DISC INFOSEC

BOOK A THREAT BRIEFING

THREAT INTELLIGENCE MITRE ATT&CK · G0032 READ · 11 MIN

The adversary that treats your *balance sheet* as the objective.

Most nation-state groups want your secrets. Lazarus Group wants your money — and in 2025 it took a billion and a half dollars in a single afternoon. Here is the defender's map.

BY HUGH DEURA, DISC INFOSEC · UPDATED JULY 2026

Lazarus Group

ACTOR PROFILE · V2026.07

ATTRIBUTION

North Korea (DPRK), Reconnaissance General Bureau. State-sponsored, active since ≥2009.

MOTIVATION

Revenue generation for a sanctioned state. Financial theft first; espionage and disruption second.

SUBUNITS

APT38 (financial), TraderTraitor, Bluenoroff, Andariel.

PRIMARY TARGETS

Crypto exchanges & DeFi, banks, fintech, and the SaaS & developer

supply chains that serve them.

$6.75B

DPRK-LINKED CRYPTO STOLEN, 2019–2025 (CHAINALYSIS)

$2.02B

TAKEN IN 2025 ALONE — A RECORD YEAR

$1.5B

SINGLE BYBIT HEIST, FEB 2025 — LARGEST EVER

76%

OF GLOBAL CRYPTO-HACK LOSSES IN EARLY 2026 (TRM LABS)

WHY THIS ONE IS DIFFERENT

When the money *is* the mission

Threat modeling usually starts with the question: *what would an attacker want to steal or break?* With Lazarus, the answer collapses to a single line item — cash, moved off your books and onto Pyongyang's. That clarity changes how you defend.

An espionage actor can afford to sit quietly and exfiltrate slowly. A financially-motivated state actor optimizes for one irreversible moment: the transaction that moves value out the door. Former FBI analysts now describe

Lazarus as an industrial-scale operation with specialization, pipelines, multi-year planning, and a laundering infrastructure that has survived three rounds of U.S. sanctions. This is not a smash-and-grab. It is a business unit with a budget.

For DISC InfoSec's clients — B2B SaaS and financial-services firms — that reframing matters. You are not only a potential victim; you are potential **infrastructure**. If your software sits in a fintech supply chain, or your engineers hold keys to systems that move money, you are on the map whether or not you hold the assets yourself.

> **Crypto is the near-perfect target: settlement is final in minutes, liquidity is deep, and cross-chain rails move value faster than any enforcement body can freeze it. For a state weighing a bank heist against a bridge heist, the bridge wins every time.**

ATTRIBUTION, DONE RIGHT

Know exactly who you're tracking

Lazarus is tracked under a sprawl of vendor aliases. Getting them straight is not pedantry — it is how you correlate intelligence across sources without double-counting or misattributing. Here's the working map.

US-CERT / CISA	HIDDEN COBRA
MICROSOFT	Diamond Sleet (formerly ZINC), Jade Sleet

CROWDSTRIKE	Labyrinth Chollima
MANDIANT	APT38 — the financially-motivated subgroup
FBI (CRYPTO OPS)	TraderTraitor
OTHER / HISTORICAL	Guardians of Peace, Whois Team, Slow Pisces, APT-C-26
MITRE ATT&CK	Group ID G0032

✕ COMMON MISLABEL — REJECT IT

If a feed or report calls Lazarus **"APT34"**, discard the source's attribution. APT34 is **OilRig** — an Iranian actor, entirely unrelated. "PlayStation Crew" is not a recognized alias either. These errors travel through AI-generated summaries; verify against MITRE G0032 and CISA advisories before you act on anyone's mapping.

ANATOMY OF A $1.5B HEIST

Bybit, February 2025

The largest cryptocurrency theft on record wasn't a smart-contract bug or a brute-forced key. It was a patient human-and-supply-chain operation that turned the industry's "gold standard" multi-signature cold wallet into the delivery mechanism. The FBI attributed it to Lazarus (TraderTraitor) within days.

01

Compromise a developer, not the exchange

Attackers gained control of a developer's machine at Safe{Wallet} — the multi-sig platform Bybit relied on — through social engineering rather than a direct breach of the exchange.

`T1566 Spearphishing · T1195 Supply-chain compromise`

02

Poison the front end

During a routine update, malicious JavaScript was injected into the Safe{Wallet} web application hosted on cloud storage, scoped specifically to intercept and rewrite Bybit's transaction flow.

`T1059.007 JavaScript · T1584 Compromised infrastructure`

03

Turn the signers into the exploit

Bybit's multi-sig approvers saw a legitimate-looking transaction and signed it. The tampered interface meant they were authorizing a transfer to attacker-controlled addresses — the humans became the vulnerability.

`T1565 Data manipulation · Business-logic abuse`

04

Pivot into the cloud

Investigators later documented stolen session tokens used to reach cloud resources and an attempt to register a fraudulent MFA device — extending control beyond the initial foothold.

`T1550 Use of stolen tokens · T1556 MFA manipulation`

05

Move ~400,000 ETH, then erase the trail

Roughly $1.5B in ETH and stETH moved to DPRK-linked accounts. The injected payload was removed immediately to frustrate forensics, and funds were dispersed across thousands of addresses.

`T1070 Indicator removal · T1486-adjacent impact`

> The exchange was never "hacked" in the way headlines imply. A developer was, a front end was, and a group of trusted signers were. Every control that failed here lives upstream of the vault.

THE KILL-CHAIN, MAPPED

TTPs → detection → mitigation

The techniques below trace a Lazarus intrusion end to end, drawn from the DISC InfoSec Lazarus TTP mapping (aligned to MITRE ATT&CK G0032). Each phase pairs how you see it with how you stop it. Scroll to trace the path.

Initial Access T1190 T1566

DETECT

WAF anomalies and unexpected process creation under web-server accounts (exploited public apps); mail-gateway anomalies, macro-enabled attachments, LNK/ISO containers, and first-seen sender domains (spearphishing — including fake-recruiter lures).

MITIGATE

Rigorous patch management, WAF and input validation, minimized internet-facing surface; attachment sandboxing, macro blocking, DMARC/DKIM/SPF, and targeted awareness training for engineering and finance staff.

Execution T1059.001

DETECT

PowerShell script-block (Event ID 4104) and module logging (4103). Flag encoded commands (`-enc`), execution-policy bypass (`-ep bypass`), and download cradles (`IEX`, `Invoke-WebRequest`).

MITIGATE

Constrained Language Mode, restricted execution policy, mandatory script-block logging, and application allow-listing via AppLocker or WDAC.

Persistence T1053 T1543.003 T1547.001

DETECT

Scheduled tasks, new services, and registry Run-key entries created shortly after a suspicious first access — correlate creation events against the initial-access timeline rather than reviewing them in isolation.

MITIGATE

Baseline autoruns and services, alert on deviations, restrict who can create services/tasks, and enforce least privilege on endpoints.

Command & Control T1071.001

DETECT

Beaconing patterns, anomalous user-agents, high-volume single-domain connections, and DNS-over-HTTPS to non-corporate resolvers.

MITIGATE

IDS/IPS and WAF, egress filtering, TLS inspection where policy allows, and control of DoH on managed endpoints.

Lateral Movement T1021.001 T1550

DETECT

RDP logons (Event ID 4624, Logon Type 10) from unusual source IPs or off-hours; and — as Bybit showed — stolen session tokens reaching cloud resources plus rogue MFA-device registration.

MITIGATE

Restrict RDP, require phishing-resistant MFA, use jump/bastion hosts, segment the network, and alert on new MFA enrollments and impossible-travel token use.

Impact T1486 T1565

DETECT

For destructive ops: mass file-modification bursts, shadow-copy deletion (`vssadmin delete shadows`), and recovery tampering (`bcdedit`). For financial ops: out-of-band verification gaps at the moment of value transfer.

MITIGATE

Offline/immutable backups, segmentation, EDR with rollback, canary files — and independent, out-of-band confirmation of any transaction that moves material value.

⚠ IMPACT CAVEAT — DO NOT ASSUME RECOVERY

Lazarus has a documented history of deploying wipers disguised as ransomware. When you see an encryption event, treat recoverability as unproven: validate your backups *before* you assume a decryption path exists, because sometimes destruction — not extortion — was the point.

THE 2025–2026 SHIFT

The interview is the intrusion

The most important change in Lazarus tradecraft has nothing to do with malware. It's a hiring funnel run in reverse.

Through 2024 and into 2026, the group pivoted hard toward social engineering aimed at **engineers and executives**: fake recruiters and "investors" open a conversation, then introduce a staged technical challenge, a "portfolio-company" diligence call, or a coding test that quietly delivers malware onto a developer's machine. In the Drift Protocol case, post-mortems describe months of manufactured investor-diligence conversations that extracted pre-signed admin-key authorizations from multiple engineers. In April 2026, the Zerion incident showed AI-enabled social engineering used to capture live sessions, credentials, and private keys.

Parallel to this runs the North Korean **IT-worker scheme** — operatives securing legitimate remote engineering jobs under false identities, turning the hiring pipeline itself into an access vector. Two U.S. nationals were sentenced in 2026 for facilitating it.

> **Every engineer who clicks a "portfolio-company interview" calendar invite, every unrotated admin key, every skipped identity check in hiring becomes — in a literal sense — a line item in a sanctioned state's revenue model.**

For SaaS and fintech teams the implication is uncomfortable but clear: your **recruiting, contractor onboarding, and developer endpoint controls are now part of your threat surface**, on equal footing with your production perimeter.

TRAJECTORY

A decade of escalation

Fewer incidents each year, larger every time. The through-line is a state actor scaling alongside the industry it targets.

2014 — **Sony Pictures**
Destructive wiper under the "Guardians of Peace" persona — the group announces itself with disruption, not theft.

2016 — **Bangladesh Bank / SWIFT**
Fraudulent SWIFT transfers drain roughly $81M — the pivot to financial theft via APT38.

2017 — **WannaCry**
Ransomware worm propagating over SMB via the EternalBlue exploit; global, indiscriminate impact.

2022 — **Ronin Bridge**
Roughly $624M stolen from the Axie Infinity bridge — attributed by U.S. Treasury and FBI. The DeFi era begins.

2025 — **Bybit**
~$1.5B via a Safe{Wallet} supply-chain compromise — the largest crypto heist ever recorded.

2026 — **Kelp DAO & Drift**
Back-to-back nine-figure DeFi exploits (~$290M and ~$285M) via off-chain infrastructure and social-engineered admin keys.

WHAT DEFENDERS SHOULD ACTUALLY DO

Hunt hypotheses worth running this quarter

Detection lists age quickly against this actor. Hypotheses age better. Start here, then tailor to your telemetry.

H1 **New MFA device + token reuse.** Hunt for MFA-device registrations closely followed by session-token use from a new ASN or geography. The Bybit cloud pivot lived in exactly this gap.

H2 **Developer endpoints talking to first-seen domains after a recruiter contact.** Correlate HR/recruiting activity and calendar invites with fresh outbound C2-style beaconing from engineering laptops.

H3 **Unexpected front-end / build-artifact changes.** Diff deployed web assets against source of truth; alert on JavaScript introduced outside the release pipeline.

H4 **High-value transactions without out-of-band confirmation.** Treat any value transfer approved solely through a UI as suspect; require an independent channel to confirm destination.

H5 **Pre-signed or long-lived admin authorizations.** Inventory standing admin keys and pre-signed approvals; each one is a Drift-style extraction target.

The highest-leverage control against this actor is unglamorous: **centralized, retained, and reviewed audit logs** (CIS Controls v8, Control 8). You cannot hunt what you never recorded. Governance frameworks make it durable — ISO 27001 for the security management system, ISO 42001 where AI is now part of both the attack and the defense, and NIST SP 800-61 to make sure the response is rehearsed before the wiper lands, not improvised after.

SOURCES & INTELLIGENCE NOTE

Technique mapping aligned to MITRE ATT&CK Group G0032 and CISA HIDDEN COBRA advisories. Campaign details and figures drawn from public reporting and investigations by the FBI, Chainalysis, TRM Labs, and Sygnia, and from protocol post-mortems (LayerZero / Kelp DAO, Drift Protocol). This actor rotates tooling frequently and attributions evolve — figures are subject to revision as investigations

continue. Verify against primary sources before operational use. This article is defensive threat intelligence intended for detection, hunting, and response.

DISC InfoSec

DEURA INFORMATION SECURITY CONSULTING LLC · PETALUMA, CA