CERTIK
SKYNET

Skynet DPRK Crypto Threats Report

North Korea has industrialized cryptocurrency theft into a primary state revenue mechanism. Between 2016 and early 2026, DPRK-linked threat actors have stolen an estimated $6.75 billion across 263 documented incidents according to independent on-chain researcher Taylor Monahan.

Executive Summary

Note that all figures cited in this report are approximations and are subject to revision as investigations progress and new incidents are disclosed.

North Korea has industrialized cryptocurrency theft into a primary state revenue mechanism. Between 2016 and early 2026, DPRK-linked threat actors have stolen an estimated **$6.75 billion** across **263 documented incidents** according to independent on-chain researcher Taylor Monahan. The discrepancy itself is revealing: hundreds of smaller thefts targeting individuals, founders, and small protocols go uncounted in mainstream reporting.

In 2025, the broader crypto ecosystem recorded **656 security incidents** resulting in **$3.4 billion** in total losses. Of those, **79** were attributed to DPRK-linked actors, accounting for **$2.06 billion**, approximately **60%** of all value stolen despite representing only **12%** of total incidents. This disproportionate ratio underscores the precision and scale of North Korean operations: fewer attacks, but systematically targeting the highest-value opportunities. The February 2025 Bybit heist alone accounted for **$1.5 billion**, making it the single largest cryptocurrency theft in history. This trend is continuing into 2026.

From the first January 2026, **185 incidents** resulted in **~$1.1 billion** in total losses across the ecosystem. Of that amount, **~$620.9 million** was attributed to DPRK, representing **55%** of global losses and driven primarily by the **$291 million** KelpDAO exploit.

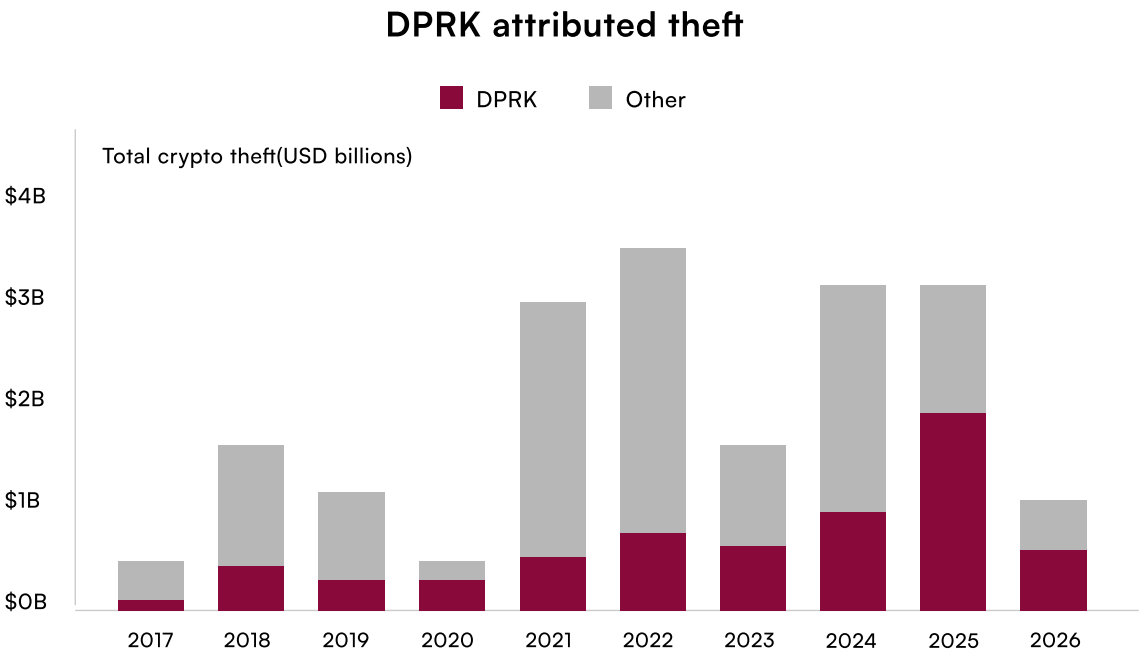


Figure 1: DPRK Attributed Theft vs Global Crypto Theft

This report provides a comprehensive technical analysis of three landmark DPRK operations: the 2022 Ronin Bridge exploit ($625 million), the 2025 Bybit heist ($1.5 billion) and the Drift Protocol attack ($285M). Together, these three incidents account for over $2.4 billion in losses

and illustrate the evolution of DPRK cyber capabilities from basic hot wallet compromises to sophisticated supply chain attacks targeting institutional-grade infrastructure.

The trajectory is clear: increasingly high-value operations, an industrialized laundering pipeline, and a massive long tail of smaller thefts that collectively rival the mega-hacks in total value. DPRK actors have consistently targeted humans and supply chain weaknesses rather than smart contract code vulnerabilities. Across nearly a decade of operations, their primary attack vector has rarely been code. It has almost always been people.

Key Takeaways

Social engineering is the dominant attack vector. From the Ronin Bridge fake LinkedIn job offer to the Bybit Safe Wallet developer compromise, most of the major DPRK heist begins with human manipulation. Fake VC impersonation, fraudulent job interviews, and malicious code repositories account for the majority of initial access across all clusters.

Supply chain attacks, the DPRK signature. The Bybit hack demonstrated that institutional-grade multisig cold wallets can be compromised when third-party infrastructure is targeted. The attackers never broke the smart contract; they broke the UI that signers trusted.

DPRK laundering infrastructure has reached industrial scale. Within one month of the Bybit hack, 86.29% of stolen ETH had been converted to Bitcoin. The pipeline leverages mixing services, cross-chain bridges, DEXs, and OTC brokers.

Crypto theft directly funds weapons of mass destruction. UN monitors and US intelligence assessments confirm that cryptocurrency theft revenue supports North Korea's nuclear and ballistic missile programs.

The threat is expanding through IT worker infiltration. For years, DPRK agents have infiltrated numerous DeFi protocols under false identities, operating as trusted insiders while feeding intelligence to state-sponsored hacking units. In several documented cases, these operatives have directly facilitated the theft of funds from the very organizations that employed them.

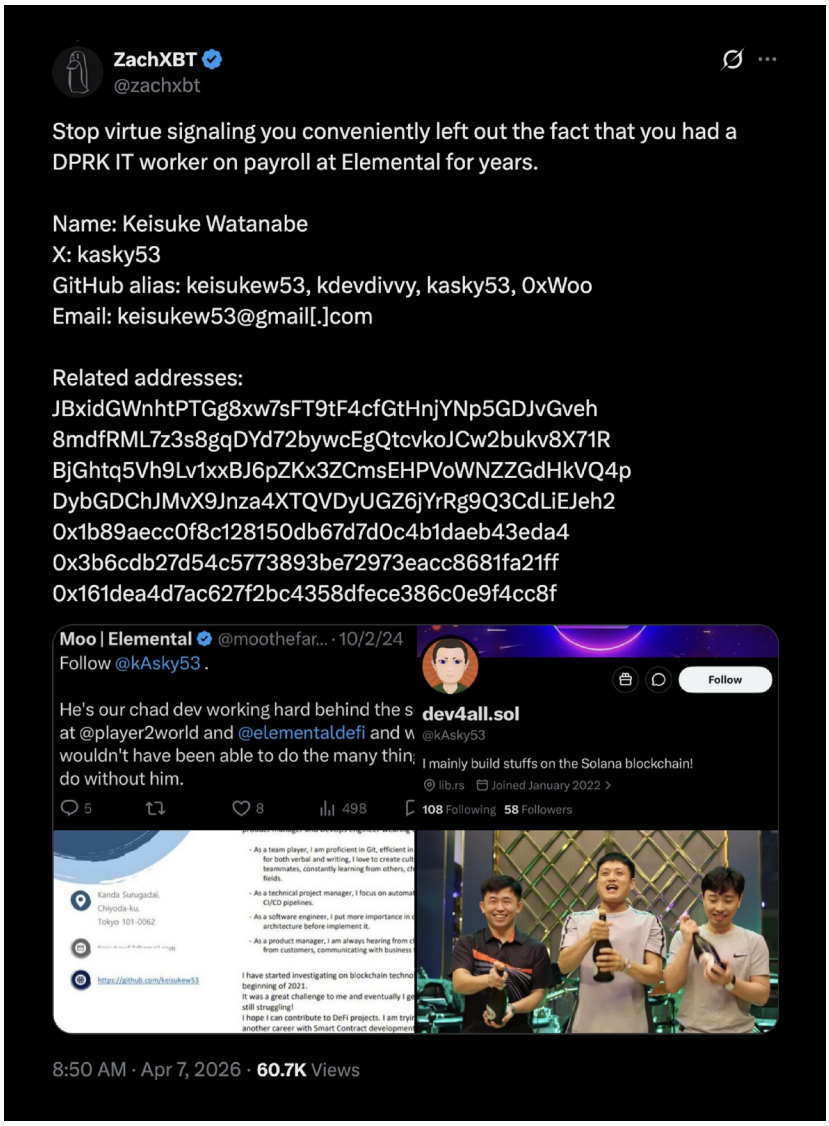


Figure 2: Tweet originating from ZachXBT account

The Strategic Context

International sanctions have severely constrained North Korea's access to foreign currency and international financial systems since the regime's first nuclear test in 2006. The UN Security Council has imposed progressively tighter restrictions on North Korean exports, banking relationships, and trade partnerships. By 2017, North Korea's export revenue had collapsed. The regime needed an alternative revenue stream that could bypass the international financial system entirely.

Cryptocurrency provided exactly that. Digital assets can be stolen remotely, moved across borders without intermediaries, and converted to fiat through networks of complicit or unwitting brokers.

US and UN officials now openly state that crypto theft has become a key funding source for North Korea's weapons of mass destruction programs. Open-source estimates suggest that cumulative DPRK crypto theft since 2017 represents a substantial share of the regime's external revenue. The connection between a compromised DeFi protocol and a ballistic missile test may seem abstract, but intelligence assessments confirm it is direct.

"Cyberwarfare is an all-purpose sword that guarantees the North Korean People's Armed Forces ruthless striking capability, along with nuclear weapons and missiles." — Kim Jong-un

DPRK cyber actors are not financially motivated criminals seeking personal enrichment. They are state employees executing a strategic mandate with the full backing of a nuclear-armed government. Their persistence, resources, and willingness to invest months in a single operation reflect institutional incentives that no criminal enterprise can match.

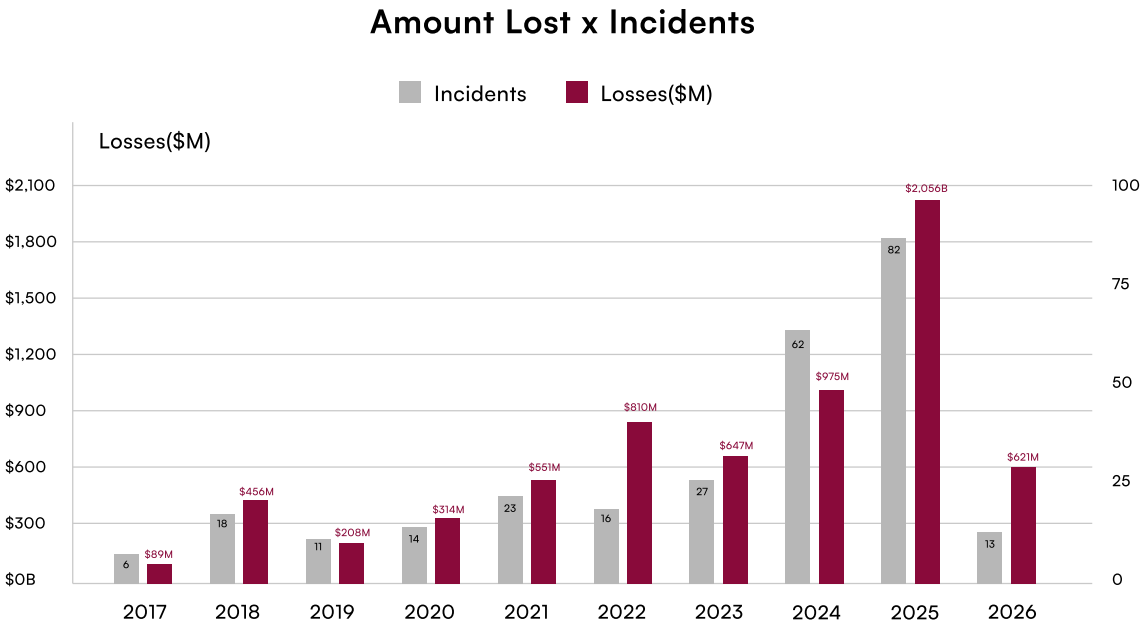


Figure 3: Amount Lost x Incident related to DPRK

Organizational Structure

The Lazarus Group is an umbrella designation encompassing multiple North Korean cyber units operating under the Reconnaissance General Bureau (RGB), Pyongyang's primary foreign intelligence service. The US Army estimates approximately 7,000 personnel across the various cyber units. They are described as extreme workaholics, typically starting at midnight UTC and working at least 15-hour days, six days a week.

Understanding the internal structure of DPRK cyber operations is critical because different clusters use different TTPs, different malware, different laundering infrastructure, and target different victim profiles. One of the most recent documents which provides a comprehensive breakdown of this organization is the DTEX system report.

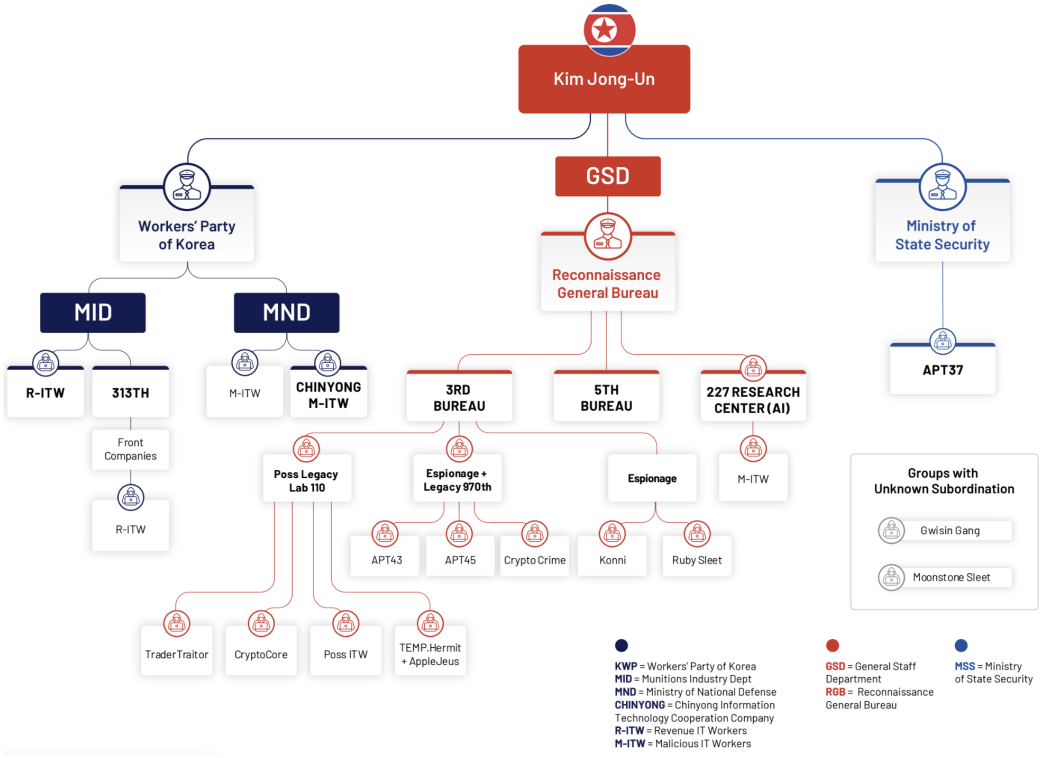


Figure 4: DPRK organization chart

Cluster Taxonomy

The following taxonomy reflects the current understanding of DPRK operational clusters as tracked by Mandiant, Microsoft, Palo Alto, and independent researchers:

SquidSquad

Also known as: Sapphire Sleet, DangerousPassword, CryptoCore, APT38, BlueNoroff, Alluring Pisces, Leery Turtle, SnatchCrypto, CryptoMimic, UNC1069, Black Alicanto, CageyChameleon.

This is one the most prolific clusters by incident count. SquidSquad specializes in impersonating venture capitalists, investors, and business partners to target crypto founders, executives, and high-net-worth individuals. Their typical approach involves initial contact via Telegram or LinkedIn, followed by a shared Google Drive link or PDF containing malware. Common lure documents include fake investment theses, stablecoin risk assessments, and meeting agendas.

- **Primary malware:** RustBucket, SwiftBucket, NimDoor (macOS), AppleScript-based payloads.
- **Laundering:** Tornado Cash, eXch, Noones, Paxful, dust collectors.

TraderTraitor

Also known as: Jade Sleet, Slow Pisces, UNC4899

Responsible for the largest exchange and infrastructure compromises. TraderTraitor targets technical and backend personnel at blockchain companies through sophisticated fake job offers and skills tests. The cluster was directly attributed by the FBI to the Ronin Bridge, Bybit, Harmony Horizon, and numerous other major exchange hacks.

- **Primary approach:** Job offers and skills tests involving Python, SQL, or JavaScript projects. GitHub repos (sometimes private) containing backdoored npm packages. LinkedIn personas typically impersonate white professionals with cloned legitimate profiles.
- **Notable characteristic:** Extended dwell time between initial compromise and theft, sometimes 6+ months.
- **Past attacks:** Bybit, Phemex, XT, Indodax, WazirX, DMM Bitcoin, Poloniex, HTX/Heco, Stake, CoinEx, Alphapo, CoinsPaid, Atomic Wallet, JumpCloud, 3CX, Harmony, Ronin...

Contagious Interview

Also known as: Famous Chollima

A rapidly scaling social engineering cluster that targets developers through fake job interviews and malicious code repositories. Victims respond to job postings or recruiter outreach and are asked to complete coding challenges. The challenge code contains backdoored npm packages or Python modules that compromise the developer's workstation upon installation.

- **Malware:** BEAVERTAIL, INVISIBLEFERRET, OTTERCOOKIE.
- **Delivery:** GitHub/Bitbucket repos, npm install, fake video conferencing tools (Willo, Survicate, Teams clones).
- **Laundering:** Stargate, Defiway, RhinoFi, Railgun, dust collectors.

AppleJeus

Also known as: Citrine Sleet, Gleaming Pisces, UNC4736

A cluster specializing in trojanized cryptocurrency trading applications. Active since at least 2018, AppleJeus creates fake trading platforms and wallet applications that exfiltrate credentials and private keys. Notable fake applications include Celas Trade Pro, JMT Trading, Union Crypto, CoinGoTrade, and Ants2Whale. The cluster has also exploited Chromium zero-days (CVE-2024-7971) and deployed the FudModule rootkit.

DPRK IT Workers

Also known as: Jasper Sleet

Thousands of North Korean IT professionals deployed domestically and abroad under fraudulent identities to obtain remote employment at Western companies. They primarily engage in legitimate work while providing intelligence or facilitating theft. The revenue from their salaries alone funds WMD programs, but the access they gain creates persistent insider threats.

- **Notable incidents:** Munchables ($62M, insider deployed malicious contract), Solareum ($1.1M, rug pull by IT worker), Paid Network ($160M, insider exploit).

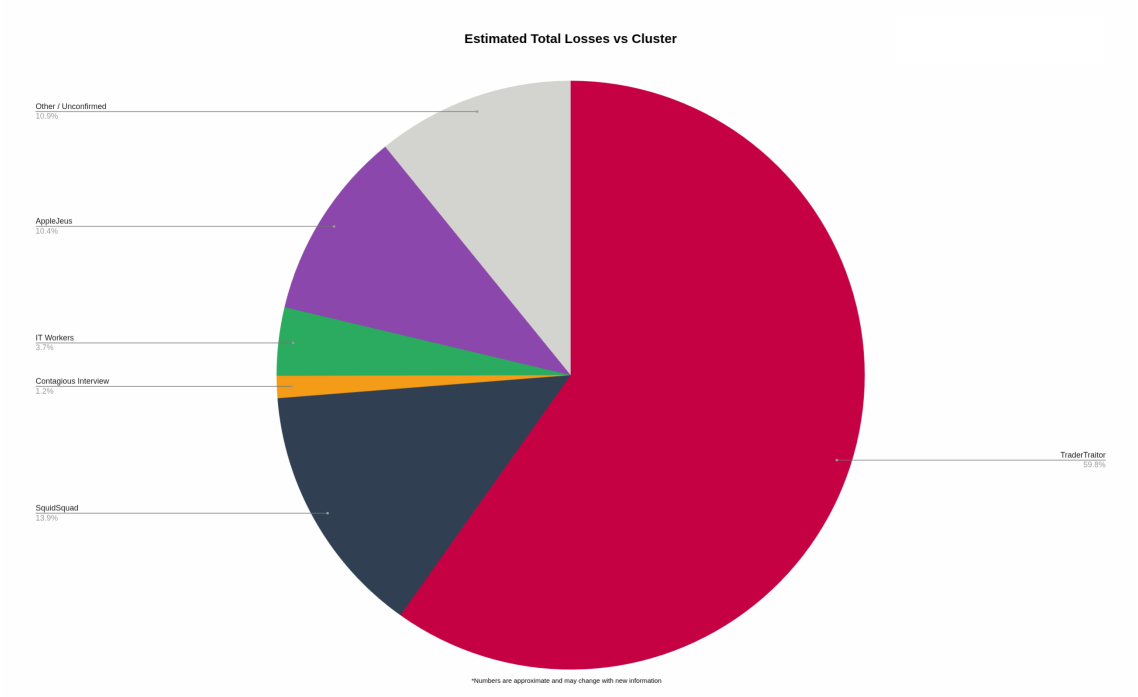


Figure 5: Estimated Total Losses vs Cluster in millions dollars

Operational Characteristics

Understanding how DPRK cyber units operate, not just what they do, is essential for building effective defenses. Several characteristics distinguish Lazarus from other threat actors:

Sophistication & Discipline

Lazarus operates as a **malware factory** producing new samples through multiple independent pipelines. They use extensive code obfuscation, commercial software protectors, and custom packers. First-stage backdoors are deliberately rudimentary and disposable; burning them has minimal operational impact. Advanced payloads are deployed only after confirming the infection is on a high-value target, protected via DLL loaders, encrypted containers, or password-protected installers that prevent sandbox analysis.

Reconnaissance

Routinely **maintain access to compromised systems for months** before executing theft, gathering intelligence on internal processes, personnel schedules, software configurations, and security procedures. In at least five major cryptocurrency exchange hacks, initial investigations mistook the attacks for inside jobs due to the depth of the attackers' knowledge.

Spear-Phishing

DPRK actors invest significant time in building rapport before delivering payloads. SquidSquad impersonators will maintain fake VC personas for weeks, conducting believable investment discussions before sharing a malicious document. Contagious Interview operators conduct multi-round technical interviews with real coding challenges before delivering the backdoored repository. This investment in social engineering makes their approaches significantly harder to detect than typical phishing campaigns.

Continuous Evolution

Lazarus evolves faster than most security teams can adapt. Their operational focus has shifted through multiple distinct phases since 2007, each driven by changing profitability dynamics, improved defensive postures in the targeted sector, and the regime's expanding technical capabilities.

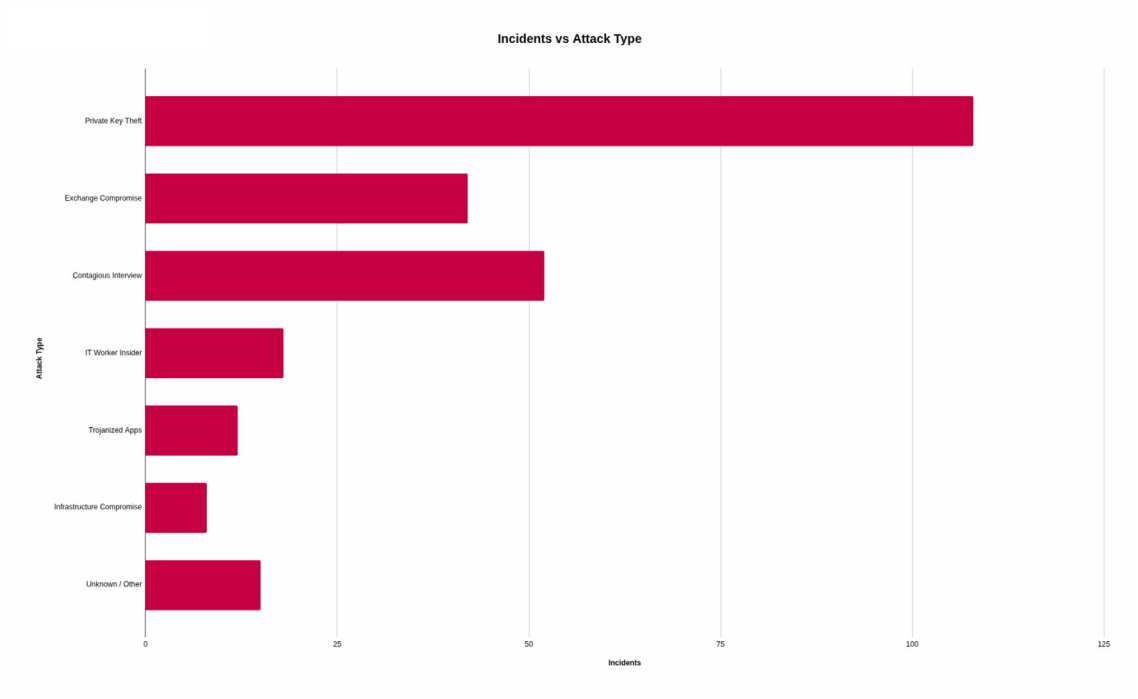


Figure 6: Incidents vs Attack Type related to DPRK

Evolution of the DPRK Crypto Playbook

DPRK cyber operations targeting cryptocurrency have undergone at least five distinct evolutionary phases since 2016. Each transition was driven by a combination of improved defensive postures in the targeted sector, changing profitability dynamics, and the regime's expanding technical capabilities.

DDoS Attacks and Destructive Operations (2007–2014)

Before financial theft became the primary objective, DPRK cyber units focused on politically motivated disruption and sabotage. Early operations included waves of DDoS attacks against South Korean government websites and financial institutions (2009, 2011, 2013), the destructive wiper attack against South Korean banks and broadcasters known as "Dark Seoul" (March 2013), and the high-profile infiltration of Sony Pictures Entertainment (November 2014) in retaliation for the film "The Interview." The shift toward revenue generation began around 2014, likely driven by tightening international sanctions following North Korea's third nuclear test in February 2013.

Banking Infrastructure (2014–2017)

Before cryptocurrency became a primary target, DPRK cyber units focused on the traditional financial system. The 2016 Bangladesh Bank heist demonstrated the operational sophistication of DPRK financial operations. However, the SWIFT system's centralized controls, correspondent banking relationships, and post-incident security upgrades made this attack vector increasingly difficult to repeat at scale.

Exchange Hot Wallets (2017–2019)

The first wave of DPRK crypto operations targeted the most basic vulnerability: exchanges storing customer funds in internet-connected hot wallets. Attacks on Bithumb ($14M, 2017), Coincheck ($530M, 2018), and multiple smaller Korean and Japanese exchanges exploited a sector that had grown faster than its security infrastructure. At the time, these operations required relatively low sophistication, the targets had not yet implemented cold storage, multisig, or adequate monitoring.

DeFi Protocols and Cross-Chain Bridges (2020–2023)

As centralized exchange security improved, DPRK actors pivoted to DeFi protocols and cross-chain bridges, which held billions in value but often operated with minimal security infrastructure. The Ronin Bridge hack ($625M, 2022) and Harmony Horizon Bridge ($100M, 2022) exploited the fundamental weakness of low-validator-count bridge designs: compromising a handful of private keys was sufficient to drain the entire bridge. Simultaneously, DPRK actors began targeting individual DeFi protocol deployments through compromised deployer keys and admin functions.

Supply Chain (2024–2025)

The Bybit hack ($1.5B, February 2025) marked a paradigm shift. Rather than attacking the target directly, DPRK actors compromised a third-party infrastructure provider (Safe{Wallet}). This supply chain approach bypassed the target's own security entirely. Simultaneously, the WazirX ($230M) and DMM Bitcoin ($305.8M) hacks demonstrated continued capability against centralized exchanges, but with increasingly sophisticated entry vectors.

Physical Infiltration (Present)

The Drift Protocol hack ($285M, April 2026) represents a new evolution. DPRK actors deployed third-party intermediaries to physically attend crypto conferences, build relationships with protocol contributors, deposit millions dollars in real capital, and ultimately compromise devices. The attack combined physical social engineering, governance manipulation, etc. Dozens of DeFi protocols are thought to be impacted. This represents a convergence of intelligence tradecraft and technical exploitation that no purely technical security model can address.

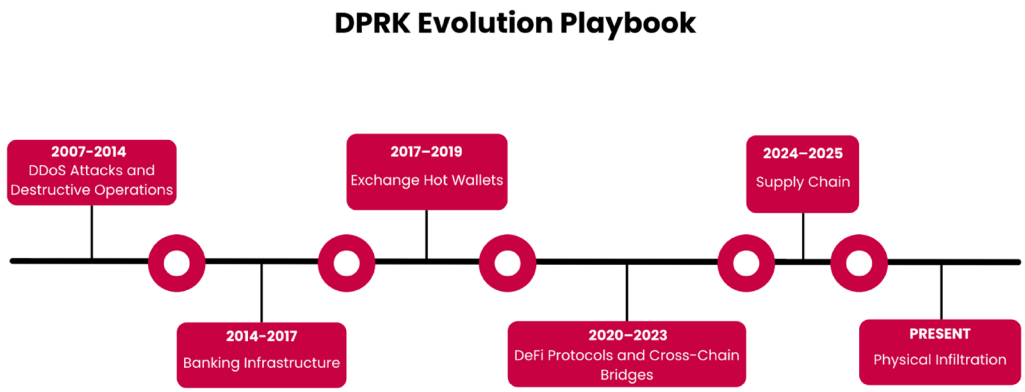


Figure 7: DPRK Evolution Playbook timeline

Case Study: Ronin Bridge (March 2022)

Background

On 23 March 2022, the Ronin Network, a sidechain supporting play-to-earn game Axie Infinity was exploited for approximately $624 million made up of 173,600 ETH and 25.5 million USDC, the largest cryptocurrency exploit at the time.

Attack Vector

The Ronin Bridge attack vector was a sophisticated social engineering campaign executed by North Korea's Lazarus Group that exploited both human and systemic vulnerabilities. A fake LinkedIn recruiter approached Sky Mavis engineers about a lucrative job opportunity to which one senior engineer replied and attended several interviews before receiving an offer. The engineer then downloaded a PDF file with compensation information that contained spyware that compromised Sky Mavis' infrastructure. The access gave attackers control of 4 of the 9 validators. They obtained a fifth validator key via a backdoor on the project's gas-free RPC node.

Execution & Aftermath

The style of exploit, a spear phishing campaign, coupled with the amount stolen and use of exchanges to launder $20M of the stolen assets naturally suggested DPRK might be responsible. Confirmation then came via OFAC sanctions against the wallet on 14 April 2022. The majority of the stolen funds were laundered through Tornado Cash via multiple wallets over the course of two months.

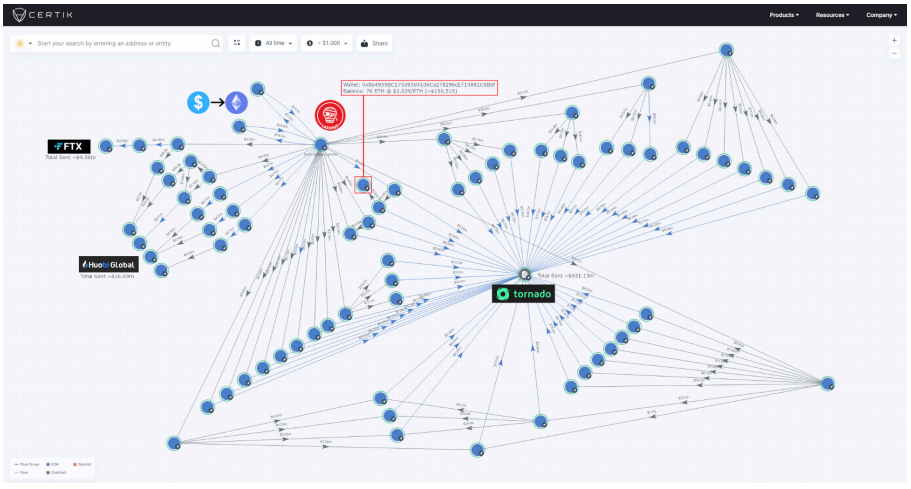


Figure 8: Ronin bridge funds flow.

Case Study: Bybit (February 2025)

Background

On February 21, 2025, Bybit Exchange was exploited, resulting in the loss of over $1.4 billion after Bybit approved malicious transactions that appeared to be legitimate. The attack remains the largest cryptocurrency exploit to date.

Attack Vector

The Bybit attack involved several sophisticated stages:

- **First:** A developer at Safe{Wallet}, a third-party multisig platform used by Bybit, was compromised on 4 February 2025. Malicious Docker files were found in the developer's download folder.
- **Second:** The attackers stole AWS session tokens, which allowed them to bypass multi-factor authentication and gain access to Safe's AWS account.
- **Third:** The attackers manipulated the Safe user interface to make it appear as though legitimate actions were being executed. Bybit employees then approved what appeared to be a routine transfer, the UI showed a legitimate transaction, but the backend code routed funds to a malicious address.

Execution & Aftermath

The size of the theft sparked probably the largest response to an incident with many 3rd parties assisting where they could with freezing stolen funds and reporting wallets. Some entities however, such as the now defunct eXch exchange, refused to prevent laundering activity. The lack of response by some intensified the debate on decentralization versus DPRK laundering.

Case Study: Drift Protocol (April 2026)

Background

On 01 April 2026 an unauthorized withdrawal of approximately $285 million in digital assets occurred from Solana-based exchange Drift Protocol, the culmination of a 6 month long operation.

Attack Vector

The exploit was executed through a multi-stage process involving administrative key compromise and collateral manipulation. By gaining access to multisig privileges, the attacker established a market for a low-liquidity token, artificially inflated its price to create a fraudulent collateral base, and disabled internal withdrawal safeguards which allowed the attacker to borrow legitimate assets, such as SOL, USDC, and Bitcoin, from the protocol's liquidity pools.

Execution & Aftermath

On-chain staging began on March 11 with a 10 ETH withdrawal from Tornado Cash, which was used to deploy the fictitious CarbonVote Token (CVT) with seeded liquidity and wash trading. On March 27, the attackers executed a zero-timelock Security Council migration, removing the protocol's last line of defense against unauthorized administrative actions. Using durable nonces, a legitimate Solana primitive that allows transactions to be pre-signed and executed later, the attackers obtained multisig approvals in advance and used them to drain ~$285 million from Drift's liquidity pools in a few minutes on April 1. The stolen funds were rapidly swapped into USDC via Solana-based DEX aggregators and bridged to Ethereum.

The individuals who attended conferences and built relationships with Drift contributors over six months were not North Korean nationals but third-party intermediaries with fully constructed professional identities.

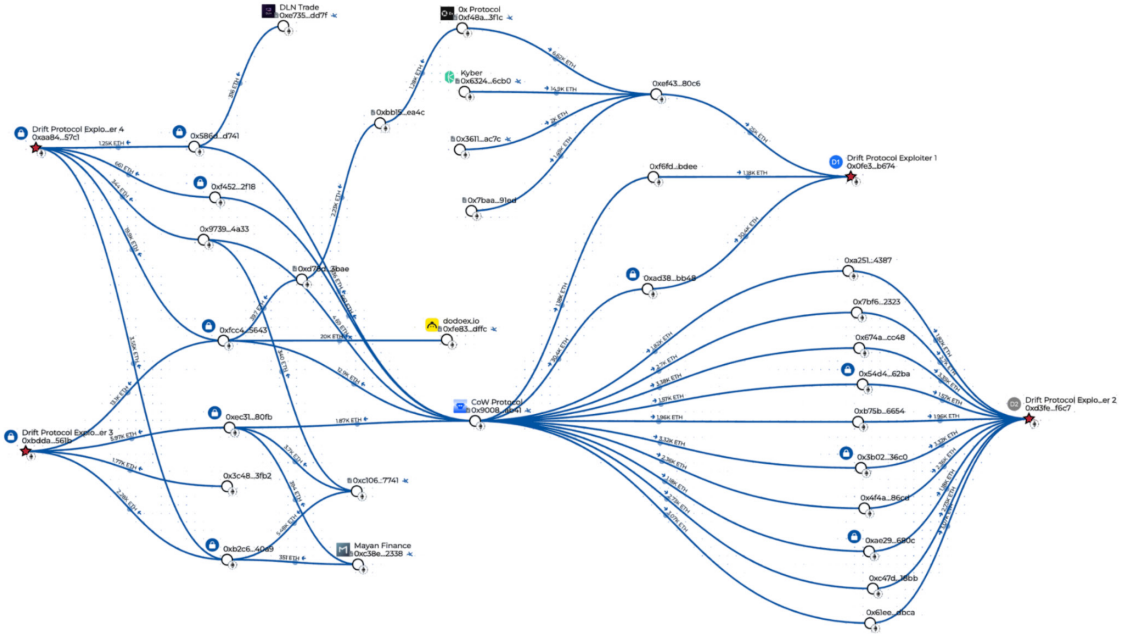


Figure 9: Drift Protocol funds flow

Cross-Case Analysis

Background

On 01 April 2026 an unauthorized withdrawal of approximately $285 million in digital assets occurred from Solana-based exchange Drift Protocol, the culmination of a 6 month long operation.

Attack Vector

The exploit was executed through a multi-stage process involving administrative key compromise and collateral manipulation. By gaining access to multisig privileges, the attacker established a market for a low-liquidity token, artificially inflated its price to create a fraudulent collateral base, and disabled internal withdrawal safeguards which allowed the attacker to borrow legitimate assets, such as SOL, USDC, and Bitcoin, from the protocol's liquidity pools.

Dimension	Ronin (2022)	Bybit (2025)	Drift Protocol (2026)
Loss	~$625M	~$1.5B	~$285M
Initial Access	Fake LinkedIn job offer	Supply chain (dev compromise)	6-month physical infiltration
Technical Vector	Validator key extraction	UI manipulation via JS injection	Oracle manipulation + governance takeover
Target Layer	Bridge consensus	Third-party signing interface	DeFi governance + oracle system
Detection Time	6 days	Minutes	12 minutes
Cluster	TraderTraitor	TraderTraitor	AppleJeus
Laundering	Tornado Cash ($455M)	DEXs, bridges, mixers, OTC	DEX aggregators, cross-chain bridges
Sophistication	Medium (social eng)	High (multi-stage supply chain)	Extreme (6-month intelligence op)
Key Lesson	Revoke residual permissions	Never trust a single signing UI	Physical presence does not equal trust

Figure 10: Comparative Analysis of Three Major DPRK Operations

The progression from Ronin to Drift illustrates a clear and alarming trajectory. The Ronin hack succeeded through a **single compromised employee** and an un-revoked permission. Bybit required **infiltrating a third-party** developer's workstation and injecting code into production infrastructure. Drift Protocol demanded a **six-month intelligence operation** involving physical intermediaries at conferences, real capital deployment, and the exploitation of multiple technical primitives (durable nonces, oracle manipulation, governance migration) simultaneously. Each successive attack required more investment from the attacker and each was harder to detect with conventional security measures.

Tactics, Techniques & Procedures

The following section maps the primary attack vectors, malware families, and post-compromise techniques observed across the full spectrum of DPRK crypto operations:

Social Engineering

DPRK IT Workers

Attackers create convincing Telegram profiles impersonating well-known VCs, investors, and crypto executives. They initiate conversations about investment opportunities, partnership proposals, or conference meetups, then share links to Google Drive documents, PDFs, or fake meeting platforms containing malware.

Defenders should treat any unsolicited investment outreach via Telegram, Discord, or LinkedIn with extreme suspicion.

Fake Job Offers

Two distinct clusters use job-related social engineering with different approaches:

- **TraderTraitor** targets senior technical staff at specific organizations with elaborate multi-round interview processes and ultimately delivers malware via job offer PDFs or skills test repositories.
- **Contagious Interview** targets a broader developer population through job postings on LinkedIn and freelance platforms, delivering malware via npm packages in coding challenges. Victims clone a GitHub repository, run npm install, and are immediately compromised. The malware exfiltrates browser credentials, wallet data, and SSH keys, then deploys a secondary payload for persistent access.

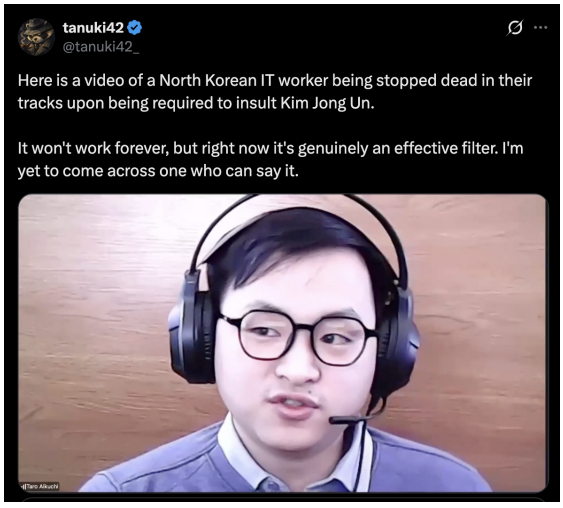


Figure 11: DPRK IT worker during interview. Source: @tanuki42_

Fake Video Conferencing Tools

Victims are invited to video calls for interviews, investor meetings, or partnership discussions. The meeting link directs to a fake platform that requires downloading a custom client (impersonating Zoom, Teams, etc). The downloaded application is trojanized. This vector is particularly effective because the social context creates urgency that overrides caution.

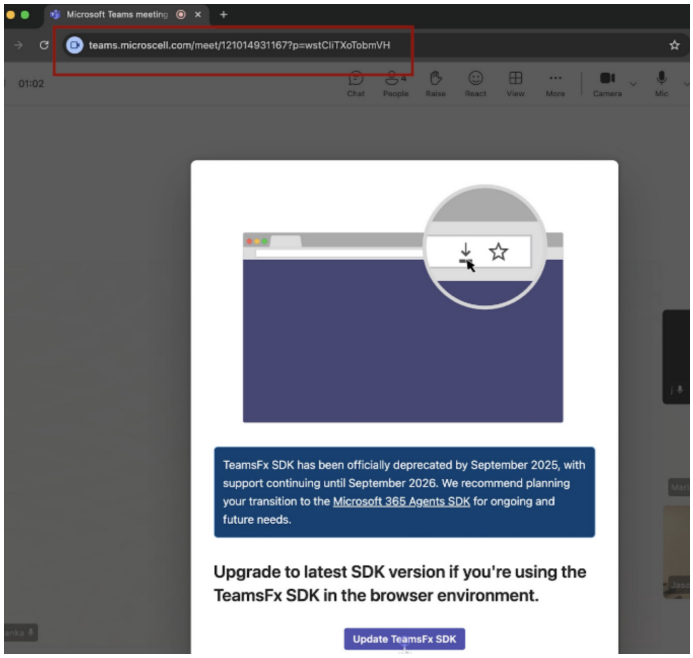


Figure 12: Fake Teams extension. Source: SEAL

Malicious Code Repositories

DPRK actors maintain a growing ecosystem of malicious npm packages, PyPI modules, and GitHub repositories. These include backdoored versions of legitimate packages, entirely fake packages with crypto-themed names, and private repositories shared during fake technical interviews. For example, in January 2026, a new delivery mechanism was identified involving VSCode and Cursor code editors. Simply opening a project folder in these editors could silently execute arbitrary code via the runOn:folderOpen task configuration, requiring no user interaction beyond opening the repository.

Malware

DPRK maintains a diverse, multi-platform toolkit that is continuously updated:

macOS: RustBucket, SwiftBucket, NimDoor, AppleScript-based payloads, KANDYKORN, trojanized trading apps.

Cross-platform: BEAVERTAIL (JavaScript/Python stealer), INVISIBLEFERRET (Python RAT), OTTERCOOKIE, custom Docker-based payloads.

Windows: MagicRAT, QuiteRAT, LPEclient, FoggyBrass, PhantomStar, Gh0st RAT variants, custom PowerShell implants.

Supply chain: Malicious npm/PyPI packages, trojanized installers (3CX, CyberLink), backdoored browser extensions (fake MetaMask).
The group is notorious for constantly evolving its malware, rarely reusing the same tools across operations.

EtherHiding

In October 2025, Google Threat Intelligence Group documented the first adoption of **EtherHiding** by a nation-state actor. **Contagious Interview** began leveraging public blockchains as decentralized command-and-control (C2) infrastructure. The technique involves storing malicious payloads within smart contract transactions, then retrieving them via read-only API calls that leave no visible transaction trace.

The attack chain works as follows: a victim is socially engineered into running an initial JavaScript downloader (**JADESNOW**), which queries a malicious smart contract on BNB Smart Chain to fetch a second-stage payload. This payload then pivots to Ethereum to retrieve the final backdoor, **INVISIBLEFERRET**, stored as calldata in transactions sent to the burn address 0×00…dEaD.

EtherHiding is particularly difficult to mitigate because the malicious code is stored on a decentralized, permissionless blockchain that cannot be taken down by law enforcement.

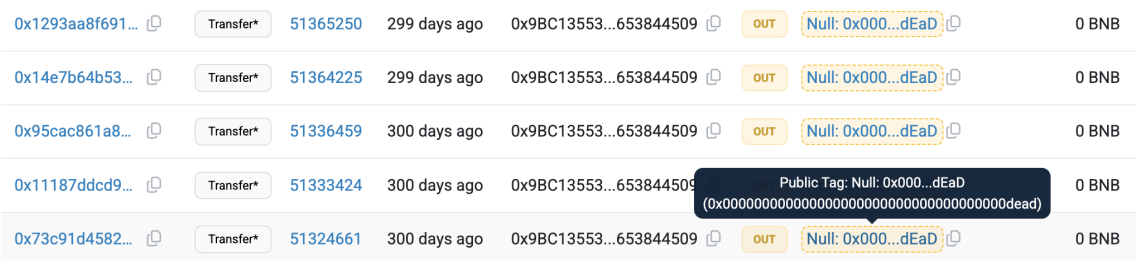


Figure 13: On-chain transaction sent to the burn address 0×00…dEaD

Post-Compromise

Private key extraction: Attackers locate wallet files, browser extension data, seed phrases, and SSH keys on compromised devices.

Contract takeover: Stolen deployer keys are used to call transferOwnership, upgrade proxy contracts, or mint unlimited tokens.

Supply chain injection: In sophisticated operations, like Bybit for example, the compromised developer's access is leveraged to modify production infrastructure, affecting downstream targets.

Laundering Infrastructure

From the point of exploitation, routing funds through bridges, exchanges, DeFi protocols and mixing services is only the first step. The stolen assets need to be converted to fiat currency either via willing assistants such as front companies or without raising suspicion via legitimate routes. On the former, in December 2024 the Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned two individuals laundering funds for DPRK via a UAE based company. https://home.treasury.gov/news/press-releases/jy2752

Analysis of DPRK's laundering methods also shows a reliance on China based individuals and organizations. According to a Multilateral Sanctions Monitoring Team report, which receives information via MSMT participating states, actionable intelligence has been provided identifying multiple Chinese nationals assisting the DPRK in converting cryptocurrency to fiat currency. https://www.mofa.go.jp/files/100922718.pdf

Ecosystem Impact & International Response

The impact from these exploits often has far wider consequences than the initial loss and potential shutdown of the victim platform, for example:

Price Effects: after the Bybit incident, the Ethereum price fell around 4.2% due to sell pressure from laundering activity.

Compliance Burden: Changes in laws to combat illicit activity such the EU's MiCA II regulations (effective January 2026) and US Executive Order 14155 forcing platforms to implement strict due diligence for transactions over $10,000.

Contagion: Stolen funds aren't always limited to the victim protocol, many web3 protocols utilise DeFi platforms to invest their own project funds and can also be left devastated by an exploit. Trust is further eroded as more victims feel the impact.

The fast pace of the web3 world can feel like little is being done to prevent actors such as DPRK from stealing and laundering billions in crypto, however several initiatives have been introduced in response.

- **Multilateral Sanctions Monitoring Team (MSMT):** Launched by the US, South Korea, and Japan, MSMT leads the tracking of DPRK sanctions violations and publishes frequent alerts on their evolving laundering tactics.
- **The UN Convention against Cybercrime:** this treaty aims to streamline cross-border evidence sharing, though its effectiveness is still being tested by geopolitical friction with Russia and China.
- **The UK-ROK Strategic Cyber Partnership:** In early 2026, London and Seoul intensified bilateral efforts to counter "adversary cooperation" between Russia and North Korea, specifically focusing on ransomware and crypto-laundering.
- **IT Worker Fraud:** In March 2026, OFAC sanctioned a network of six individuals and two entities for orchestrating "IT worker schemes" in which North Korean operatives pose as legitimate developers with the aim of planting backdoors and stealing private keys.
- **Shadow Banking Interdiction:** Law enforcement is actively targeting Southeast Asian "shadow-banking" brokers and facilitators (notably the Huione Group in 2025) who assist DPRK in cashing out stablecoins like USDT.
- **Stablecoin Freezing:** Increased pressure on stablecoin issuers (like Tether) has led to more frequent proactive freezing of addresses linked to DPRK.

Recommendations

Whilst there are some more novel methods of detecting DPRK IT workers such as asking individuals to speak ill of their supreme leader, preventing state sponsored exploits requires an in-depth approach. DPRK undeniably have some of the most skilled exploiters in the world and if there is a weakness in the system they will go to any length to exploit it. For protocols in custody of large amounts of funds it is highly likely a case of when and not if.

- **Rigorous Identity Verification:** Use mandatory video interviews with "liveness" checks and background verification services that specialize in detecting the AI-generated or "borrowed" identities often used by North Korean agents.
- **Zero-Trust Hiring:** Assume any remote freelancer could be a high-risk actor. Restrict their access to sensitive "production" code and private keys until they have established a long-term, verifiable physical presence or trust.
- **De-risking Communications:** Train employees to recognize "social engineering" on platforms like LinkedIn and Discord. Lazarus often initiates contact via fake job offers or technical collaboration requests that contain malware-laden "coding tests."
- **Protecting the Infrastructure:** Since many thefts target the "bridges" between different blockchains or the "hot wallets" of exchanges, technical hardening is essential.
- **Withdrawal Delays & Circuit Breakers:** Implement mandatory "cooling-off" periods for large withdrawals. As seen in recent South Korean regulations, a 24-to-72-hour delay allows security teams to flag and freeze suspicious transactions before the funds are laundered through mixers. Protocols should also enforce timelocks on all administrative and governance actions.
- **Hardware Security Modules (HSMs):** Store private keys used for signing high-value transactions and managing treasury funds in air-gapped hardware that requires physical interaction to authorize any operation.

For further information, we recommend consulting the SEAL framework dedicated to this subject.

2026 Outlook

DPRK crypto operations will continue to scale. Seven incidents totaling **~$620.9M** were documented in the first four months of 2026 alone. Several trends are expected:

- **AI-enhanced social engineering:** Deepfake technology and AI-generated personas will make social engineering campaigns harder to detect. Autonomous agents managing thousands of simultaneous fake interactions will enable industrial-scale targeting.

- **Expanded IT worker infiltration:** DPRK operatives are expected to target AI, defense, and enterprise SaaS sectors. Dozens of DeFi protocols have already been infiltrated.

- **New laundering vectors:** DPRK actors continue to leverage Tornado Cash alongside privacy coins (Monero) and alternative blockchains to obfuscate stolen funds. Expect further diversification across emerging cross-chain protocols.

- **VSCode and IDE-based attacks:** The January 2026 discovery of malicious VSCode tasks (runOn:folderOpen) represents a new delivery mechanism targeting the developer workflow itself.

The fundamental challenge remains: North Korea has weaponized cryptocurrency theft as an essential revenue stream for regime survival. Until that incentive structure changes, the threat will persist and evolve.

Sources & References

The following sources were consulted during the preparation of this report:

- Barnhart, M. (2025) “Exposing DPRK's Cyber Syndicate and Hidden IT Workforce”. DTEX Systems.
- CrowdStrike (2026) “2026 Global Threat Report”.
- Department of the Army (2020) “ATP 7-100.2: North Korean Tactics”.
- Expel (2026) “Inside Lazarus: How North Korea Uses AI to Industrialize Attacks on Developers”. Marcus Hutchins.
- GitLab (2026) “GitLab Threat Intelligence Reveals North Korean Tradecraft”. Oliver Smith.
- Google Threat Intelligence Group (2025) “DPRK Adopts EtherHiding: Nation-State Malware Hiding on Blockchains”. Google Cloud Blog, 16 October.
- Google Threat Intelligence Group (2025) “UNC5142 Leverages EtherHiding to Distribute Malware”. Google Cloud Blog, 16 October.
- Group-IB (2026) “Cyber Saga: In the Footsteps of the DPRK IT Workers”.
- Kaspersky (2017) “Operation AppleJeus Sequel”. Securelist.
- Ministry of Foreign Affairs of Japan (2022) “Advisory on North Korean Cyber Threats”.
- MITRE ATT&CK (2025) “Lazarus Group (G1049)”.
- Monahan, T. (n.d.) “Lazarus-BlueNoroff Research”. GitHub repository.
- Orcasia (2022) “North Korea's Cyber Offensive”.
- pcaversaccio (2025) X post.
- Radar Security Alliance (2026) “Advisory on DPRK UNC1069: Fake Microsoft Teams and Zoom Calls”.
- Security Alliance (n.d.) “DPRK IT Workers Framework”.
- tanuki42_ (n.d.) X post.
- Université de Strasbourg (2021) “Joint Cybersecurity Advisory: AppleJeus Analysis of North Korea's Cryptocurrency Malware”. FBI report.
- US Department of the Treasury (2022) “Treasury Designates DPRK Weapons Representatives”, Press Release jy2752.
- ZachXBT (n.d.) X profile.
- Yoo, S.W. (2019) “The All-Purpose Sword: North Korea's Cyber Operations and Strategies”. Center for Strategic and International Studies.

CERTIK
SKYNET

COMPANY INTRO

CertiK is the largest Web3 security services provider, founded in December 2017 in New York by two professors from Yale and Columbia University.

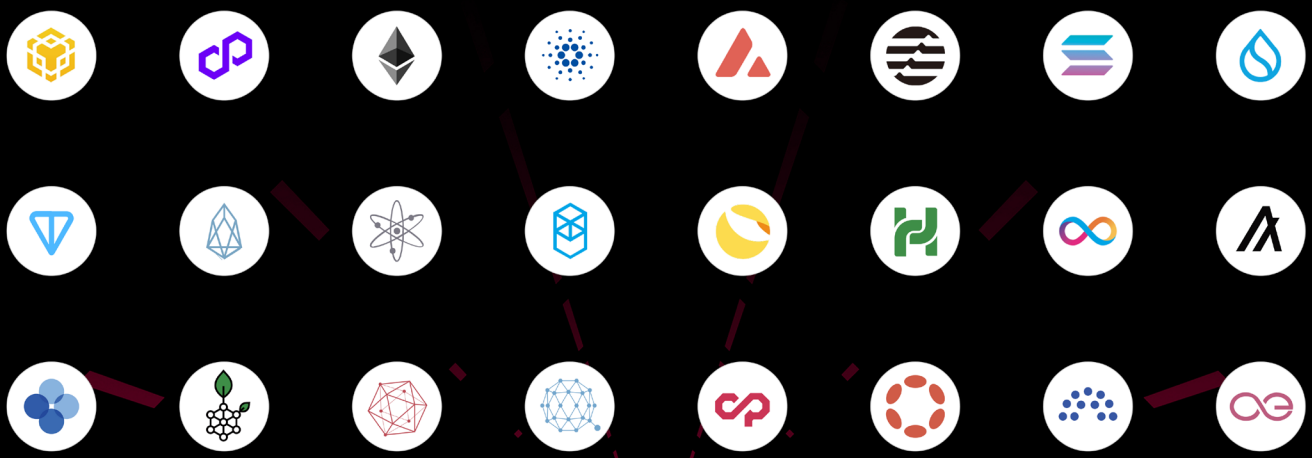
Powered by the industry's largest proprietary Web3 security database, CertiK provides actionable insights, including incident analyses, security reports and guidelines. It has also become a trusted security partner for global regulators, institutions, and Web3 enterprises, supporting both their security needs and their pursuit of innovation.

5,000+
CLIENTS SERVED

180,000+
VULNERABILITIES DETECTED

>$600B
MARKET CAP ASSESSED

>70% OF TOP 500 CMC PROJECTS AUDITED



DIVERSITY IN ECOSYSTEMS