exfiltration Over C2	T1041	Exfiltration Over C2 Channel
Exfiltration to Cloud	T1567.002	Exfiltration to Cloud Storage
File & Directory Discovery	T1083	File and Directory Discovery
Gather Identity Info	T1589	Identity Information
Identify Roles	T1591.002	Identify Roles
Impersonation	T1656	Impersonation
Indicator Removal	T1070.004	File Deletion
Ingress Tool Transfer	T1105	Ingress Tool Transfer
Internal Spear phishing	T1534	Internal Spear phishing
Masquerading File Type	T1036.008	Masquerade File Type

Lazarus Group: A Persistent Cyber Threat with Global Reach

Tactic	Technique ID	Technique/Sub-technique Name
Native API	T1106	Native API
Obfuscation: Packing	T1027.002	Software Packing
Obfuscation: Encryption	T1027.003	Encrypted/Encoded File
Obtain Capabilities	T1588.003	Code Signing Certificates
Obtain Capabilities	T1588.002	Tool
Phishing: Attachment	T1566.001	Spearphishing Attachment
Phishing: Link	T1566.002	Spearphishing Link
Phishing via Service	T1566.003	Spearphishing via Service
Scheduled Task	T1053.005	Scheduled Task
Search via Social Media	T1593.001	Social Media
Server Component (IIS)	T1505.003	IIS Components
Stage Capabilities: Malware	T1608.001	Upload Malware
Stage Capabilities: Tool	T1608.002	Upload Tool
Subvert Trust: Code Signing	T1553.002	Code Signing
System Binary Proxy	T1218.011	Rundll32
System Binary Proxy	T1218.010	Regsvr32
System Language Discovery	T1614.001	System Language Discovery
Template Injection	T1221	Template Injection
User Execution: Link	T1204.001	Malicious Link
User Execution: File	T1204.002	Malicious File
Sandbox Evasion: Checks	T1497.001	System Checks
Sandbox Evasion: Timing	T1497.003	Time Based Evasion

Tactic	Technique ID	Technique/Sub-technique Name
WMI	T1047	Windows Management Instrumentation
XSL Script Processing	T1220	XSL Script Processing

Appendix C: Yara Rules & Sigma Rules

Yara Rules

```
rule APT_Lazarus_AppleJeus_Downloader {
  meta:
    description = "Detects Lazarus Group malware downloader from Operation AppleJeus"
    author = "Florian Roth (Nextron Systems)"
    reference = "https://securelist.com/operation-applejeus/87553/"
    date = "2018-08-24"
  strings:
    $s1 = "H:\\DEV\\TManager\\" ascii
    $s2 = "\\Release\\dloader.pdb" ascii
    $s3 = "Z:\\jeus\\" ascii
    $s4 = "\\Debug\\dloader.pdb" ascii
    $s5 = "Moz&Wie;#t/6T!2yW29ab@ad%Df324V$Yd" fullword ascii
    $s6 = "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)" fullword ascii
  condition:
    uint16(0) == 0x5a4d and filesize < 500KB and (1 of ($s1, $s2, $s3, $s4) or 2 of ($s1, $s2, $s3, $s4, $s5, $s6))
```

Lazarus Group: A Persistent Cyber Threat with Global Reach

```
rule Lazarus_Dec_17_2 {
  meta:
    description = "Detects Lazarus malware from December 2017 incident"
    author = "Florian Roth (Nextron Systems)"
    reference = "https://goo.gl/8U6fY2"
    date = "2017-12-20"
  strings:
    $s1 = "SkypeSetup.exe" fullword wide
    $s2 = "%s\\SkypeSetup.exe" fullword ascii
    $s3 = "Skype Technologies S.A." fullword wide
    $a1 = "Microsoft Code Signing PCA" ascii wide
  condition:
    uint16(0) == 0x5a4d and filesize < 7000KB and (all of ($s1, $s2, $s3) and not $a1)
```

Sigma Rules

```
title: Mshta Suspicious Bitly URL
id: 12345678-1234-1234-1234-1234567890ab
description: Detects suspicious non-browser attempts to access Bitly URLs using mshta.exe
status: experimental
author: F-Secure Countercept
date: 2020/09/25
logsource:
 category: process_creation
 product: windows
detection:
 selection:
    Image|endswith: '\mshta.exe'
    CommandLine|contains:
      - 'bit.ly'
  condition: selection
level: high
references:
  - https://labs.f-secure.com/publications/ti-report-lazarus-group-cryptocurrency-vertical
  - https://labs.f-secure.com/blog/catching-lazarus-threat-intelligence-to-real-detection-logic
title: Microsoft Word Launching Explorer
id: 87654321-4321-4321-4321-0987654321ba
description: Detects Microsoft Word launching explorer.exe, which is uncommon and may indicate malicious activity
status: experimental
author: F-Secure Countercept
date: 2020/09/25
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    ParentImage|endswith: '\winword.exe'
    Image|endswith: '\explorer.exe'
  condition: selection
level: high
references:
  - https://labs.f-secure.com/publications/ti-report-lazarus-group-cryptocurrency-vertical
  - https://labs.f-secure.com/blog/catching-lazarus-threat-intelligence-to-real-detection-logic
title: Suspicious Execution from ProgramData Directory
id: abcdef12-3456-7890-abcd-ef1234567890
description: Detects suspicious execution of binaries from the ProgramData directory, which is uncommon and may indicate malicious activity
status: experimental
author: F-Secure Countercept
date: 2020/09/25
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    Image|contains: 'C:\ProgramData\'
  condition: selection
level: high
references:
  - https://labs.f-secure.com/publications/ti-report-lazarus-group-cryptocurrency-vertical
  - https://labs.f-secure.com/blog/catching-lazarus-threat-intelligence-to-real-detection-logic
```

title: Suspicious Execution from ProgramData Directory

```
id: abcdef12-3456-7890-abcd-ef1234567890
description: Detects suspicious execution of binaries from the ProgramData directory, which is uncommon and may indicate malicious activity
status: experimental
author: F-Secure Countercept
```

```
date: 2020/09/25
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    Image|contains: 'C:\ProgramData\'
  condition: selection
level: high
references:
  - https://labs.f-secure.com/publications/ti-report-lazarus-group-cryptocurrency-vertical
  - https://labs.f-secure.com/blog/catching-lazarus-threat-intelligence-to-real-detection-logic
```

Appendix D: References

[1] U.S. Department of the Treasury. (2022). *Treasury Sanctions North Korean Lazarus Group for Ronin Bridge Hack*. U.S. Department of the Treasury. https://home.treasury.gov/news/press-releases/jy0700

[2] Federal Bureau of Investigation (FBI). (2014). *FBI Statement on Sony Investigation*. FBI.gov. https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

[3] Cybersecurity and Infrastructure Security Agency (CISA). (2023). *North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare Sector*. CISA.gov. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-187a

[4] MITRE. (2024). *Lazarus Group (G0032)*. MITRE ATT&CK. https://attack.mitre.org/groups/G0032/

[5] Kaspersky. (2022). *DeathNote Cluster Evolution*. Securelist. https://securelist.com/lazarus-deathnote-cluster-evolution/107130/

[6] Zscaler ThreatLabz. (2023). *Naver-Themed Lazarus Phishing Campaign*. Zscaler Blog. https://www.zscaler.com/blogs/security-research/naver-ending-game-lazarus-apt

[7] ESET Research. (2021). *Operation In(ter)ception: Lazarus Targets Aerospace and Defense*. WeLiveSecurity. https://www.welivesecurity.com/2020/06/18/operation-interception-lazarus-targets-aerospace-defense/

[8] Cisco Talos. (2023). *Threat Spotlight: Lazarus Group Campaign Analysis*. Talos Intelligence. https://blog.talosintelligence.com/lazarus-group-malware-campaign/

[9] Florian Roth. (2018). *YARA Rule: AppleJeus Downloader*. GitHub. https://github.com/Neo23x0/signature-base

[10] MITRE ATT&CK. (2024). *T1566.001 - Spearphishing Attachment*. MITRE ATT&CK. https://attack.mitre.org/techniques/T1566/001/