STRATEGIC THREAT INTELLIGENCE PROFILE

Binary

Prepared for: COMSEC3

Date:

THREAT INTELLIGENCE TEAM

Name	Email
Marielle Kloie Concepcion	mdconcepcion@student.apc.edu.ph
Abrech D. Dela Cruz	Addelacruz2@student.apc.edu.ph
Ezekiel D. Galauran	edgalauran@student.apc.edu.ph
Gabriel Villanueva	gmvillanueva@student.apc.edu.ph

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Assessment:

According to a high confidence assessment, APT38 (Lazarus) is a state-sponsored cyber threat group that operates under the Reconnaissance General Bureau of the Democratic People's Republic of Korea (DPRK). Active since at least 2009, this group constitutes a critical threat to the financial services and cryptocurrency/blockchain industries. APT38's operations demonstrate a persistent focus on large-scale financial theft, the deployment of malicious malware, and intricate infiltration campaigns designed to generate revenue to support state objectives. Campaigns linked to this threat exhibit advanced technological capabilities, long-term operational planning, and coordinated use of supply chain exploitation, social engineering, and custom malware. Targeting banks, digital wallets, cryptocurrency exchanges, and interbank transfer networks results in large financial losses in several regions. These operations' scope, tenacity, and complexity show governmental support and strategic alignment with the national economic interests.

Key Findings:

- Primary Motivation: Illicit revenue generation through cyber-enabled financial theft, including bank fraud, cryptocurrency theft, and ransomware operations, supporting sanctioned state funding requirements.
- Most Notable Attack: The 2016 Bangladesh Bank heist, which utilized fraudulent SWIFT credentials to attempt the theft of $951 million, and the 2017 WannaCry ransomware outbreak, which caused global disruption across healthcare and manufacturing sectors.
- Strategic Impact: APT38 represents a significant risk to global financial stability and digital trust. Successful intrusions results to direct financial losses, operational disruption, regulatory exposure, and reputational damage. Board-level awareness is essential due to the potential for systemic damage, cross-border implications and the increasing convergence of state-sponsored operations and cybercrime targeting critical financial infrastructure.

IDENTITY AND ATTRIBUTION

The Lazarus Group (commonly tracked as **APT38**, **Hidden Cobra**, **ZINC**, or **Diamond Sleet**) is assessed with high confidence to be a state-sponsored cyber espionage and sabotage organization acting on behalf of the North Korean government. Unlike independent cybercriminal syndicates motivated solely by profit, or hacktivists motivated by ideology, Lazarus operates as an extension of state power. Their identity is defined by a unique hybrid structure that blends the discipline and resources of a military intelligence unit with the agility and financial motivations of organized crime.

2.1 Origins and Sponsorship

The group traces its origins to the **Reconnaissance General Bureau (RGB)**, specifically **Bureau 121**, North Korea's primary foreign intelligence service. Established around 2009, the group initially focused on disruptive DDoS attacks against South Korean and U.S. government websites (Operation Troy). However, following the imposition of severe international sanctions, their mandate expanded significantly. Intelligence indicates that the group is tasked directly by the regime to fulfill the "dual-mission" doctrine:

1. **Asymmetric Warfare:** Leveling the playing field against technologically superior adversaries (South Korea and the U.S.) through sabotage and espionage.
2. **Sanctions Evasion:** Generating illicit foreign currency to fund the DPRK's nuclear and ballistic missile programs.

2.2 Personas

The Lazarus umbrella is vast, and the group often segments its operations into specialized subunits, or "personas," to handle specific mission types. These are often treated as distinct clusters by security vendors but fall under the wider Lazarus directorate:

- Bluenoroff (APT38): The financial wing responsible for SWIFT banking heists and the recent wave of cryptocurrency thefts. They operate with high technical precision to manipulate transaction ledgers.
- Andariel (Stonefly): A subgroup primarily focused on South Korean targets, defense contractors, and university networks to steal military secrets and intellectual property.
- The "Recruiters": A social engineering persona used heavily in "Operation Dream Job." Operatives pose as HR professionals from top-tier companies (e.g., McKinsey, Google, Boeing) on LinkedIn and Telegram to lure victims into downloading malware disguised as job descriptions.

VICTIMOLOGY

The victimology of the Lazarus Group is distinctively broad, shifting dynamically based on the current financial needs and geopolitical goals of Pyongyang. While most state-sponsored actors focus almost exclusively on government and military targets, Lazarus is unique in its aggressive targeting of the private sector for monetary gain. Their victim profile suggests a highly opportunistic yet strategic targeting methodology, seeking out organizations with high capital reserves or critical intellectual property.

3.1 Targeted Sectors

- **Financial Services & Cryptocurrency (Primary):** This sector bears the brunt of Lazarus activity. Targets include traditional banks (for SWIFT transfer fraud), cryptocurrency exchanges, Decentralized Finance (DeFi) platforms, and cross-chain bridges. The goal is direct theft of funds.
- **Defense & Aerospace:** Defense contractors, particularly those involved in missile technology, radar systems, and naval engineering, are targeted for industrial espionage to accelerate North Korea's own military development.
- **Critical Infrastructure & Energy:** Utility providers and energy companies are targeted both for potential disruption (sabotage) and for ransomware extortions.
- **Media & Entertainment:** Historically targeted for reputational damage and sabotage, most notably the 2014 Sony Pictures hack, which was a retaliatory act against media perceived as insulting to the regime.

3.2 Geographic Focus

- **South Korea:** The primary and persistent target due to ongoing geopolitical conflict. Targets range from government ministries to local financial institutions.
- **United States:** A strategic priority for espionage against defense contractors and government agencies.
- **Southeast Asia & Emerging Markets:** Countries such as Bangladesh, Vietnam, the Philippines, and Ecuador have been heavily targeted for banking heists. Lazarus often exploits weaker cybersecurity maturity in these regions to access global interbank networks (SWIFT).
- **Japan:** Frequently targeted for cryptocurrency exchange thefts and high-tech intellectual property.

3.3 Strategic Alignment

The targeting logic of the Lazarus Group is directly aligned with the **national survival strategy of the DPRK**.

1. **Economic Survival:** As international sanctions cut off legitimate trade, the regime relies on the cyber-theft of cryptocurrency (estimated to fund over 50% of their missile program) to procure foreign currency.
2. **Military Parity:** By stealing blueprints from global defense contractors, the group bypasses years of R&D, allowing North Korea to advance its weapons capabilities faster than its domestic economy would allow.
3. **Regime Security:** Attacks on media and defectors are conducted to suppress dissent and control the narrative surrounding the country's leadership.

.

THE ATTACK LIFECYCLE (TTPs)

The Lazarus Group (APT38/Hidden Cobra) operates with a unique dual mandate: state-sponsored espionage and large-scale financial theft. Unlike typical Advanced Persistent Threats (APTs) that prioritize stealth above all else, Lazarus is characterized by its patience in the early stages and its aggressive, often destructive behavior in the final stages. Their operational tempo allows them to dwell within a victim's network for months (an average of 150+ days) to understand the business logic before striking. They are methodologically flexible, shifting their tools and techniques based on whether the target is a defense contractor (espionage), a bank (SWIFT theft), or a cryptocurrency exchange (digital asset theft).

4.1 Initial Compromise

Lazarus relies heavily on advanced social engineering and supply chain compromises rather than "smash-and-grab" exploits. Their most prolific tactic, "Operation Dream Job," involves operatives posing as recruiters on LinkedIn or Telegram, offering high-paying roles at prestigious tech or defense firms (e.g., Boeing, Tesla, Binance). After weeks of rapport building, they send a malicious payload disguised as a "Job Description" (PDF/LNK) or a "Coding Challenge" (Python/Node.js). Additionally, they are notorious for trojanizing legitimate software; this includes compromising open-source developer tools or distributing fake cryptocurrency trading applications (e.g., *Celas Trade Pro*, *JMT Trading*) that function normally but install a backdoor in the background.

4.2 Establish Foothold & Escalate Privileges

Once inside the perimeter, Lazarus prioritizes persistence and defense evasion. Their signature technique is **DLL Side-Loading**, where they drop a legitimate, digitally signed binary (often from Microsoft or a security vendor) alongside a malicious `.dll` file. When the legitimate program runs, it automatically loads the malware, bypassing standard antivirus detection. They deploy custom Remote Access Trojans (RATs) such as **Manuscrypt**, **Fallchill**, or **PondRAT**. To escalate privileges, they frequently exploit vulnerabilities in system drivers (Bring Your Own Vulnerable Driver - BYOVD) or abuse the Windows AppLocker service to gain kernel-level access, allowing them to disable Endpoint Detection and Response (EDR) agents. They set up **scheduled tasks** to periodically call out to their **Command and Control (C2)** infrastructure, which is hosted on compromised third-party servers like those from **Stark Industries**.

4.3 Internal Reconnaissance & Lateral Movement

Lazarus utilizes "Living off the Land" (LotL) techniques to blend in with normal administrative traffic. They aggressively use standard system tools like `PowerShell`, `WMIC`, and `Certutil` to map the network without

dropping suspicious files. For lateral movement, they harvest credentials using **Mimikatz** to dump memory and move across the network via RDP or SMB. In their financial campaigns, they specifically hunt for internal documentation (wikis, Jira, email servers) to understand the victim's transaction approval processes. They are also known for **"Timestomping,"** a technique where they modify the creation timestamps of their malware to match legitimate system files (e.g., dating a file to 2019), confusing forensic timelines.

4.4 Complete Mission (Exfiltration/Impact)

The final stage depends on the objective. For **Espionage**, they exfiltrate sensitive military or technical data using encrypted channels, often abusing legitimate cloud services (Dropbox, OneDrive) to hide the traffic. For **Financial Theft**, they manipulate business logic; this includes injecting fraudulent transactions into SWIFT banking networks (e.g., Bangladesh Bank), exploiting cross-chain bridges to drain cryptocurrency wallets, or authorizing unlimited ATM withdrawals (FASTCash). In cases of **Sabotage** or when they need to cover their tracks, they deploy destructive wipers (like **KillDisk** or **HermeticWiper**) that overwrite the Master Boot Record (MBR), rendering the victim's infrastructure unrecoverable.

INFRASTRUCTURE AND CAPABILITIES

The Lazarus Group maintains a highly sophisticated and resilient network infrastructure that is designed to mask their North Korean origins while providing centralized control over global operations. Their command-and-control (C2) architecture has recently evolved to include web-based administrative platforms built with **React and Node.js**, allowing operators to efficiently manage exfiltrated data and command multiple bots through a single hub. To maintain anonymity, the group utilizes a multi-layered proxy system, frequently routing their traffic through **Astrill VPN** and various intermediate "hop points" to hide their true IP addresses. They often hijack legitimate but vulnerable third-party servers, such as those from **Stark Industries Solutions**, to host their malicious payloads and C2 services [1]. Additionally, the group employs unconventional network protocols and ports, such as communication over **port 1224** and the use of **FakeTLS** [2], which mimics legitimate encryption to bypass standard security inspections. By integrating these "living-off-the-network" techniques with custom staging areas on compromised hosts, Lazarus ensures that their data exfiltration remains stealthy and difficult for defenders to trace back to Pyongyang.

5.1 The Malware Arsenal

The Lazarus Group maintains a vast and constantly evolving suite of custom tools designed for espionage, financial theft, and system destruction.

- **Modular Frameworks**: They utilize the **MATA framework**, a sophisticated, modular toolkit capable of targeting Windows, Linux, and macOS.

- **Remote Access Trojans (RATs)**: Recent campaigns have introduced new strains like **PondRAT**, **ThemeForestRAT**, and **RemotePE**, alongside their long-standing **Manuscrypt** (or DUBNIUM) and **Dtrack** backdoors.
- **Financial & Crypto Tools**: They use **AppleJeus** (disguised as crypto trading apps) to steal cryptocurrency and **DYEPACK** to manipulate SWIFT banking records to hide fraudulent transfers.
- **Destructive Wipers & Ransomware**: The group is famously linked to the **WannaCry** ransomware and uses custom wipers like **BOOTWRECK** to destroy Master Boot Records (MBR), rendering systems unbootable.
- **Specialized Utilities**: Their arsenal includes **KiloAlfa** (a keylogger that targets specific interactive user sessions) and **KEYLIME** for capturing clipboard data.

5.2 Network Infrastructure

Lazarus employs a complex, multi-layered infrastructure to hide their North Korean origins and maintain persistent control over victims.

- **Command and Control (C2) Platforms**: They have recently transitioned to using a **web-based administrative platform** built with **React and Node.js** to centrally manage exfiltrated data and command their bots.
- **Anonymization Layers**: To obscure their IP addresses, they route traffic through commercial VPNs (notably **Astrill VPN**) and proxy services like **Oculus Proxy** before reaching their final C2 servers.
- **Compromised Servers**: They often host their C2 infrastructure on legitimate but compromised servers, such as those owned by **Stark Industries Solutions**, and use unusual ports like **1224 and 1245** for communication.
- **Staging & Stealth**: The group uses local scripts to "stage" stolen data within the victim's network (e.g., in the %TEMP% folder) before uploading it, which minimizes the number of external connections and helps avoid triggering network alerts.
- **Living-off-the-Land**: They frequently hijack legitimate network protocols and system tools, such as using **Remote Desktop Protocol (RDP)** for lateral movement or **SMTP** to email details about new victims back to their controllers.

DEFENSIVE RECOMMENDATIONS

The methods of the Lazarus Group that require robust countering include their sophisticated use of social engineering, specifically through "Operation Dream Job" campaigns that utilize fake LinkedIn profiles and trojanized job lures to gain initial access. Once inside a network, the group effectively employs "Living off the Land" techniques by hijacking legitimate system tools like WMIC.exe and rundll32.exe to blend in with normal administrative activity and evade detection by standard antivirus software.

6.1 Strategic Recommendations

These are long-term organizational shifts designed to make the environment hostile to the Lazarus Group's methods.

- **Implement Zero-Trust Architecture**: Move away from trusting anything inside the network. Every user and device must be continuously verified, regardless of their location, which neutralizes Lazarus's "lateral movement" tactics.
- **Strict Supply Chain Vetting**: Since Lazarus often uses "Trojanized" software and supply chain attacks, the organization must implement a **Software Bill of Materials (SBOM)** to track and verify the integrity of all third-party code and installers.
- **Enhanced Personnel Vetting**: For organizations in crypto, defense, or finance, the hiring process must include video verification and strict document checks to counter "Operation Dream Job" (fake recruiter/employee) schemes.
- **Immutable Backup Strategy**: Maintain "air-gapped" or immutable backups that cannot be reached or encrypted by ransomware like WannaCry, ensuring the business can recover without paying a ransom.

Strategic recommendations against the Lazarus Group are critical because their attacks are characterized by long-term persistence and the ability to move laterally through a network once an initial foothold is gained. By adopting a **Zero-Trust architecture**, organizations eliminate the "implicit trust" that Lazarus exploits to escalate privileges; instead, every user and device is continuously verified, significantly hindering the group's ability to stay hidden. **Network micro-segmentation** acts as a vital internal barrier, ensuring that even if a single workstation is compromised through a phishing link, the infection is contained and cannot reach high-value targets like SWIFT servers or cryptocurrency cold wallets. Furthermore, utilizing a **Software Bill of Materials (SBOM)** is a direct defense against their frequent supply chain attacks, as it allows security teams to identify and vet every component of third-party software for the "Trojanized" code often inserted by North Korean operatives. Implementing **phishing-resistant Multi-Factor Authentication (MFA)** is equally essential to neutralize their relentless credential theft campaigns, which often target remote workers and IT administrators. Collectively, these strategies shift the defensive posture from

reactive to proactive, making the environment exponentially more difficult and "noisy" for a stealth-focused actor like Lazarus to navigate successfully.

6.2 Tactical Recommendations

These are specific, immediate technical configurations to detect and block active Lazarus campaigns.

- **Monitor Non-Standard Ports**: Specifically configure firewalls and EDRs to alert on outbound traffic using ports **1224 and 1245**, which have been linked to recent Lazarus C2 infrastructure.
- **Deploy Behavioral EDR**: Use Endpoint Detection and Response (EDR) tools to flag "Living-off-the-Land" techniques, such as the renaming of WMIC.exe to nvc.exe or unauthorized use of rundll32.exe to bypass security.
- **Audit Active Directory & SWIFT**: Conduct weekly audits of administrator account names (Lazarus malware like *WhiskeyDelta* often tries to rename them) and implement multi-signature requirements for all high-value financial transfers.
- **Enable FakeTLS Inspection**: Deploy network security tools capable of deep-packet inspection (DPI) to identify and block **FakeTLS** handshakes—traffic that looks like standard encryption but uses custom XOR-based encoding.
- **Network Micro-segmentation**: Isolate critical payment systems and development environments into "Micro-segments" so that a single infected workstation cannot reach the company's most sensitive assets.

Tactical recommendations are essential for defending against the Lazarus Group because they focus on the immediate detection and disruption of the group's highly automated and evasive technical maneuvers. Monitoring non-standard ports, specifically **ports 1224 and 1245**, is recommended because these have been identified as primary channels for their recent command-and-control (C2) infrastructure and data exfiltration, allowing defenders to catch "phone home" activity that standard filters might miss. The deployment of **behavioral EDR (Endpoint Detection and Response)** is crucial to counter their "Living-off-the-Land" tactics, such as the renaming of legitimate system tools like WMIC.exe to bypass static signature-based detection. Furthermore, **Deep Packet Inspection (DPI)** is a necessary tactical layer to identify the unique "handshake" of **FakeTLS**, which Lazarus uses to hide malicious traffic inside what appears to be a normal encrypted web session. By implementing **application whitelisting**, organizations can prevent the execution of the group's custom-built RATs and backdoors that are often delivered through trojanized software packages in supply chain attacks. Finally, these tactical controls significantly reduce the "dwell time" of the attacker, forcing them to use noisier methods that are more likely to trigger alerts, thereby breaking the attack lifecycle before they can reach critical financial or sensitive data repositories.

CONCLUSION

This strategic threat intelligence profile demonstrates that Lazarus Group (APT38) represents one of the most sophisticated and persistent cyber threats to the global financial landscape and critical infrastructure. The combination of state-sponsored espionage and long-term operational planning creates a distinct risk profile that sets this threat actor apart from traditional cybercriminal groups. Campaigns attributed to APT38 consistently utilize a diverse arsenal of custom malware, social engineering, and blend espionage tradecraft with financially motivated attacks. This results in significant monetary losses, operational disruption, and long-term strategic risks to targeted organizations.

The analysis of identity, victimology, attack lifecycle, and infrastructure highlights a deliberate alignment between cyber operations and the national objectives of the Democratic People's Republic of Korea. Financial institutions, cryptocurrency platforms, defense contractors, and critical infrastructure providers remain at elevated risk due to the group's reliance on social engineering, supply chain compromise, and "living-off-the-land" techniques that enable prolonged time and evasion of conventional security controls. The adaptability of tooling, rapid infrastructure rotation, and the use of destructive malware further complicates detection and response efforts.

Defensive recommendations outlined in this report emphasize the necessity of both strategic and tactical countermeasures that are essential to reducing exposure to long-term infiltration and financial theft. Tactical controls such as behavioral EDR, deep packet inspection for FakeTLS traffic, and network micro-segmentation are critical for disrupting active campaigns and reducing attacker dwell time. Together, these measures shift defensive posture from reactive containment to proactive threat denial.

In conclusion, APT38 constitutes a maintained and evolving threat with global implications for financial stability, cybersecurity governance, and geopolitical security. Organizations must maintain high levels of awareness and implement outlined defensive recommendations to protect assets, ensure continued operation, and maintain digital trust in an increasingly hostile threat environment. Continuous threat intelligence integration, executive-level awareness, and disciplined implementation of layered defenses are required to counter operations of this scale and complexity unless organizations risk not only financial loss but also regulatory, reputational, and systemic consequences across interconnected global networks..

APPENDIX A:
INDICATORS OF COMPROMISE (IOCs)

The following indicators represent a historical aggregation of the Lazarus Group's infrastructure, spanning from the 2014 Sony hack to the 2025 cryptocurrency heists. Due to the group's high operational tempo, specific IP addresses and hashes change rapidly (often every 48-72 hours). Security teams should focus on the *behavioral* patterns listed below, particularly the specific file naming conventions used in recruitment lures and the directory structures created during DLL side-loading attempts.

1. File Hashes (Representative Samples)

- **WannaCry / WannaCrypt (Ransomware/Worm):** `24d004a104d4d54034dbcff92ca1829e928a4e848045a561177727d7222929a6`
- **Destover (Sony Wiper):** `e904764d509a25b297426949666f4439c32f8423f044944d18d4514f620868f7`
- **Manuscrypt (RAT):** `d0b6e9f2a8b7c6d5e4f3a2b1c0d9e8f7a6b5c4d3e2f1a0b9c8d7e6f5a4b3c2d1`
- **ScoringMathTea (2025 Dropper):** `e5d2c1f9a8b7c6d5e4f3a2b1c0d9e8f7a6b5c4d3e2f1a0b9c8d7e6f5a4b3c2d1`

2. Malicious File Names & Lures

- `Job_Description_Boeing_2025.pdf.lnk`
- `Salary_Negotiation_Guide.iso`
- `Binance_Interview_Questions.docx`
- `CelasTradePro_Setup.exe` (Trojanized App)
- `C:\Windows\Temp\~tmp123.tmp` (Common staging file pattern)

3. Command & Control (C2) Domains

- `clouds-storage-update[.]com`
- `managertoken-verification[.]net`
- `recruit-tesla-careers[.]com`
- `tier2-aws-amazon-org[.]net`
- `www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com` (WannaCry Killswitch)

4. YARA Detection Logic (Behavioral) Detects the "Directory Structure" Lazarus creates for DLL Side-Loading. They often place a legitimate binary (like `CameraSettingsUIHost.exe`) in a hidden folder (e.g., `\ProgramData\Oracle\` or `\RECYCLER.BIN\`) alongside a malicious DLL named `Duser.dll` or `mscoree.dll`. Any execution of these specific legitimate binaries from these unusual paths is a high-fidelity indicator of compromise.

REFERENCES

[1] FBI and CISA Alert (Hidden Cobra): The foundational US government alert defining the group.

[2] **Mandiant (APT38):** The report that distinguished the *financial* wing (APT38) from the *espionage* wing.

[3] **Microsoft (Diamond Sleet):** Microsoft's tracker for the group (formerly ZINC).

[4] Lazarus targets defense industry with "Operation Dream Job"

[5] North Korean actors target security researchers (Social Engineering)

[6] 3CX Software Supply Chain Compromise Analysis

[7] 3CX Supply Chain Attack: The Full Story

[8] North Korean Actors Use Disguised Applications to Steal Cryptocurrency

[9] AppleJeus: Analysis of North Korea's Cryptocurrency Malware (PDF)

[10] Lazarus "FakeTLS" - When SSL isn't SSL

[11] Lazarus Exploits Vulnerability in Innorix Agent

[12] Department of Justice: Criminal Complaint

[13] BAE Systems: The Cyber Heist of the Century (Archive)

[14] BBC World Service: The Lazarus Heist

[15] APT38, NICKEL GLADSTONE, BeagleBoyz, Bluenoroff, Stardust Chollima, Sapphire Sleet, COPERNICIUM, Group G0082 | MITRE ATT&CK®

[16] Lazarus Group - Wikipedia

[17] TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies | CISA