UPay

UPAY RESEARCH

QUARTERLY REPORT • Q1 2026

Crypto Hack Trend Report Q1 2026

$501 million lost, why people are the new attack surface, and how to protect your funds in the new era of operator and infrastructure attacks.

$501M	145	-70%
TOTAL LOSSES	INCIDENTS	VS Q1 2025

JANUARY – MARCH 2026

PUBLISHED MAY 2026

Sources: PeckShield, CertiK, SlowMist, Chainalysis, Halborn, Immunefi

Table of Contents

SECTION 01

Executive Summary

Q1 2026 was the quarter the threat moved. Smart contract exploit losses fell roughly 89% year-over-year, but the dollars did not stay safe. They were redirected toward attacks on humans, operators, and infrastructure. A single individual lost $282 million to a hardware wallet support impersonation scam. A protocol lost $40 million because one executive's device got compromised. Two of the most widely used open source libraries in the world were poisoned with North Korean malware. The headline is not that crypto got safer. The headline is that the attack surface changed faster than most users adapted.

TOTAL LOSSES

$501M

Across 145 incidents in Q1 2026, per CertiK

YOY CHANGE

-70%

Down from $1.67B in Q1 2025 (Bybit-inflated)

LARGEST SINGLE LOSS

$282M

One individual, hardware wallet social engineering

SMART CONTRACT LOSSES

-89%

YoY drop in code-level exploits

OFF-CHAIN LOSSES

~$360M

Social engineering, key theft, supply chain

DPRK SHARE

High

Bitrefill, axios npm, Sapphire Sleet activity

Three forces defined Q1 2026

1. A single $282 million hardware wallet social engineering attack on one individual whale on January 10.
2. A wave of operational security failures at protocols, including Step Finance's $40M executive device compromise, Resolv Labs' $25M AWS KMS breach, and IoTeX's $4.4M validator key leak.
3. The first cluster of EIP-7702 delegated account exploits in DeFi, plus the first major DeFi hack tied to AI-written Solidity code.

WHAT THIS MEANS FOR UPAY READERS

Smart contracts kept your assets safer in Q1 2026 than at any time in five years. But your private keys, your devices, your DNS, your X account, and the cloud accounts of every protocol you use are all now in scope. Treat operational security like portfolio risk. The protocols are getting safer. The humans operating them, and the humans using them, are now the target.

SECTION 02

Key Findings

1. **$501 million across 145 incidents.** Total Q1 2026 losses across all Web3 incidents reached approximately $501 million, per CertiK's running tally. Counting only protocol-level exploits above $1 million, the figure was closer to $168 million across 34 incidents.

2. **January was the heaviest month.** PeckShield logged 16 protocol hacks totaling $86.01 million, but when phishing and individual social engineering are added (led by a single $282 million theft) January's all-in figure exceeded $370 million.

3. **February was the quietest month at $26.52 million** across 15 main incidents, the lowest monthly figure in roughly 11 months. The 98.2% year-over-year drop is distorted by the $1.4 billion Bybit attack in February 2025.

4. **March rebounded to roughly $52 million** across 20 incidents, a 96% month-over-month jump, with Resolv Labs' $25 million AWS KMS compromise driving most of the damage and triggering "shadow contagion" across Morpho, Euler, and Fluid lending vaults.

5. **Smart contract exploits fell roughly 89% year-over-year.** Off-chain attacks (private keys, social engineering, supply chain, cloud infrastructure) filled the gap.

6. **Recovery rates collapsed for the second consecutive quarter.** Aside from a handful of negotiated white-hat returns (Makina Finance's 920 ETH, IPOR Fusion, Solv Protocol's full user reimbursement), the base case for Q1 2026 incidents was "funds gone."

7. **North Korea remained the dominant nation-state threat.** The Bitrefill breach on March 1, attributed to Lazarus/Bluenoroff, and the axios npm supply chain attack on March 31, attributed by Google's Threat Intelligence Group to UNC1069, both targeted the developer and operator side of the crypto stack rather than smart contracts.

8. **EIP-7702 produced its first cluster of confirmed protocol exploits.** The Ethereum Pectra upgrade feature that lets externally owned accounts temporarily behave like smart contracts, became a new attack surface. The most notable case was Fusion by IPOR's $336,000 loss on January 6.

SECTION 03

The Q1 2026 Numbers at a Glance

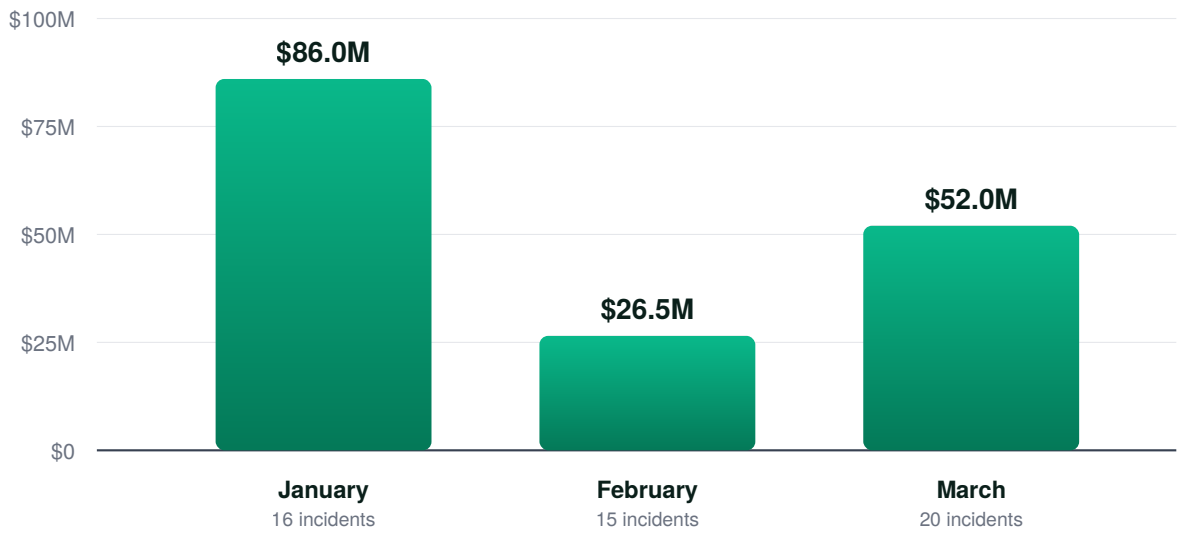
Year-over-Year Comparison

METRIC	Q1 2026	Q1 2025	CHANGE
Total losses (CertiK, all incidents)	**$501M**	$1.67B	**-70%**
Protocol-only losses ($1M+)	**$168M**	$1.50B	**-89%**
Number of incidents	**145**	197	**-26%**
Largest single incident	**$282M (Jan 10 whale)**	$1.5B (Bybit)	n/a
DPRK-attributed share	Ongoing (Bitrefill, axios)	$1.5B+ (Bybit)	Down in dollar terms
Recovery rate	Low single digits	0.4%	Flat-to-worse

Monthly Breakdown

Q1 2026 Monthly Losses (PeckShield, protocol-only)

Bars show protocol-level hack losses by month. CertiK's wider scope including phishing puts January alone above $370M.



MONTH	INCIDENTS	PROTOCOL LOSSES	MOM CHANGE	ALL-IN TOTAL (CERTIK)
January 2026	**16**	**$86.01M**	+13.25%	**~$370M**
February 2026	**15**	**$26.52M**	-69.2%	**~$50M**
March 2026	**20**	**$52.00M**	+96.0%	**~$80M**

Sources: PeckShield monthly reports, CertiK Skynet quarterly tracker. CertiK includes individual phishing and wrench attacks.

SECTION 04

Top 10 Largest Q1 2026 Incidents

The top 10 list below is heavily skewed by individual social engineering targeting whales. Six of the ten largest losses of the quarter were not protocol exploits at all. They were attacks on people, on operator devices, and on cloud key infrastructure.

#	TARGET	DATE	LOSS	ATTACK TYPE
1	**Anonymous whale** (hardware wallet)	Jan 10	**$282M+**	Social engineering, Trezor support impersonation
2	**Step Finance** + SolanaFloor + Remora	Jan 31	**~$40M**	Executive device compromise, private key theft
3	**Truebit**	Jan 8	**$26.44M**	Legacy contract integer-overflow in pricing logic
4	**Resolv Labs** / USR stablecoin	Mar 22	**~$25M**	AWS KMS compromise, off-chain signer key
5	**Sillytuna** (individual whale)	Mar 5	**~$24M**	Address poisoning + physical wrench attack
6	**Kraken whale** (individual)	Mar	**~$18M**	Social engineering
7	**SwapNet**	Jan 25	**$13.43M**	Arbitrary-call vulnerability, closed-source contracts
8	**YieldBlox DAO**	Feb	**$10M**	Oracle manipulation
9	**SagaEVM**	Jan 21	**$7M**	Smart contract vulnerability
10	**IoTeX ioTube bridge**	Feb 21	**$4.4M**	Compromised validator private key

NOTABLE MID-SIZE INCIDENTS

Several mid-size incidents matter for trend analysis even though they did not crack the top 10: MakinaFi ($4.13M, partly recovered), CrossCurve ($3M), Aperture Finance ($3.67M), Solv Protocol ($2.7M), FOOMCASH ($2.26M), Venus Protocol ($2.15M bad debt), Moonwell ($1.78M), and Arbitrum's USDGambit/TLP access control failure ($1.5M).

SECTION 05

The $282 Million Whale: Anatomy of Q1's Biggest Loss

$282M+

LOST BY ONE PERSON IN A SINGLE ATTACK

On January 10, 2026, at around 11 p.m. UTC, an anonymous victim lost more than $282 million in Bitcoin and Litecoin to a hardware wallet social engineering scam. The breakdown comes from on-chain investigator ZachXBT, who posted on X: "On January 10, 2026 at around 11 pm UTC a victim lost $282M+ worth of LTC & BTC due to a hardware wallet social engineering scam. The attacker began converting the stolen LTC & BTC to Monero via multiple instant exchanges causing the XMR price to sharply increase."

LITECOIN LOST

2.05M LTC

Worth approximately $153M at time of theft

BITCOIN LOST

1,459 BTC

Worth approximately $139M at time of theft

MONERO PRICE SPIKE

+60%

XMR pumped on the attacker's laundering flow

The Attack Vector

Security firm ZeroShadow identified the specific pretext: the attacker impersonated Trezor "Value Wallet" support to manipulate the victim into sharing their seed phrase backup. CertiK's January 2026 report pegged the single victim's loss at approximately $284 million (the small discrepancy with ZachXBT's $282M+ reflects BTC and LTC price timing). ZachXBT explicitly dismissed early speculation about DPRK involvement.

No funds were recovered. The attacker laundered the proceeds through instant exchanges into Monero, with secondary BTC flows bridged to ETH, XRP, and LTC via THORChain. Monero's price briefly spiked more than 60% on the inflows.

WHY THIS MATTERS

This single incident is the most important data point of Q1 2026. It is larger than every protocol exploit combined. It targeted an individual, not a protocol. It required no code knowledge from the attacker, only a phone call or message convincing enough to extract a backup phrase. **Hardware wallets do not protect you from social engineering. Nothing does, except verification discipline.**

Incident Spotlight: How the $282M Was Stolen

Step 1 – Pretext. Attacker contacts victim posing as Trezor "Value Wallet" support.

Step 2 – Trust. Victim follows guidance from supposed support team, treating attacker as official.

Step 3 – Seed extraction. Victim shares the recovery seed backup phrase, believing it is part of a legitimate support process.

Step 4 – Drain. Attacker uses the seed to derive private keys and sweeps all addresses.

Step 5 – Laundering. Funds routed to Monero via instant exchanges, with secondary flows bridged via THORChain.

Hardware Wallet | Social Engineering | Seed Phrase Theft | Instant Exchange Laundering | Monero

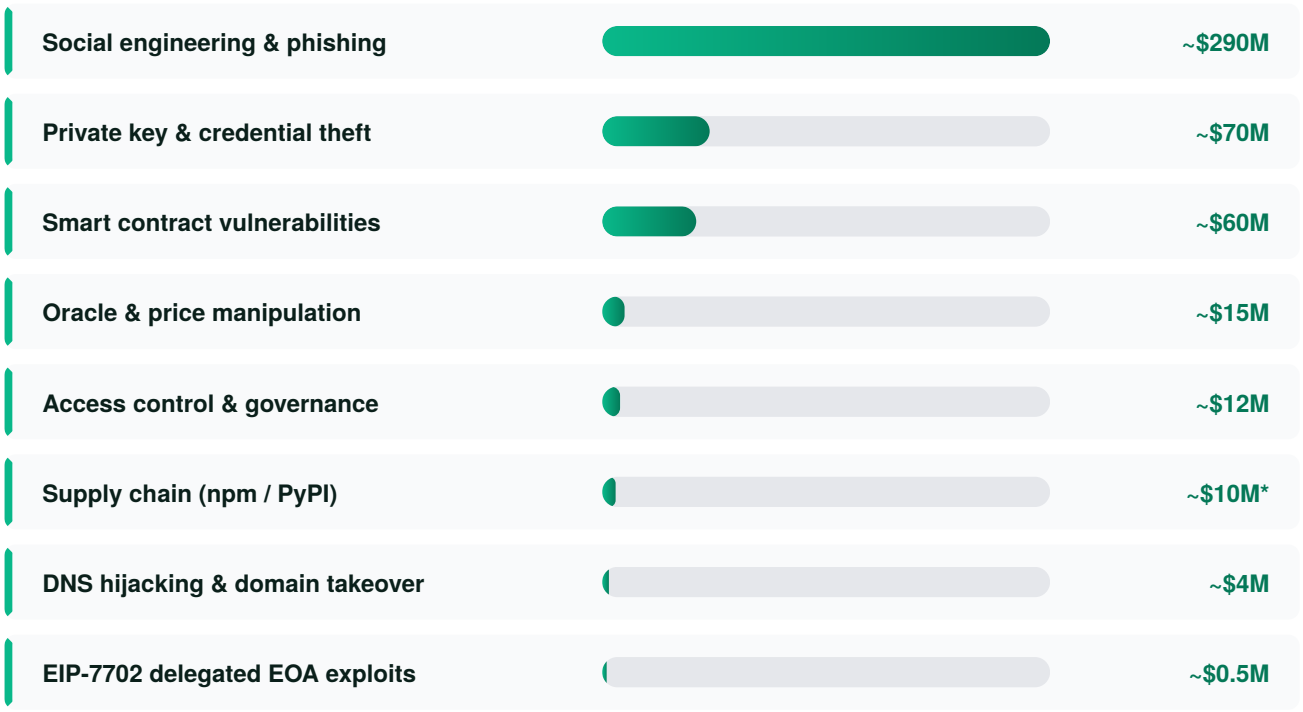
SECTION 06

Attack Vector Analysis: People, Not Code

Q1 2026 broke decisively with the pattern that defined 2021 through 2023. Smart contract exploits used to dominate. This quarter, the dominant categories were operational and human.

Q1 2026 Losses by Attack Vector

Approximate distribution of $501M total across vector categories



**Supply chain attack value is estimated based on reported credential exfiltration. True downstream impact is likely multiples higher.*

Vector-by-Vector Detail

Social engineering and phishing (~$290M)

The largest single bucket, driven by the January 10 whale loss, plus the Sillytuna and Kraken whale incidents, plus dozens of smaller phishing wallet drains. PeckShield noted in its January summary that phishing-related losses alone exceeded $300 million for the month, calling the trend out plainly: *"Phishing remains the most persistent threat. Instead of trying to hack the contract, bad actors are increasingly focused on hacking the human."*

Private key and credential compromise (~$70M)

Step Finance's $40M executive-device breach, IoTeX's $4.4M validator key, Resolv Labs' $25M AWS KMS theft, Bitcoin Depot's $3.665M settlement-account credential leak, and at least nine X account takeovers (Darren Lau, Bitlight Labs, Scroll's @shenhaichen, Arbitrum DAO governance, Solana_zh, Arf, and others). The pattern Halborn, Trail of Bits, and TRM Labs all flagged for 2025 has carried into 2026: top-tier adversaries now compromise signing

infrastructure, key custody, and exchange operator workflow rather than hunting for novel logic errors in DeFi protocols.

Smart contract vulnerabilities (~$60M)

Truebit's $26.44M integer overflow was the biggest, followed by SwapNet and Aperture's shared arbitrary-call flaw, FutureSwap's reentrancy, Solv Protocol's ERC-3525 double-mint reentrancy, FOOMCASH's zkSNARK verification key misconfiguration, SynapLogic's swap function flaw, Revert Lend's vault bug, and Gondi's purchase bundler exploit. Still a meaningful share, but a fraction of the historical norm.

Oracle manipulation and price manipulation (~$15M)

Moonwell's $1.78M cbETH oracle misconfiguration on February 15, Venus Protocol's nine-month THE-token TWAP manipulation on March 15 ($3.7M extracted, $2.15M bad debt), Inverse Finance's $240K DOLA manipulation, dTRINITY's $257K dLEND deposit inflation, and several BSC pool manipulations.

Supply chain attacks

LiteLLM on March 24 (versions 1.82.7 and 1.82.8 with credential stealers; PyPI Stats recorded 96,830,964 monthly downloads at the time) and axios npm on March 31 (versions 1.14.1 and 0.30.4, with a North Korea-attributed cross-platform RAT). No direct on-chain losses confirmed yet from either, but every developer machine that ran the compromised versions during the exposure window must be treated as fully credential-leaked.

EIP-7702 delegated EOA exploits

Fusion by IPOR's $336K loss on January 6 was the first protocol-level EIP-7702 exploit confirmed by SlowMist. Wintermute researchers later found that most EIP-7702 delegations on Ethereum mainnet pointed to contracts with identical code, much of it built specifically to automate fund theft.

DNS hijacking and domain takeover

BONKfun on March 11 (DNS hijacking through DNS provider social engineering, $30K lost, 110% user compensation) and Neutrl on March 19 (DNS hijacking via social engineering on the project's DNS provider).

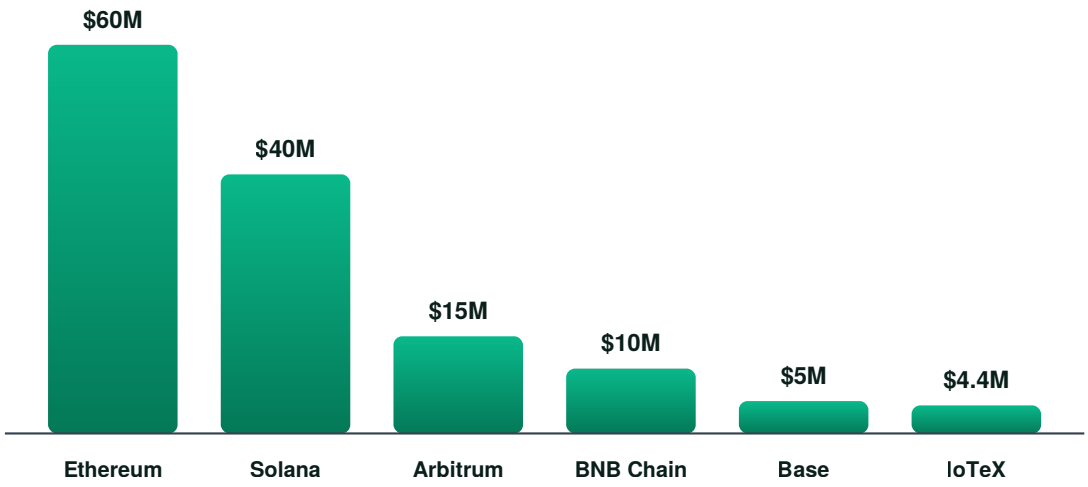
SECTION 07

Chain-by-Chain Breakdown

Ethereum and BNB Chain stayed the largest targets by dollars and incidents. BSC had the highest incident frequency for low-value exploits. Arbitrum hosted the SwapNet, Aperture, FutureSwap, TMX, USDGambit/TLP, and IPOR Fusion incidents. Base hosted Moonwell, Revert Lend Aerodrome vault, and parts of the SwapNet/Aperture multi-chain drains. Solana was hit hardest at the operational layer through Step Finance.

Q1 2026 Protocol Losses by Chain

Approximate share of protocol-level losses (excluding whale phishing events)



CHAIN	NOTABLE INCIDENTS	APPROX. LOSSES
Ethereum	Truebit, Resolv Labs, parts of SwapNet/Aperture, Gondi	**~$60M**
Solana	Step Finance dominated	**~$40M**
Arbitrum	SwapNet, Aperture, TMX, USDGambit/TLP, IPOR Fusion, MakinaFi	**~$15M**
BNB Chain	Venus, multiple sandwich and burn-mechanism exploits	**~$10M**
Base	Moonwell, SwapNet, Aperture, parts of FOOMCASH	**~$5M**
IoTeX → Ethereum bridge	ioTube validator key compromise	**$4.4M**

SECTION 08

Protocol Type Breakdown

DeFi lending and yield protocols

Took the largest hit in dollar terms when you exclude the whale phishing event. Resolv Labs, Moonwell, Venus, MakinaFi, Solv Protocol, Stake Nova, dTRINITY, and Revert Lend all sit here. The common thread is misplaced trust in either an oracle, an off-chain signer, or a known-but-disputed audit finding.

Cross-chain bridges

Delivered a smaller absolute hit in Q1 than in past quarters, with IoTeX's ioTube ($4.4M) and CrossCurve ($3M) the headline events. But cross-chain laundering through THORChain remained the dominant outflow path for stolen funds, including 1,572 ETH bridged to 66.78 BTC after the IoTeX hack.

DEX aggregators and routers

Produced the largest single-incident DeFi loss with the SwapNet $13.43M arbitrary-call exploit, and a related $3.67M loss at Aperture Finance.

Trading bots and DeFAI smart wallets

A new addition to the attack surface. Polycule (Polymarket trading bot, $230K on January 7), Mithril (via Paradex, 57 user subkeys exposed on January 21), and Holdstation (DeFAI smart wallet, $462K USDT on February 25) all fell in Q1. The Mithril incident is particularly important because the attack method remains unknown as of publication.

Centralized services

Bitrefill (gift cards) lost an undisclosed amount in hot wallets plus 18,500 customer records on March 1. Bitcoin Depot lost 50.9 BTC ($3.665M) from corporate settlement wallets on March 23 (or March 20 per ZachXBT's onchain tracing, which means the company did not notice for three days). Step Finance was a centralized portfolio dashboard but custodied user-facing assets.

NO MAJOR EXCHANGE EXPLOIT IN Q1 2026

That is the single most notable absence in the data. After the Bybit catastrophe in February 2025 (~$1.5B), centralized exchanges across the industry appear to have hardened multi-signature workflows, Safe Wallet UI, and signing infrastructure. The 98% year-over-year February drop is almost entirely a Bybit base effect, but the structural improvement at large CEXs is real.

SECTION 09

Emerging Threats

EIP-7702 Delegated Accounts

EIP-7702 went live as part of Ethereum's Pectra upgrade in mid-2025 and lets externally owned accounts temporarily delegate to smart-contract code. Q1 2026 produced the first cluster of protocol-level exploits abusing this feature.

Fusion by IPOR on January 6 was the first confirmed case. SlowMist's MistEye flagged the suspicious activity, and SlowMist explained the root cause: *"The underlying contract delegated by the EOA account controlled by the project team through EIP-7702 contains a vulnerability that allows arbitrary external [calls]."* CertiK Alert traced the $336K USDC drain from the Fusion PlasmaVault on Arbitrum. IPOR pledged to repay affected users and the funds were recovered through a white-hat with a 10% bounty.

PHISHING KITS ARE CATCHING UP FAST

Wintermute researchers reported that most EIP-7702 delegations on Ethereum mainnet point to contracts using identical code, "many of them built to automate fund theft." If you have an EIP-7702 upgraded account, audit the contract you delegated to before signing anything new.

AI-Era Supply Chain Attacks

Two of the most significant Q1 2026 incidents never touched a smart contract.

LiteLLM PyPI compromise – March 24

The threat actor group TeamPCP, which had already compromised Aqua Security's Trivy scanner on March 19 and Checkmarx KICS on March 23, used stolen PyPI credentials to publish malicious LiteLLM versions 1.82.7 and 1.82.8.

The packages were live for 40 minutes to three hours, during which they injected an obfuscated dropper that stole SSH keys, cloud provider credentials (AWS, GCP, Azure), Kubernetes configs, .env secrets, and crypto wallets, then installed a systemd persistence backdoor.

LiteLLM is a dependency for Stripe, Netflix, Google, CrewAI, DSPy, and MLflow integrations. If a DeFi project used LiteLLM in any AI-related backend during the exposure window, every credential on those machines should be considered compromised.

PyPI | 96.8M downloads/month | Credential Stealer | AI Infrastructure

axios npm compromise – March 31

Microsoft Threat Intelligence and Google Threat Intelligence Group attributed this attack to UNC1069 / Sapphire Sleet, a financially motivated North Korean state actor.

Two malicious axios versions (1.14.1 and 0.30.4) were live on npm from 00:21 to about 03:15 UTC, injecting a malicious dependency called plain-crypto-js@4.2.1 that deployed cross-platform RATs (named WAVESHAPER.V2 by Google) to macOS, Windows, and Linux. Huntress observed at least 135 endpoints contacting the attacker's command-and-control during the 3-hour window.

axios is downloaded 100+ million times per week. The blast radius is gigantic.

npm | 100M+ downloads/week | DPRK / UNC1069 | Cross-platform RAT

AI-Written Smart Contracts

Moonwell's $1.78M cbETH oracle misconfiguration on February 15 is the first major DeFi loss publicly tied to AI-co-authored Solidity. Smart contract auditor pashov first flagged the issue on X on February 17, 2026, posting: *"Claude Opus 4.6 wrote vulnerable code, leading to a smart contract exploit with $1.78M loss [...] Is this the first hack of vibe-coded Solidity code?"* He later told Cointelegraph that the commits showed "the developer was using Claude to write the code, and this has led to the vulnerability." SlowMist founder Cos described the formula error as a "very low-level bug" that human review or even basic integration testing should have caught. Audits had been performed but did not flag the issue.

Wrench Attacks Going Mainstream

The Sillytuna case on March 5 is the clearest Q1 2026 example. What began as an address poisoning scam involving aEthUSDC escalated, per multiple investigators, into a physical "wrench attack" that forced the victim to transfer roughly $24 million. The victim later announced their exit from crypto. CertiK's separate Wrench Attacks Report, published February 2 2026, called this category "a structural threat to digital asset ownership," organized rather than opportunistic and combining OSINT-driven targeting with extreme physical violence.

SECTION 10

Recovery Wins

For all the bad news, Q1 2026 saw some of the strongest white-hat and protocol response work in years.

INCIDENT	DATE	RECOVERY OUTCOME
Fusion by IPOR	Jan 6	Funds recovered via white-hat with a 10% bounty.
MakinaFi	Jan 20	$4.13M drained, of which roughly 920 ETH returned via MEV builder under SEAL Safe Harbor terms with a 10% bounty.
Step Finance	Jan 31	~$4.7M recovered through Solana Token22 protections and partner coordination ($3.7M Remora, $1M other).
IoTeX	Feb 21	40.5M IOTX blacklisted at chain level. 52.4M deposited to Binance with 41.6M routed through Easybit and ChangeNow for freezing.
Solv Protocol	Mar 5	Fewer than 10 users affected. Solv covered all losses from protocol reserves and offered a 10% bounty.
BONKfun	Mar 11	110% user compensation paid after the DNS hijacking attack.

THE HARD TRUTH

The very largest losses generated minimal recovery: the $282 million whale, Step Finance's $40M, Resolv Labs' $25M, Truebit's $26.44M, and Bitrefill's hot wallets. Once funds enter THORChain, Tornado Cash, RailGun, or convert to Monero on instant exchanges (as the $282M attacker did, briefly causing Monero to spike over 60%), they are gone for practical purposes.

SECTION 11

Lazarus and DPRK Activity Spotlight

Bitrefill blamed Lazarus/Bluenoroff for its March 1 attack based on malware similarities, reused IP and email addresses, on-chain tracing patterns, and the social engineering vector that started with a compromised employee laptop. About 18,500 customer purchase records were exposed (emails, crypto payment addresses, IP metadata, and 1,000 encrypted product names). Bitrefill said it would absorb the losses from operational capital.

The Block noted Lazarus often embeds fraudulent IT workers inside crypto services to gain privileged access. The same playbook has now appeared at Bybit (2025), Bitrefill (March 2026), and Drift Protocol (an April 2026 incident that began with five months of social engineering, falling outside Q1 but worth noting because the campaign started in Q4 2025).

Google's Threat Intelligence Group attributed the axios npm compromise on March 31 to UNC1069, a North Korea-linked financially motivated actor active since 2018, based on infrastructure overlap and the use of the WAVESHAPER.V2 backdoor.

CHAINALYSIS 2026 CRYPTO CRIME REPORT

"North Korean hackers stole $2.02 billion in cryptocurrency in 2025 — a 51% increase over 2024 — pushing their all-time total to $6.75 billion." The same report found that "North Korean hackers accounted for a record 76% of all service compromises." The Q1 2026 data suggests the DPRK shift toward operator and infrastructure compromise (rather than protocol exploits) is now permanent.

DPRK Activity Timeline – Q1 2026

DATE	TARGET	VECTOR	ATTRIBUTION
Mar 1	Bitrefill	Employee laptop compromise via social engineering	Lazarus / Bluenoroff (self-attributed by Bitrefill)
Mar 31	axios npm package	Maintainer credential compromise, malicious dependency injection	UNC1069 / Sapphire Sleet (Google TIG)
Ongoing	Multiple unidentified projects	Fake IT worker employment, privileged access compromise	Lazarus subgroup

SECTION 12

How to Protect Your Funds: 10 Lessons

Generic "use a hardware wallet" advice does not match the actual Q1 2026 attack data. The $282M January 10 victim was already using a hardware wallet. The attacker did not crack the device. They impersonated the support team. Here is what the data actually says you should do.

1 Assume you are being targeted if you hold more than $100K in crypto

Hardware wallets do not protect against social engineering. Anyone messaging you claiming to be from a wallet vendor, an exchange, or a project support team is, with very high probability, an attacker. Verify out of band, always.

2 Multisig is not optional above six figures

Across both Resolv Labs (single AWS KMS signer) and Step Finance (executive devices able to drain treasury), single-signer key control was the root cause. The fix is a 2-of-3 or 3-of-5 multisig with at least one offline signer.

3 Treat any DM on X, Telegram, or Discord as hostile by default

Eight or more crypto X accounts were compromised in Q1 2026 alone. If a "founder" you trust DMs you out of the blue with an opportunity, an airdrop, or a "private call," it is almost certainly stolen access being used to phish your network. Confirm via a second channel before clicking anything.

4 Revoke unused token approvals on every chain you use

The SwapNet/Aperture $17M loss happened to users who had granted infinite token approvals to those routers. The arbitrary-call vulnerability turned every infinite approval into a drain target. Use revoke.cash or Etherscan's token approval checker monthly. Prefer Permit2 with scoped allowances over unlimited approvals.

5 Watch out for EIP-7702 delegations

If you have an EIP-7702-upgraded account, audit the contract you delegated to before signing anything new. Phishing kits already automate the abuse of EIP-7702 batch transactions to hide drains inside what looks like a normal approval.

6 Pin your dependencies and audit your CI/CD pipeline if you build

The Trivy → LiteLLM → axios cascade in March showed that one poisoned upstream tool can hand attackers the keys to thousands of downstream projects. Pin to cryptographic hashes. Disable auto-updates for security-sensitive packages. Adopt OIDC-based trusted publishing rather than long-lived API tokens.

7 Diversify custody

If you keep funds across UPay, a centralized exchange, and a self-custody wallet, no single operational failure wipes you out. Step Finance users learned this the hard way.

8 Cold-storage seed-phrase hygiene matters more than ever

Do not type your seed phrase into anything except the hardware wallet's recovery flow. Do not photograph it. Do not store it in a password manager. Do not enter it on a "support" website. The $282M victim's attacker did not bypass Trezor, they bypassed the human.

9 Read protocol post-mortems before depositing

Venus Protocol had a documented donation-attack vulnerability flagged in an August 2023 Code4rena audit that the team disputed at the time. The same class of bug drove the March 15 $3.7M exploit. Moonwell had two oracle-misconfiguration incidents in four months. Solv Protocol's BRO vault was unaudited. Past behavior is the single best predictor of future incidents.

10 Stablecoin holders, watch for protocol-level contagion

The Resolv Labs depeg cascaded into bad debt at Morpho, Euler, and Fluid. If you hold positions in lending vaults that allow exotic stablecoins as collateral, you are exposed to whatever happens to those collateral assets, not just to the lending protocol itself.

SECTION 13

Outlook for Q2 2026

A few directional calls based on Q1 patterns. Treat these as analyst views, not certainties.

1. **Operator and infrastructure attacks will keep expanding.** The economics for sophisticated attackers now strongly favor compromising teams, CI/CD pipelines, DNS providers, and cloud key vaults over hunting for novel Solidity bugs. Expect more incidents like Resolv Labs and Step Finance.

2. **EIP-7702 exploits will scale up in dollar terms.** Q1's $336K Fusion incident was a proof of concept. The pattern at scale will combine phishing with malicious delegate contracts.

3. **Bridge exploits remain the highest single-event tail risk.** Q1 2026 was quiet by bridge standards, with only IoTeX and CrossCurve at meaningful size. The structural weaknesses (single validator keys, oracle quorum thresholds set to one, asynchronous source-destination verification) have not changed since 2022.

4. **DPRK activity will keep shifting upstream.** Bitrefill, the axios npm attack, and Drift's months-long social engineering campaign all started in Q1 2026 or earlier. Expect more attempts to plant insiders inside crypto teams and to compromise widely used open source libraries.

5. **Whale-targeted social engineering will get worse.** The $282M Jan 10 incident, the Kraken whale loss in March (~$18M), and Sillytuna's $24M wrench attack all targeted individuals rather than protocols. As crypto wealth concentrates, so does the criminal targeting.

THE Q1 2026 BOTTOM LINE

Q1 2026 was not a quiet quarter. It was a quarter in which the attack surface shifted faster than most users adapted. The headline that "smart contract losses are down 89% year-over-year" is true and important, but it does not mean crypto is safer. It means the threat moved.

For UPay readers using crypto cards and payments daily, the practical implication is that the boring stuff (account hygiene, device security, withdrawal whitelists, multi-channel verification, revoked approvals) now matters more than the exciting stuff (audited contracts, formal verification, bug bounty programs). **The protocols are getting safer. The humans operating them, and the humans using them, are now the target.**

SECTION 14

Methodology and Caveats

Data sources

This report is built from primary incident data published by PeckShield, CertiK, SlowMist, Halborn, Immunefi, Chainalysis, BlockSec Phalcon, Cyvers Alerts, Hacken, and Beosin. Cross-checks were performed against The Block, CoinDesk, Decrypt, Rekt News, and Cointelegraph coverage of specific events.

Scope

The report covers incidents from January 1, 2026 to March 31, 2026 inclusive. Incidents that began before January 1 but were disclosed in Q1 (such as Drift Protocol's months-long social engineering campaign that surfaced in April) are noted but not counted toward Q1 totals.

Caveats

- **Figures vary by source.** CertiK puts March at $59.5M; PeckShield puts it at $52M. CertiK puts the January whale at $284M; ZachXBT puts it at $282M+. These reflect scoping differences (incident inclusion thresholds, asset valuation timing, whether wrench attacks and phishing are counted), not data quality issues. Where figures conflict in this report, the more conservative figure is used.
- **The $501M total is dominated by one incident.** Strip the $282M January 10 whale out and the quarter's individual and protocol exploit losses combined are closer to $220M, which is the lowest level since 2020 in inflation-adjusted terms.
- **State attribution is inferential.** Attribution of state-sponsored activity (Lazarus, Bluenoroff, UNC1069, Sapphire Sleet, TraderTraitor) relies on indicators (malware overlap, reused IPs, on-chain patterns) rather than confirmed identification. The FBI publicly attributed the 2025 Bybit hack. Bitrefill's Lazarus attribution is the company's own assessment based on similar indicators.
- **The Q2 outlook is analyst commentary.** Subsequent April 2026 events (Drift Protocol $285M, KelpDAO $290M) are outside Q1 scope but suggest the threat trajectory is accelerating, not slowing.

Disclaimer

This report is published for informational purposes only. It does not constitute investment, legal, or security advice. UPay Research compiles publicly available information and adds analysis; readers are responsible for their own security decisions. Specific protocol mentions are not endorsements or warnings about future safety. Past security incidents do not guarantee future incidents.

PUBLISHED BY UPAY RESEARCH

For crypto card and payment users who want to keep their funds safe.

© 2026 UPay. All rights reserved. Q1 2026 Crypto Hack Trend Report.