# Lazarus Group (APT38) Explained: Timeline, TTPs, and Major Attacks

Picus Labs ⋮ ⋮ 10/18/2025


Picus Labs | 12 MIN READ

LAST UPDATED ON OCTOBER 20, 2025

Summarize with:
ChatGPT perplexity Google AI

Most cyber threat groups usually stick to a single specialty—some focus on spying, others on stealing money, and some just want to wreak havoc. Lazarus Group? They do it all. This notorious group has made a name for itself by combining espionage, sabotage, and massive financial theft into a single, formidable operation. Active since at least 2009, Lazarus has been behind some of the most talked-about cyberattacks in recent history.

Also known as APT38 or Hidden Cobra, the Lazarus Group is widely linked to North Korea, with suspected connections to its Reconnaissance General Bureau. Analysts point to repeated patterns in their operations and technical overlaps as evidence of these ties. What sets Lazarus apart is their ability to run multiple types of operations at the same time—they're not just spies, they're thieves and saboteurs too. The group first emerged focusing on regional targets like South Korea's government, defense sectors, and media outlets, but they quickly expanded to a global stage. Some of their most high-profile attacks include the hugely destructive Sony Pictures Entertainment hack in 2014—which combined data-wiping malware with public leaks for maximum effect—and, later, the SWIFT fraud attacks on banks, as seen in the Bangladesh Bank incident.

Lazarus doesn't stop there—they've touched nearly every sector imaginable, from finance and government to healthcare, media, defense, aerospace, and more recently, cryptocurrency and blockchain companies. Their technical skill is impressive, exploiting zero-day vulnerabilities in both Windows and macOS, compromising supply chains, and using multi-stage attack tools. Their malware arsenal is huge and constantly evolving, including custom RATs, wipers, ransomware like WannaCry, modular frameworks such as MATA, and tools for ATM attacks like FASTCash. Tactics range from spear-phishing and social engineering using fake recruiter profiles to watering-hole attacks and software supply chain compromises.

Globally, Lazarus has struck across Asia, the Americas, Europe, and the Middle East, often picking targets that offer the greatest strategic or financial gain. In short, Lazarus Group's seamless combination of espionage, disruption, and theft in long-term, coordinated campaigns makes them a cyber threat that governments and security researchers monitor closely around the world.

In this post, we'll dive into Lazarus' playbook, their biggest hits, and the tactics.



# History & Major Activities of Lazarus Group

- 24 November 2014 - Carried out a destructive attack on Sony Pictures Entertainment using wiper malware and public data leaks in retribution for perceived offenses.
- 5 February 2016 - Attempted to steal nearly one billion dollars using SWIFT from Bangladesh Bank, ultimately exfiltrating $81 million.
- 12 May 2017 - Launched the WannaCry ransomware campaign, causing global disruption to healthcare, critical infrastructure, and corporations.
- 2 October 2018 - CISA/FBI/Treasury published a technical alert on the FASTCash ATM cash-out campaign.
- 17 February 2021 - CISA/FBI/Treasury published a joint advisory analysing AppleJeus (trojanized crypto apps).

- 14 April 2022 - The FBI attributed the $620 million theft from the Ronin Bridge cryptocurrency platform to Lazarus operations.

# ATT&CK Mapping (TTPs) of Lazarus Group

## Tactic: Initial Access

### T1566 Spearphishing via Service

Lazarus has used spearphishing through compromised vendor/partner email chains and third-party collaboration platforms to deliver weaponized documents and installers. These lures have delivered loaders or droppers that stage backdoors such as Dtrack, MATA loaders, and components of the AppleJeus / TraderTraitor campaigns**.**

### T1189 Drive-by Compromise

Lazarus has used watering-hole and malicious/typosquat websites to push macOS/Windows installers and document-based droppers that ultimately deployed **AppleJeus** (macOS/Windows backdoor variants) and other downloaders. Reports describe fake cryptocurrency sites and malicious installers masked as trading apps.

## Tactic: Execution

### T1204.002 User Execution: Malicious File

The Lazarus crew rolled out a campaign pushing trojanized crypto trading apps—packaged as Windows MSI and macOS DMG installers—that look legitimate but carry a hidden payload. Those installers drop a stealthy, cross-platform "updater" that quietly harvests environment info, wraps it in a GIF-style envelope (starts with GIF89a), XOR-obfuscates the blob, and POSTs it to www.celasllc[.]com/checkupdate.php endpoint. The server replies with encoded blobs that updater base64-decodes and runs through an RC4 decryption, then uses the result to drop an encrypted **Fallchill** loader.

### T1047 Windows Management Instrumentation

During Operation Dream Job, the Lazarus Group copied and renamed the Windows WMI command-line utility (WMIC.exe to nvc.exe), placed it in a deceptively named folder, and created a scheduled task that periodically invoked the renamed binary to fetch and execute a remote XSL script—leveraging WMIC to gain an initial foothold and maintain persistence on the compromised host.

## Tactic: Persistence

### T1547.001 Registry Run Keys / Startup Folder

The Lazarus Group maintains its foothold on infected machines by dropping a crafty **.lnk** shortcut into the Windows Startup folder. When the system boots, that shortcut launches a DLL, passing along the exact parameters the malware needs to run.

#### T1574.001 Hijack Execution Flow: DLL

Lazarus pulled off a classic **DLL side-loading trick** by swapping out win_fw.dll — a DLL the IDA Pro installer expects to load — for a malicious drop-in. When the installer ran, Windows happily loaded the attacker's DLL from a location it checked before the real one, allowing the malicious code to download and execute a payload under the guise of a trusted process. It's a neat, dangerous example of **search-order hijacking**: legitimate software inadvertently becomes the execution vehicle for an attacker.

#### T1574.013 Hijack Execution Flow: KernelCallbackTable

In the 2022 Lazarus campaign, weaponized Word macros retrieved the process **PEB** (Process Environment Block), read the KernelCallbackTable pointer, replaced the USER32!_fnDWORD callback with a malicious WMIsAvailableOffline routine, and overwrote WMIsAvailableOffline in wmvcore.dll with base64-decoded shellcode.

## Tactic: Privilege Escalation

#### T1068 Exploitation for Privilege Escalation

Lazarus Group exploited significant vulnerabilities in Windows. Notably, CVE-2024-38193 — a zero-day in the Windows AFD.sys driver, part of WinSock — allowed the group to gain SYSTEM-level access and circumvent security defenses.

Another critical vulnerability, CVE-2024-21338, a Windows kernel flaw with a CVSS score of 7.8 (High), was also targeted. Although Microsoft later released a patch, Lazarus Group had already leveraged this flaw to escalate privileges on affected systems.

#### T1134.002 Access Token Manipulation: Create Process with Token

**KiloAlfa**, a Lazarus Group keylogger, calls WTSEnumerateSessionsA to list active Windows Terminal Services sessions and checks each session for **explorer.exe** (to filter for interactive user sessions); it then obtains the session user's token and uses CreateProcessAsUserA to launch the installed binary mscorsw.exe with the -run argument so the keylogger executes under that user's context.

## Tactic: Defense Evasion

#### T1027.002 Obfuscated Files or Information: Software Packing

Lazarus packages binaries and libraries with commercial packers (e.g., Themida) to hide code structure and signatures from static scanners and sandboxes, making detection and analysis harder during campaigns like Operation Dream Job.

#### T1027.007 Obfuscated Files or Information: Dynamic API Resolution

Lazarus implements custom hashing inside shellcode or loaders so **Windows API functions** are located at runtime rather than referenced by name, avoiding simple string-based detection and complicating reverse engineering.

#### T1027.009 Obfuscated Files or Information: Embedded Payloads

Lazarus has concealed executable payloads inside benign-format files (for example, embedding malicious binaries or scripts inside PNG files) so that casual inspection appears innocuous and some bypass content checks.

#### T1027.013 Obfuscated Files or Information: Encrypted/Encoded File

Lazarus has used symmetric ciphers (AES), stream ciphers (RC4), simple XOR, Caracachs encryption, Base64 encoding, and aliasing of native APIs to encode or encrypt payloads and configuration data; during Operation Dream Job, they used XOR for DRATzarus malware and Base64-encoded DLLs to further frustrate analysis.

## Tactic: Lateral Movement

#### T1021.001 Remote Services: Remote Desktop Protocol (RDP)

Lazarus leverages Remote Desktop Protocol (RDP) connections and credentials to move laterally and propagate across compromised Windows hosts. For instance, SierraCharlie, which is Lazarus Group malware, uses RDP to propagate. The code below runs Microsoft's Remote Desktop client (mstsc.exe) to initiate a remote desktop session to the specified host or IP using the provided username and password.

```
mstsc.exe /v:{hostname/ip} /u:{user} /p:{password}
```

## Tactic: Collection

#### T1074 Data Staged

Collected files and credential caches were staged locally using custom scripts in attacks before exfiltration to minimize the number of external connections to their command-and-control server. This reduces the risk of triggering alerts from security systems that monitor for high volumes of small, suspicious outbound connections.

## Tactic: Command and Control

### T1095 Non-Application Layer Protocol

Cyber adversaries often exploit OSI protocols outside the application layer to facilitate communication, either between compromised hosts and their command-and-control (C2) servers or among infected devices within a network. A notable example is the Lazarus Group, which has deployed a backdoor malware known as Cryptoistic, developed in Swift. This malware is capable of leveraging TCP for its communications with C2 infrastructure.

The **IndiaIndia** malware used by the Lazarus Group writes harvested victim data to the **%**TEMP**%**folder, compresses and encrypts the file, and uploads it to a command-and-control (C2) server.

## Tactic: Exfiltration

### T1048.003 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol

The Lazarus Group's SierraBravo-Two malware has been observed generating email messages via SMTP to transmit details about newly infected victims. This functionality allows threat actors to efficiently track and manage compromised systems.

### T1041 Exfiltration Over C2 Channel

Lazarus implants in the HaoBao campaign opened HTTP-based C2 channels, contacting hardcoded IPs/domains (e.g., worker[.]co[.]kr and palgong-cc[.]co[.]kr) and issuing HTTP POST requests to specific paths to communicate with their servers.

Before sending, the malware XOR-encoded the collected host data with key 0x34, base64-encoded the result, and placed the encoded computer\username and the encoded process list/registry flag into POST parameters (no and mode) so the server could receive staged exfiltration.

### T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

During Operation Dream Job, the Lazarus Group archived stolen data into a RAR file and exfiltrated it to Dropbox using a custom build of the open-source command-line client dbxcli. Because many enterprise hosts routinely communicate with such cloud platforms, routing stolen data through them can substantially obscure an adversary's activity within normal network traffic.

## Tactic: Impact

### T1486 Data Encrypted for Impact

In the WannaCry and TFlower ransomware campaigns, Lazarus encrypted user data at scale, disrupting hospital, enterprise, and government operations globally.

The infamous WannaCry ransomware exploited a critical Windows vulnerability known as EternalBlue, which specifically targets the SMBv1 (Server Message Block) protocol. Originally developed by the NSA and later leaked by the Shadow Brokers group, EternalBlue enabled WannaCry to infiltrate systems with alarming efficiency. The ransomware encrypts a broad range of file types—including documents, images, videos, and databases—using AES (Advanced Encryption Standard) for the files themselves and RSA to secure the AES encryption key. After the encryption process is complete, victims are confronted with a ransom note demanding payment in Bitcoin.

TFloweris a ransomware variant first identified in August 2019, designed to target and compromise corporate networks.

It's manually triggered post-compromise, displays a live encryption console, deletes shadow copies, disables Windows repair, and terminates Outlook to encrypt mail files.

Instead of changing file extensions, it prepends "*tflower" and an encrypted key to affected files, while sending status updates to a hard-coded C2 server.

**T1561.001 Disk Wipe: Disk Content Wipe**

Lazarus Group's wipe tools target critical regions efficiently: WhiskeyAlfa first overwrites the initial 64MB of a drive (then hits logical drives and may try full-drive wipes), WhiskeyBravo targets the first 4.9MB, and WhiskeyDelta overwrites the first 132MB or 1.5MB of each drive with random data from heap memory.

By corrupting the drive's initial sectors—MBR, partition tables, and filesystem metadata—the malware can render a system unbootable or inaccessible without erasing every byte, and targeting only those key regions lets it inflict maximum damage quickly while reducing time on target.

## How Picus Simulates Lazarus Group Attacks?

We also strongly suggest simulating Lazarus Group Attacks to test the effectiveness of your security controls against real-life cyber attacks using the Picus Security Validation Platform. You can also test your defenses against hundreds of other threat groups within minutes with a 14-day free trial of the Picus Platform.

Picus Threat Library includes the following threats for the Lazarus Group:

| Threat ID | Threat Name | Attack Module |
|---|---|---|
| 48451 | KANDYKORN Malware Campaign | macOS Endpoint |
| 22472 | AppleJeus Campaign HOPLIGHT Malware Download Threat | Network Infiltration |
| 23413 | Lazarus Threat Group Campaign Malware Download Threat - 1 | Network Infiltration |
| 24171 | Lazarus Threat Group Campaign Malware Email Threat - 1 | Network Infiltration |
| 29951 | Lazarus Threat Group Campaign Backdoor Malware Email Threat | Network Infiltration |
| 32137 | Lazarus Threat Group Campaign Malware Email Threat - 2 | Network Infiltration |
| 33197 | Lazarus Group Threat Group Campaign Malware Email Threat | Network Infiltration |
| 37880 | PowerRatankba Malware Campaign | Windows Endpoint |

| | | |
|---|---|---|
| 44487 | Lazarus Threat Group Campaign Malware Email Threat - 3 | Network Infiltration |
| 60215 | Lazarus Threat Group Ghostscript Exploit Vulnerability .HWP Threat | Network Infiltration |
| 63011 | Lazarus Threat Group Campaign Malware Download Threat - 2 | Network Infiltration |
| 64763 | Lazarus Threat Group Campaign RAT Download Threat | Network Infiltration |
| 65515 | Lazarus Threat Group Microsoft Office Malware Downloader Threat | Network Infiltration |
| 73886 | Lazarus Threat Group Campaign Malware Email Threat - 4 | Network Infiltration |
| 79230 | Lazarus Threat Group Campaign Backdoor Malware Download Threat | Network Infiltration |
| 79291 | AppleJeus Campaign HOPLIGHT Malware Email Threat | Network Infiltration |
| 81051 | Lazarus Group Threat Group Campaign Malware Download Threat | Network Infiltration |
| 81835 | Lazarus Threat Group Campaign | Windows Endpoint |
| 86305 | Lazarus Threat Group Campaign Malware Download Threat - 4 | Network Infiltration |
| 87206 | Lazarus Threat Group Campaign RAT Email Threat | Network Infiltration |
| 87866 | Lazarus Threat Group Campaign Malware Download Threat - 3 | Network Infiltration |
| 88061 | Lazarus Threat Group Ghostscript Exploit Vulnerability .DLL Threat | Network Infiltration |
| 95078 | Lazarus Threat Group Campaign Downloader Download Threat | Network Infiltration |
| 96175 | Lazarus RATs Malware Campaign | Windows Endpoint |
| 98305 | Lazarus Threat Group Campaign Downloader Email Threat | Network Infiltration |

Start simulating emerging threats today and get actionable mitigation insights with a 14-day free trial of the Picus Platform.

## Aliases of Lazarus Group

Lazarus group is also known as**:** Labyrinth Chollima, HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY, Diamond Sleet, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Citrine Sleet, Jade Sleet, TraderTraitor, Gleaming Pisces, Slow Pisces, Operation DarkSeoul, Dark Seoul, Hidden Cobra, Andariel, Unit 121, Bureau 121, Bluenoroff, Subgroup: Bluenoroff, Operation Troy, Operation GhostSecret, Operation AppleJeus, APT38, APT 38, Stardust Chollima, Zinc, Nickel Academy, NICKEL GLADSTONE, COVELLITE, ATK3, G0032, ATK117, G0082, DEV-1222, Sapphire Sleet, COPERNICIUM, Lazarus group, BeagleBoyz, Moonstone Sleet, Lazarus, Genie Spider.