INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-21 06:38 UTC

Lazarus Group's DVN Poisoning Attack: How $290M Left KelpDAO Through Falsified Cross-Chain Consensus

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0190
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	KelpDAO (rsETH token), LayerZero DVN/RPC infrastructure, Compound, Euler, Aave, Unichain
Published	2026-04-20T18:23:52
Discovery Source	Rss

Executive Summary

On April 18, 2026, North Korean state-sponsored actors attributed to Lazarus Group's TraderTraitor cluster stole approximately $290 million from KelpDAO by compromising RPC nodes within LayerZero's Decentralized Verifier Network, injecting falsified cross-chain messages that the protocol accepted as legitimate. A critical single-node DVN configuration in KelpDAO's rsETH implementation meant one compromised verifier was sufficient to bypass all on-chain validation. This incident, linked to concurrent activity from the same threat group targeting Drift Protocol ($280 million), signals systematic nation-state operations against decentralized finance infrastructure at the cross-chain verification layer, a control gap not addressed by standard smart contract audits.

Technical Analysis

Attack vector: Lazarus Group (TraderTraitor cluster) compromised RPC nodes within LayerZero's Decentralized Verifier Network (DVN), then injected falsified cross-chain messages that were accepted as valid by the rsETH protocol bridge. Root cause misconfiguration: KelpDAO's rsETH relied on a 1-of-1 single DVN setup (CWE-1188, insecure default initialization), meaning compromise of one verification node bypassed the entire validation chain. This is an off-chain infrastructure attack; it circumvented smart contract logic entirely, rendering prior on-chain audits insufficient.

Weaknesses exploited: CWE-940 (Improper Verification of Source of a Communication Channel), CWE-345 (Insufficient Verification of Data Authenticity), CWE-693 (Protection Mechanism Failure), CWE-1188 (Insecure

Default Initialization).

MITRE ATT&CK techniques observed: T1584 (Compromise Infrastructure, RPC node compromise), T1565.002 (Transmitted Data Manipulation, falsified cross-chain messages), T1498 (Network Denial of Service, suspected DDoS of healthy RPC nodes to isolate compromised node), T1027 (Obfuscated Files or Information, Tornado Cash laundering), T1496 (Resource Hijacking, unauthorized rsETH minting/transfer), T1199 (Trusted Relationship, abuse of LayerZero DVN trust model).

Post-exploitation: Funds moved through Tornado Cash. LayerZero threat intelligence and post-incident analysis corroborate the DVN/RPC attack chain. No CVE identifier is currently assigned. No patch is available for retroactive loss recovery; remediation is architectural. Affected scope: KelpDAO rsETH token, LayerZero DVN/RPC infrastructure, with downstream exposure to integrated protocols including Compound, Euler, Aave, and Unichain.

Action Checklist

1. Step 1: Containment. If your protocol integrates LayerZero for cross-chain messaging, immediately audit your DVN configuration. Identify any 1-of-1 single DVN setups and temporarily suspend cross-chain message acceptance from those channels until multi-DVN thresholds are enforced. Contact LayerZero support to confirm your current DVN configuration status.
2. Step 2: Detection. Review cross-chain message logs for anomalous minting events, unexpected token transfers, or message source inconsistencies originating from LayerZero DVN endpoints. Monitor for RPC node substitution or unexpected changes in verifier node identity. If you custody rsETH or interact with KelpDAO bridges, audit all cross-chain transactions from April 18, 2026 onward for unauthorized minting or transfer events. Flag Tornado Cash-linked wallet addresses in your transaction monitoring pipeline.
3. Step 3: Eradication. Migrate any LayerZero-integrated deployment from 1-of-1 single DVN configurations to a multi-DVN threshold model (minimum 2-of-3 independent verifiers recommended). Rotate RPC node credentials and endpoints. Verify RPC node integrity through independent out-of-band channels. Contact LayerZero support for current DVN configuration best practices and post-incident remediation guidance.
4. Step 4: Recovery. After reconfiguring DVN thresholds, validate that cross-chain message acceptance requires multi-node consensus before resuming bridge operations. Monitor all subsequent cross-chain transactions for anomalous minting or transfer patterns for a minimum of 30 days. Confirm with LayerZero that your DVN endpoints have not been previously substituted or tampered with.
5. Step 5: Post-Incident. Expand smart contract audit scope to explicitly cover off-chain infrastructure dependencies including DVN configurations, RPC node trust models, and cross-chain oracle assumptions. Add DVN configuration review to your DeFi integration security checklist. Implement on-chain circuit breakers for large minting or transfer events. Evaluate whether your bridge architecture assumes trusted off-chain components that lack independent verification; this incident demonstrates that nation-state actors are specifically targeting that assumption.

Detection Guidance

Organizations using LayerZero for cross-chain messaging should focus detection on the off-chain verification layer, not smart contract events alone. Key indicators: (1) Unexpected or anomalous rsETH minting events on any chain where KelpDAO rsETH is deployed; cross-reference minting volume against corresponding deposit

events - discrepancies indicate falsified messages were accepted. (2) RPC node identity changes; monitor for substitution of known-good RPC endpoints with unrecognized nodes in your LayerZero DVN configuration. (3) Cross-chain messages accepted from a single DVN verifier where multi-verifier consensus was expected; log DVN verifier signatures on accepted messages and alert on single-signature acceptance. (4) Large outbound transfers to Tornado Cash-linked addresses (on-chain mixer contract addresses are publicly documented); integrate these into your blockchain transaction monitoring rules. (5) Behavioral indicator: DDoS activity targeting specific RPC nodes immediately preceding unusual cross-chain message acceptance may indicate an attempt to isolate a compromised node (MITRE T1498) - correlate RPC node availability logs with cross-chain transaction timestamps. No authoritative public IOC list (specific IP addresses, C2 domains, or file hashes) has been published by threat intelligence vendors or law enforcement as of April 20, 2026. Tornado Cash wallet addresses remain the primary available IoC; integrate documented mixer contract addresses into transaction monitoring rules.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Tornado Cash mixer contract addresses (publicly documented on-chain)`	Post-exploitation laundering — funds from KelpDAO theft routed through Tornado Cash; specific contract addresses not confirmed in available sources	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1498** — Network Denial of Service
- **T1027** — Obfuscated Files or Information
- **T1565.002** — Transmitted Data Manipulation
- **T1584** — Compromise Infrastructure
- **T1020** — Automated Exfiltration
- **T1583.006** — Web Services
- **T1557** — Adversary-in-the-Middle
- **T1486** — Data Encrypted for Impact
- **T1496** — Resource Hijacking
- **T1036** — Masquerading
- **T1195** — Supply Chain Compromise
- **T1199** — Trusted Relationship

NIST-800-53R5

- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CP-9** — System Backup

- **CP-10** — System Recovery and Reconstitution
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5** — Allowlist Authorized Software

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1498	Network Denial of Service	Impact
T1027	Obfuscated Files or Information	Defense-Evasion
T1565.002	Transmitted Data Manipulation	Impact
T1584	Compromise Infrastructure	Resource-Development
T1020	Automated Exfiltration	Exfiltration
T1583.006	Web Services	Resource-Development
T1557	Adversary-in-the-Middle	Credential-Access
T1486	Data Encrypted for Impact	Impact
T1496	Resource Hijacking	Impact
T1036	Masquerading	Defense-Evasion
T1195	Supply Chain Compromise	Initial-Access
T1199	Trusted Relationship	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/kelpdao-suffers-290-...	T3

Source	URL	Tier
An open-source AI tool no one was watching flagged a $292 million ...	https://www.techflowpost.com/en-US/article/31202	T3
Kelp DAO claims LayerZero's 'default' settings are what ... - CoinDesk	https://www.coindesk.com/tech/2026/04/20/kelp-dao-claims-layerzero-...	T3
LayerZero Post Mortem Shows Lazarus Group Stole $290M From ...	https://thedefiant.io/news/hacks/lazarus-kelpdao-290m-layerzero-rpc...	T3
KelpDAO rsETH was configured with a 1-of-1 single DVN setup ...	https://x.com/GoPlusSecurity/status/2046129954187002037	T3

Generated 2026-04-21 06:38 UTC by TJS Security Command Center