RESONANCE // 2025

Web3 Cybersecurity Report

A comprehensive review of hacks, exploits & learnings

RESONANCE // 2025

TABLE OF CONTENTS

RESONANCE SECURITY™

RESONANCE // 2025

EXECUTIVE SUMMARY

The **2025 Web3 Cybersecurity Report** presents a comprehensive, month-by-month analysis of all major and minor security incidents across the crypto and Web3 ecosystem from **January to December 2025**. Covering centralized exchanges, DeFi protocols, bridges, wallets, NFTs, social layers, and individual user losses, the report documents how attackers exploited not just smart contract vulnerabilities, but also governance flaws, key management failures, infrastructure weaknesses, and human behavior. Each incident is analyzed through a consistent framework (what happened, how it happened, the root cause, and the real-world impact) offering a complete forensic view of the year's threat landscape.

This report is designed to serve both as a **historical record** and a **practical reference** for founders, developers, auditors, investors, and security teams. By mapping incidents across ecosystems and attack categories, it reveals clear patterns in attacker behavior and systemic weaknesses in Web3 security architecture. The insights contained here are intended not only to explain what went wrong in 2025, but to help the ecosystem **avoid repeating the same mistakes in 2026 and beyond.**

RESONANCE // 2025

NOTABLE HACKS OF 2025

January

phemex | January 2025

Phemex Exchange

A centralized crypto exchange used for spot and derivatives trading services globally.

Amount Lost: $69.1M (some analyses cite ~$73M depending on attribution/valuation)

How It Happened

1. Attackers drained hot wallets across multiple networks after suspicious outflows were detected.
2. The pattern matches a classic “CEX hot wallet compromise” where the attacker can sign/authorize withdrawals from exchange-controlled wallets.

Root Cause

- Compromised private keys / key-management failure for hot wallets (keys stored/accessible in a way that allowed theft at scale).

Impact

- Large-scale asset loss from hot wallets.
- Emergency incident response (pauses/monitoring, forensic tracing, user comms).
- Reputational damage + heightened scrutiny on exchange custody/key ops.

Moby | January 2025

Moby Trade

A DeFi trading protocol (perps-style) with liquidity pools (sOLP/mOLP).

Amount Lost: $2.5M (with ~$1.47M USDC recovered per report)

How It Happened:

1. An attacker leveraged a leaked private key to execute a malicious smart contract upgrade, triggering an emergency withdrawal of user funds.
2. Moreover, the public summaries in widely-cited sources don't consistently publish a detailed step-by-step exploit path for this one.

Root Cause

1. Privileged key compromise (upgrade/admin control). In upgradeable systems, that single key effectively becomes the "god mode" for fund safety.

Impact

- Exposure/drain of pool assets (wBTC, wETH, USDC cited).
- Partial recovery assisted by external responders.
- Emergency response: pauses, key rotation, post-mortem, user comms.

---

noOnes | January 2025

NoOnes (Crypto Platform)

A crypto services platform (includes P2P trading and other services) that had a Solana bridge component involved in the incident.

Amount Lost: $7.9M-$8M

How It Happened

- An exploit of the Solana bridge led to theft from hot-wallet infrastructure.
- The team stated the bridge exploit was contained and disabled quickly.

Root Cause (Likely)

- Bridge/security control failure enabling unauthorized movement of funds through the Solana bridge path (exact technical exploit chain not fully public).

Impact

- Multi-million dollar loss tied to bridge/hot-wallet exposure.
- Forced shutdown/containment action on bridge components.
- Reputational impact and user trust stress.

orange | January 2025

Orange Finance (DeFi, Arbitrum Liquidity Management)

An Arbitrum-based DeFi liquidity management and yield optimization protocol.

Amount Lost: $830K-$840K

How It Happened:

- A misconfigured multisig / ownership setup allowed the attacker to gain control of vaults, modify implementations, and withdraw deposited assets; a smaller slice of losses came from excessive token approvals.
- Team warned users not to interact with the contracts because "the contract is no longer Orange."

Root Cause

- Governance/ownership misconfiguration (privilege boundary failure) + unsafe approval hygiene.

Impact

- Direct loss of vault TVL.
- Forced pause + incident response and migration work.
- User trust damage + re-audit/controls hardening.

NO LOGO AVAILABLE | January 2025

IPC (BSC Token/Project)

(Not a widely known DeFi project with very limited information available on the surface web.)

Amount Lost: $554.9K-$590K (sources vary slightly)

How It Happened:

- Exploit involved bypassing protections (reported as bypassing flash-loan protection) and abusing token mechanics to extract value.

Root Cause

- Contract logic weakness (protective checks/assumptions bypassable under adversarial execution ordering).

Impact

- Liquidity/value extraction from the ecosystem.
- Likely trading disruption and token volatility.
- Emergency mitigations + contract changes/redeploys.

January 2025

UniLend Finance (DeFi Lending)

A DeFi lending protocol (UniLend V2 on Ethereum, referenced in analyses) enabling permissionless asset markets.

Amount Lost: $197K-$200K

How It Happened:

- Exploit in the redeem/health factor validation flow.
- Analysis describes a scenario where incorrect health factor validation / stale balance logic lets an attacker bypass proper collateral safety checks (flash-loan style behavior is commonly referenced in analyses).

Root Cause

- Business-logic flaw in collateral/health factor calculation during redemption (using old balance state / incorrect validation).

Impact

- Direct loss (stETH value referenced in analysis).
- Deposits warned/paused for the affected version while remediation proceeded.
- Reputation hit + requirement for deeper invariant testing around redemption paths.

January 2025

The Idols NFT (NFT Project on Ethereum)

An Ethereum-based NFT project with a rewards mechanism tied to transfers/claims.

Amount Lost: $340K (in stETH)

How It Happened:

- Exploit leveraged a self-transfer / transfer hook logic bug.
- Repeated self-transfer manipulated _beforeTokenTransfer reward accounting, enabling repeated/incorrect reward claims.

Root Cause

- Reward accounting logic flaw on transfers (failure to correctly handle sender=receiver or snapshot resets), enabling repeated claims.

Impact

- Reward pool drained (~$340K stETH).
- Secondary market confidence hit.
- Highlights typical NFT “reward hook” risk: transfer callbacks + state accounting edge cases.

January 2025

Sorra Finance (Staking Contract Exploit)

A DeFi staking/rewards setup for the Sorra token ecosystem.

Amount Lost: $41K (reported as ~3.07M SOR tokens valued around that at the time)

How It Happened:

- A flaw in reward calculation allowed repeated withdrawal of rewards due to missing "already distributed" tracking in the pending rewards logic.

Root Cause

- Rewards accounting bug (pending rewards function failed to properly account for previously distributed rewards).

Impact

- Reward drain from the staking contract.
- Contract trust breakdown for stakers.
- Forces redesign of reward bookkeeping + tests for double-claim scenarios.

Incidents widely cited in January totals, but with limited public technical detail in mainstream summaries. ***These are named in multiple roundups, but the public "how/root-cause" details aren't consistently published in the broadly referenced sources.***

NO LOGO AVAILABLE

January 2025

LAURA (Token / Project)

A token crypto project on Ethereum.

Amount Lost: $48.2K

How It Happened:

- Tracked as a contract vulnerability exploit leading to value extraction.

Root Cause (Likely)

- Reported as a token mechanics / liquidity-related vulnerability (details vary by write-up; not always standardized across public sources).

Impact

- Direct financial loss and token market disruption.
- Liquidity/provider confidence hit.
- Pressure to harden token logic + add monitoring for abnormal LP events.

January 2025

Odos (DEX Aggregator)

A DEX aggregator / routing protocol.

Amount Lost: $98K (As Reported)

How It Happened:

- Public reporting indicates a targeted exploit with limited blast radius (exact execution path is not known).

Root Cause (Likely)

- Smart contract vulnerability (not fully disclosed).

Impact

- Limited direct losses vs. CEX-scale incidents.
- Rapid response + monitoring rule updates.
- Increased user caution around approvals/routes.

January 2025

Pika Infinity (DeFi)

A web3 infrastructure that integrates gaming, a launchpad, and a suite of decentralised services.

Amount Lost: Included in the smaller-loss bracket in January rollups (reported range across the "smaller incidents" bucket: ~$43K to $330K)

How It Happened:

- Not consistently detailed in the open rollups that mention it.

Root Cause

- Undisclosed / insufficient public data.

Impact

- Localized liquidity loss.
- Likely contract pause + remediation.

January 2025
Alien Base (DeFi, Base Ecosystem)

Base-chain DeFi project; incident cites a specific contract (BunniHub).

Amount Lost: $38K

How It Happened:

- Multiple exploit transactions targeted a contract component (BunniHub).

Root Cause (Likely)

- Contract vulnerability (public writeup minimal).

Impact

- Limited but real pool loss.
- Heightened scrutiny on Base DeFi contract quality.

NO LOGO AVAILABLE

January 2025
FortuneWheel (BSC)

BSC project (small).

Amount Lost: $21.6K

How It Happened:

- Classified as price manipulation (likely thin-liquidity/AMM manipulation).

Root Cause

- Economic design weakness (insufficient anti-manipulation controls/oracle defenses).

Impact

- LP losses / volatility spike.
- Reputation hit; likely contract/parameter changes.

NO LOGO AVAILABLE

January 2025

Mosca (BSC)

BSC token/project (small).

Amount Lost: $19.5K

How It Happened:

- Reported as a contract vulnerability incident.

Root Cause (Likely)

- Smart contract flaw (details not public).

Impact

- Localized liquidity loss + price shock.

NO LOGO AVAILABLE

January 2025

HORS (BSC)

BSC token/project (small).

Amount Lost: $10.3K

How It Happened:

- Classified as contract vulnerability exploit.

Root Cause (Likely)

- Smart contract flaw (minimal public detail).

Impact

- Small but real user/LP losses.

NO LOGO AVAILABLE

January 2025

BUIDL (BSC)

BSC token/project (small).

Amount Lost: $8K

How It Happened:

- Tracked as a contract vulnerability exploit.

Root Cause (Likely)

- Smart contract flaw

Impact

- Minor liquidity hit; reputational damage.

RESONANCE // 2025

NOTABLE HACKS OF FEBRUARY

BYBIT | February 2025
Bybit (CEX)

A top global centralized crypto exchange used for spot/derivatives trading and custody.

Amount Lost: $1.4B-$1.5B (largest known crypto heist)

How It Happened:

Attackers targeted Bybit's cold-wallet signing flow and executed a transaction that moved a massive ETH position out in one sweep.

- Multiple investigations and summaries attribute it to operational/security-process failure rather than a typical smart contract bug.

Root Cause

- A human-in-the-loop signing failure: attackers manipulated what signers believed they were approving (a "looks safe" approval that wasn't), enabling a high-value transfer from custody wallets.

Impact

- Massive immediate loss + industry-wide "flight to safety" behavior across exchanges.
- Incident became a benchmark case for approval UX, signer verification, and malware-resilient ops.
- Large-scale tracing/attribution efforts publicly tied the event to sophisticated threat actors.

INFINI | February 2025

Infini (Stablecoin Neobank)

A crypto neobank / payments-card issuer positioning as a bridge between TradFi-style payments and crypto rails; also offered vault/earn products.

Amount Lost: $49.5M

How It Happened:

- Reports describe an attacker gaining control of admin-privileged access and draining funds (large USDC outflows swapped into DAI/ETH and moved to fresh wallets).
- Multiple write-ups point to access control / retained privileges consistent with an insider/ contractor risk.

Root Cause

- Access-control failure / privileged key management (admin permissions were not fully revoked or were mishandled).

Impact

- Significant user fund losses and trust collapse.
- Raise fresh scrutiny around offboarding, role revocation, and treasury controls.
- Secondary contagion: fear-driven withdrawals / risk-off sentiment around similar "yield" operators.

---

zkLend | February 2025

zkLend (DeFi Lending on Starknet)

A lending/money-market protocol on Starknet where users supply and borrow crypto assets.

Amount Lost: $9.5M-$9.57M

How It Happened:

- The attacker exploited a decimal precision / rounding vulnerability tied to internal accounting (accumulator + mint/withdraw math).
- By manipulating an empty market + donations and repeating deposit/withdraw cycles, they inflated internal balances and borrowed/drained other pools.

Root Cause

- A rounding/precision bug in core accounting logic (division/rounding behavior), which allowed the attacker to create profitable state transitions that protocol treated as valid.

Impact

- Immediate fund drain + protocol risk controls tightened.
- Sparked broader review of fixed-point arithmetic and accumulator design on L2s.
- Increased demand for invariant-based testing and adversarial simulations in audits.

February 2025

Ionic Money (aka Midas) on Mode (DeFi Lending/Borrowing)

A DeFi lending market on Mode (L2 ecosystem), where users borrow against collateral.

Amount Lost: $6.9M

How It Happened:

- A major write-up describes a month-long social engineering: the attacker persuaded the team to add a fake LBTC-like token, then minted a large amount and used it as collateral to drain liquidity/borrow real assets.

Root Cause

- Asset onboarding / verification failure (weak checks for "is this collateral real/legit?"), combined with governance/ops processes that allowed a malicious listing.

Impact

- Direct protocol solvency damage (bad debt) + user confidence hit.
- Reputational damage amplified by the "trust/process" nature of the compromise.
- Forced tighter controls on listing pipelines, allowlists, and issuer verification.

February 2025

Four.Meme (Memecoin Launchpad/Ecosystem Project)

A memecoin/launch-related project in the on-chain trading ecosystem (users interact with token creation/trading flows).

Amount Lost: $183K

How It Happened:

- Attacker pre-created a PancakeSwap v3 pool with an extremely skewed price.
- When the token was integrated, liquidity was added following that manipulated pool state.
- Because price validation checks were missing, attacker drained assets via the bad-price pool setup.

Root Cause

- Business logic / integration flaw: the system trusted an attacker-prepared pool's price state, and didn't enforce sanity checks when adding liquidity.

Impact

- Direct liquidity loss + temporary disruption of launches.
- Forced tighter guardrails around pool initialization, price bounds, and integration validation.
- Increased scrutiny of "launchpad → AMM" automation flows.

Incidents widely cited in February totals, but with limited public technical detail in mainstream summaries. ***These are named in multiple roundups, but the public "how/root-cause" details aren't consistently published in the broadly referenced sources.***

WEMIX | February 2025
WEMIX (Gaming Project)

WEMIX is a blockchain/gaming ecosystem project (Wemade-linked ecosystem brand).

Amount Lost: $6.2M

- How It Happened (summary)?
- Public trackers label it as "seems hacked," but detailed post-mortem mechanics weren't broadly published in the same canonical way as the largest incidents.

Root Cause

- Not fully disclosed publicly

Impact

- Treasury/user loss (reported), plus ecosystem trust hit.
- Likely prompted internal key/ops review and incident response actions.

Cardex | February 2025
Cardex (Project/Protocol)

An AI-powered cryptocurrency payment platform that enables real-time crypto-to-fiat conversions.

Amount Lost: $400K

How It Happened:

- Public summaries classify it as an exploit/drain event with limited postmortem detail (typical of small-cap incidents).

Root Cause (Likely)

- Likely contract exploit or compromised operational access (insufficient public technical disclosure).

Impact

- User fund loss.
- Liquidity shock/LP disruption
- Elevated counterparty risk perception for similar small protocols.

NO LOGO AVAILABLE

February 2025

LIBRA (Memecoin)

The “LIBRA” token, a politically hyped meme token launched on social media.

Amount Lost: $250M (reported as losses tied to the crash/rug dynamic)

How It Happened:

- Token was promoted publicly, price spiked rapidly, then suffered a severe collapse consistent with rug/pump-and-dump dynamics.

Root Cause (Likely)

- Market-structure + insider/issuer control risk (exit scam).

Impact

- Large retail drawdown event.
- Political/social amplification became part of the damage story.
- More pressure for exchange/listing diligence and disclosure norms.

NO LOGO AVAILABLE

February 2025

Cashverse (BSC Project)

A unique passive income crypto project with play-to-earn game and all-in-one platform.

Amount Lost: $107.9K

How It Happened:

Incident reported as a quick fund-drain style exploit; deep technical details were not broadly published.

Root Cause (Likely)

Unclear publicly (likely contract weakness or key/role compromise; no detailed postmortem found in major summaries).

Impact

- User losses.
- Liquidity instability and trust damage.
- Increased scrutiny of project security posture.

BANXA

February 2025

BankX (BSC / ETH / Optimism)

A cross-chain DeFi project (not much about the protocol is available on the surface web).

Amount Lost: $43K

How It Happened:

Flagged as suspected exploit across BSC, Ethereum, and Optimism; categorized as contract vulnerability.

Root Cause (Likely)

- Not sufficiently disclosed publicly.

Impact

- Multi-chain incident response required.
- Short-term trust hit; likely prompted deployments/permission tightening.

NO LOGO AVAILABLE

February 2025

GoldReserve NFT (NFT Project)

A gold reserve elite NFT collection.

Amount Lost: $8.5K

How It Happened:

- Public notes describe it as reward manipulation (light technical detail available publicly).

Root Cause (likely)

- Incentive/reward logic manipulation (insufficient anti-abuse checks).

Impact

- Small direct financial loss, but outsized trust impact for NFT communities.
- Increased suspicion on reward mechanics + claim contracts.

RESONANCE // 2025

NOTABLE HACKS OF MARCH

March 2025

Abracadabra (DeFi Lending)

A DeFi lending/borrowing protocol best known for the Magic Internet Money (MIM) stablecoin and collateralized debt positions.

Amount Lost: Reported in incident trackers as a multi-million dollar exploit (commonly cited around $13M)

How It Happened:

- Reported as a flash-loan-enabled exploit abusing a bug in the protocol's smart contracts, resulting in ~$13M theft and conversion/exit into ETH.

Root Cause

- Smart contract bug exploitable via composable DeFi interactions (flash loans used to amplify attack path).

Impact

- Protocol treasury/contract funds drained (notable TVL shock).
- Risk repricing for MIN-related positions.
- Renewed attention on complex DeFi integrations and audit depth.

March 2025

1inch (DEX Aggregator)

A widely used DEX aggregation and routing protocol that sources liquidity across DEXs.

Amount Lost: Approximately $5M reported (with partial recovery/freeze efforts noted by trackers/reporting)

How It Happened:

- Attacker exploited a vulnerability tied to obsolete Fusion v1-based resolver contracts, draining USDC + WETH.
- Funds affected were reported as belonging to resolvers (order fillers) rather than end users.

Root Cause

Use of obsolete/legacy implementation in production paths (insufficient hardening/controls around their Fusion v1 smart contracts).

Impact

- Direct financial loss and operational disruption.
- Resolver confidence hit; stricter resolver security expectations.
- Increased scrutiny on legacy modules still reachable in production.

March 2025

Pond.fun (Launchpad)

A memecoin launchpad on Linea.

Amount Lost: $145,000

How It Happened:

Project disclosed evidence pointing to an insider incident: the lead software engineer allegedly drained liquidity from the smart contract and sold project tokens.

Root Cause

Insider manipulation / privileged access abuse (insufficient separation of duties + key management + deployment controls).

Impact

- Liquidity drained; token sell pressure.
- Reputation damage (insider risk narrative).
- Likely team restructuring + access revocations.

March 2025

Berally (Berachain Ecosystem)

Social trading platform using AI agents in the Berachain ecosystem.

Amount Lost: $86,725

How It Happened:

- Project stated deployer key information leaked, which enabled attackers to dump vesting tokens and pull liquidity; dApp contract reportedly unaffected.

Root Cause

- Private key leakage (deployer/vesting/liquidity control exposure).

Impact

- Liquidity/price shock from token sell-off.
- Emergency revokes requested; trust hit.
- Highlights deployer-key operational risk.

March 2025

SIR.trading (DeFi/Perps-Style Trading)

A DeFi trading protocol (leveraged trading/perps-style product).

Amount Lost: Reported as a six-figure loss (trackers + postmortem discussions widely cite ~$300k-$400k range)

How It Happened:

- Exploit involved transient storage (tstore) behavior: a transiently stored value used for permissioning was not cleared, letting an attacker craft malicious addresses to bypass checks and transfer tokens.

Root Cause

- State/permissioning bug tied to transient storage lifecycle assumptions (failure to reset/clear transient values).

Impact

- Loss of protocol funds and forced mitigation actions.
- Confidence damage typical for early-stage trading protocols.
- Security spotlight on newer EVM patterns and misuse risks.
- Likely triggers code refractor + formal verification focus for auth logic.

Zoth | March 2025
Zoth: Attack #1 (RWA/Structured-Yield Protocol)

A protocol positioned around RWA / yield / vault-style products.

Amount Lost: $285,000

How It Happened:

- Attacker exploited a bug in collateral calculations, manipulating how the system accounted for collateral and value, then extracted profit.

Root Cause

- Smart contract logic flaw in collateral/value accounting (insufficient validation of collateral received vs assumed).

Impact

- Loss of protocol funds/LP value.
- Immediate trust hit for a “RWA + restaking” narrative product.
- Forced incident response and monitoring upgrades.

Zoth | March 2025
Zoth: Attack #2 (RWA/Structured-Yield Protocol)

A protocol positioned around RWA / yield / value-style products.

Amount Lost: $8.29M

How It Happened:

- Attacker obtained admin privileges, upgraded a proxy/logic contract to a malicious implementation, withdrew large amounts (notably USD0++ exposure reported), then swapped into other assets ending with thousands of ETH-equivalent value.

Root Cause

- Admin/private key leakage enabling malicious upgrade + weak privilege protection around upgradeability.

Impact

- Additional losses shortly after/around the earlier Zoth exploit.
- Increased user distrust and likely liquidity flight.
- Highlights upgradeable-contract governance/key custody as existential risk.

March 2025

Voltage Finance (Fuse Ecosystem DEX / DeFi)

A DeFi protocol in the Fuse ecosystem (DEX/liquidity + related contracts).

Amount Lost: $320,000 (USDCE + WETH)

How It Happened:

- Unauthorized withdrawals from Simple Staking pools resulted in two main asset losses (USDCE and WETH). Project published a transparency postmortem.

Root Cause

- Contract vulnerability in staking pool withdrawal/security controls (per incident classification/ postmortem framing).

Impact

- Liquidity disruption + user trust loss in Fuse DeFi.
- Security + operational remediation and disclosure pressure.

March 2025

Min Token (MIN) (BNB Chain)

A token project on BNB Chain (BSC).

Amount Lost: $21,415

How It Happened:

- Reported as price manipulation, consistent with thin-liquidity exploitation / pool manipulation to siphon value

Root Cause

- Market/oracle design weakness (spot-price reliance + low-liquidity pools enabling manipulation).

Impact

- LP/treasury losses (small but real).
- Demonstrates how “small caps” get hit via cheap manipulation.
- Reinforces need for oracle hardening + liquidity protections.

Incidents widely cited in March totals, but with limited public technical detail in mainstream summaries. ***These are named in multiple roundups, but the public "how/root-cause" details aren't consistently published in the broadly referenced sources.***

NO LOGO AVAILABLE

March 2025

WeKey

Sufficient information about the project is not available on the surface web.

Amount Lost: ~$700,000

How It Happened:

- Public roundups cite the loss figure, but don't consistently publish a full technical postmortem or universally accessible transaction-level breakdown.

Root Cause (Likely)

- Not clearly established publicly.

Impact

- Direct fund loss.
- Uncertainty increases reputational damage (no clear narrative = worst narrative).
- Puts pressure on project/team for transparency and remediation steps.

Hyperliquid

March 2025

Hyperliquid (Trading Project)

Decentralized perpetuals trading venue; HLP vault acts as a market-making/liquidity backstop.

Amount Lost: $4,000,000 (reported vault losses)

How It Happened:

- Reports describe a whale/trader using position sizing + collateral withdrawal/liquidation mechanics to offload losses onto the HLP vault.
- Hyperliquid publicly denied a smart-contract "hack", framing it as economic/mechanics exploitation rather than code execution.

Root Cause

- Mechanism-design weakness (liquidation/margin system allowed losses to be socialized to the vault under certain behaviors), plus ambiguity over whether to classify as "exploit" vs "trade outcome".

Impact

- LP/vault participants absorbed losses (~$4M).
- Reputation hit and "CeDeFi vs DeFi" debate reignited.
- Pressure to redesign margin/liquidation and risk parameters.

RESONANCE // 2025

NOTABLE HACKS OF APRIL

April 2025

UPCX (Payments Platform)

An open-source crypto payments network/platform.

Amount Lost: $70M (18.4M UPC withdrawn)

How It Happened:

- Attacker gained control of a privileged/management address (likely key compromise).
- Used that privilege to perform a malicious ProxyAdmin upgrade.
- Called an admin withdrawal function (withdrawByAdmin) to drain UPC from multiple management accounts.
- Platform halted deposits/withdrawls while investigating.

Root Cause

- A privileged/ key/account compromise (or equivalent unauthorized admin access) that enabled an upgrade + admin withdrawal path; this is a governance/key-management failure more than a "bug-only" exploit.

Impact

- Large treasury/management funds drained.
- Deposits/withdrawls paused; user confidence hit.
- Incident highlighted single-point-of-failure risk in upgrade/admin controls.
- Follow-on risk of copycat attacks on similar ProxyAdmin setups.

KiloEx | April 2025

KiloEx (Multi-Chain Perps DEX)

A decentralized perpetual futures exchange deployed across chains.

Amount Lost: $7.5M - ~$8.44M

How It Happened:

- Attacker abused a publicly accessible forwarder/execution path.
- Crafted calls that reached the price-setting pathway and manipulated oracle prices.
- Opened and closed positions against fake prices to extract profit.
- Attack executed across multiple deployments/chains.

Root Cause

- Access control design break (the "forwarder/execute" path allowed attacker-controlled calldata/signature context to reach sensitive price update logic).

Impact

Multi-chain loss event; liquidity/market disruption.

Emergency response, negotiations, and coordination with security firms/exchanges.

- Highlighted how "one weak link" in a call chain breaks otherwise strong controls.
- Increased scrutiny of meta-tx forwarders and keeper/price-feed architecture.

---

zkSync | April 2025

zkSync (L2) - Airdrop "Unclaimed Tokens" Admin Compromise

An Ethereum Layer-2 scaling network (zk rollup).

Amount Lost: $5M in ZK (unclaimed airdrop allocation), with 90% returned under a bounty arrangement

How It Happened:

- A privileged admin account tied to airdrop distribution was compromised.
- Attacker gained control over unclaimed token handling.
- Security Council issued an on-chain safe-harbor offer (return 90%, keep 10%).

Root Cause

- Privileged account compromise around token distribution controls (security boundary failure on admin ops, not a base L2 consensus break).

Impact

- Short-term supply/market fear (airdrop token integrity concerns).
- Governance/security council intervention + public bounty negotiation.
- Operational hardening pressure for admin key management.
- Reputational hit despite patrial recovery.

Loopscale | April 2025

Loopscale (Solana Lending Market)

A modular DeFi lending protocol on Solana.

Amount Lost: $5.8M (5.7M USDC + ~1,200 SOL), later fully returned per reports

How It Happened:

- Attacker targeted how Loopscale priced RateX PT (principal token) collateral.
- Used mispricing to take undercollateralized borrows.
- Extracted funds from affected vaults.
- Negotiation/bounty led to return of assets.

Root Cause

- A collateral pricing/oracle logic flaw (isolated to Loopscale's RateX-based collateral valuation, enabling borrow power to exceed real collateral value).

Impact

- Temporary pause/disruption of lending operations.
- Loss concentrated to specific vaults/markets (protocol-level risk realization).
- Recovery reduced net damage but didn't remove trust impact.
- Strong lesson: collateral valuation needs adversarial modeling not just "reasonable pricing."

TERM | April 2025

Term Finance / Term Labs (Fixed-Rate Lending)

A fixed-rate lending market on Ethereum.

Amount Lost: 918 ETH affected

How It Happened:

- During an oracle update, a decimal precision inconsistency occurred.
- tETH pricing was wrong, triggering unintended liquidations.
- Team negotiated to recover a portion of impacted value.
- Protocol treasury planned to cover remaining hole (per reports).

Root Cause

- Human/operational error during a sensitive oracle upgrade (misconfiguration/precision mismatch), leading to systemic mispricing and cascading liquidations.

Impact

- Forced liquidation and user/protocol losses.
- Immediate reputational and risk-model damage.
- Reinforced need for staged rollouts, circuit breakers, and dual-oracle sanity checks.
- Recovery efforts reduced loss but didn't erase confidence shock.

numa. | April 2025

Numa (NumaMoney) (Arbitrum DeFi Protocol)

LST-backed synthetic assets / DeFi protocol on Arbitrum.

Amount Lost: $506K - $530K

How It Happened:

- Attacker used flash liquidity across venues to manipulate NUMA-related pricing.
- Exploited the protocol's pricing/validation assumptions in core vault logic.
- Extracted value and moved funds (bridging + privacy tooling cited in some reports).
- Post-event analysis showed the exploit was detectable minutes prior.

Root Cause

- Price manipulation exposure: insufficient real-time validation / slippage protection and reliance on internally derived pricing that could be skewed with flash liquidity.

Impact

- Direct asset loss and urgent incident response.
- Users questioned "zero-slippage" / pricing guarantees.
- Renewed focus on oracle hardening + MEV/flash-loan adversirial testing.
- Copycat risk for similar valut/oracle designs.

April 2025

Impermax V3 (Base DeFi Lending Against UniV3 LP)

DeFi lending that allows borrowing against Uniswap V3 LP positions.

Amount Lost: ~$300K - ~$400K (and additional funds at risk at the time)

How It Happened:

- Attacker used a flash loan to manipulate conditions around UniV3 LP valuation.
- Exploited an edge-case in collateral value / fee / tick-related calculations.
- Borrowed against inflated/incorrect collateral accounting.
- Drained funds from affected V3 pools.

Root Cause

- A valuation edge-case in handling Uniswap V3 LP positions (collateral math/fee accounting under adversarial swaps), enabling borrowing beyond safe limits.

Impact

- V3 pools drained; users warned to avoid interaction.
- Postmortem + mitigations required (valuation and liquidation logic).
- Base ecosystem confidence hit for LP-collateral lending designs.
- Increased demand for formal verification / simulation on LP math.

April 2025

Zora (Base Creator/NFT Ecosystem) - Airdrop Claim Exploit

Creator/NFT ecosystem with token distribution components.

Amount Lost: $128K

How It Happened:

- A flaw in the claim flow allowed misuse of signature-based claiming.
- Attacker abused weak checks around who can claim to whom.
- Used transaction routing/settlement mechanics to execute the drain efficiently.
- Extracted tokens from the claim contract path.

Root Cause

- Weak claim validation (authorization/recipient constraints in claim logic were insufficient), enabling a crafted claim to redirect value.

Impact

- Loss from distribution/claim pipeline.
- Trust hit for token claim contracts (a common, repeated failure point).
- Emergency pathing and ecosystem-wide code reviews of claim patterns.
- Increased skepticism around "rushed" airdrop tooling.

NO LOGO AVAILABLE

April 2025

Bitcoin Mission (Arbitrum)

A web3 project on Arbitrum (incident analyzed publicly by security monitoring).

Amount Lost: $1.3M

How It Happened:

- Attacker exploited a caller validation weakness in a function path ("OverPaper" cited).
- Executed hundreds of transactions over multiple days to extract funds.
- Drained assets systematically rather than a single one-shot hit.
- Attack pattern was observable through monitoring signals.

Root Cause

- Authorization bug (call validation logic insufficient), allowing an attacker-controlled caller to trigger value-moving actions repeatedly.

Impact

- Significant treasury/contract loss for a smaller project.
- Shows how "medium severity" auth bugs become catastrophic when looped at scale.
- Incident response and user trust erosion.
- Highlights need for invariant checks + rate limiting on sensitive actions.

April 2025
Texture (Solana Lending Protocol)

Solana-based lending protocol with vaults (including USDC vault referenced publicly).

Amount Lost: $2.2M, with $1.98M returned after a bounty offer

How It Happened:

- Attacker exploited a vault smart contract vulnerability.
- Drained funds from a specific vault (public reports focus on USDC vault).
- Protocol offered a 10% bounty to encourage return.
- Attacker returned most funds and retained the bounty portion.

Root Cause (Likely)

- A smart contract flaw inside a vault implementation (public disclosures don't fully detail the precise bug mechanics).

Impact

- Short-term vault disruption and user fear on Solana DeFi.
- Partial recovery reduced loss but validated exploitability.
- Forced audits/patches and more conservative vault design expectations.
- Reputation hit despite "good outcome" negotiation.

Incidents widely cited in April totals, but with limited public technical detail in mainstream summaries. ***These are named in multiple roundups, but the public "how/root-cause" details aren't consistently published in the broadly referenced sources.***

Zapper.fi

April 2025
Zapper (.fi) Domain Hijack (DeFi Portfolio Tracker)

A DeFi portfolio tracking and "zaps" interface used to manage positions across protocols.

Amount Lost: $7.9M

How It Happened:

- Attacker used social engineering against the domain/provider side.
- zapper.fi was hijacked and served a malicious page.
- Users were warned off the domain; safe access shifted to an alternate domain.
- Funds were reportedly lost via user interaction with malicious front-end.

Root Cause

- Domain / DNS / registrar supply-chain weakness + social engineering, enabling a trusted brand domain to deliver attacker-controlled content.

Impact

- Users exposed to wallet drain / malicious approvals.
- Emergency comms + migration to alternate safe domain.
- Brand trust damage; increased phishing/impersonation attempts.
- Real-time incident response burden for the team/community.

April 2025

ROAR (DeFi) - Staking Contract Backdoor / Insider Manipulation

A DeFi project/token ecosystem with staking contracts.

Amount Lost: $780K - $790K

How It Happened:

- Contract contained a backdoor that could alter storage/accounting.
- Attacker (or malicious insider) changed internal staking balances.
- Used as emergency withdrawal path to pull funds out.
- Project stated a "nefarious developer" was responsible and removed.

Root Cause

- Malicious code/backdoor introduced in deployment (insider threat), enabling direct manipulation of staking accounting and withdrawal.

Impact

- Heavy losses and trust collapse (insider narratives are brutal for communities).
- Governance/access reviews and contributor offboarding.
- Token/community sentiment damage.
- Raises diligence bar for contractors and deploy processes.

April 2025

Bitcoin Theft (Individual, Not a Protocol)

A major wallet theft attributed to social engineering (not a protocol bug).

Amount Lost: 3,520 BTC (~$330M)

How It Happened:

- Victim was tricked via social engineering/phishing into compromising wallet access.
- BTC moved through laundering patterns (including swaps that impacted XMR price).
- On-chain investigation traced flows and identified likely theft.
- Some funds reportedly frozen, but broad recovery wasn't public.

Root Cause

- Human-layer compromise (credential/seed exposure, wallet access manipulation), illustrating that the biggest losses can be "no exploit, just deception."

Impact

- One of the largest single-incident losses of the month; drove April loss totals up.
- Spiked fear around targeted "whale" attacks.
- Reinforced demand for multisig, custody controls, and anti-phishing education.
- Increased attention on laundering routes (cross-exchange flows, privacy assets).

NO LOGO AVAILABLE

April 2025

LIFE Protocol (BSC) - Price Manipuilation

A BSC-based protocol/token.

Amount Lost: $51K

How It Happened:

- Attacker manipulated on-chain pricing/liquidity conditions.
- Executed trades/swaps to extract value
- Monitoring flagged the event as a price manipulation attacks.
- No extensive public tecnical postmortem found.

Root Cause (Likely)

- Thin liquidity + manipulable pricing assumptions (classic “small-cap price manipulation” pattern).

Impact

- LP/holders impacted; volatility spike.
- Trust damage and liquidity flight risk.
- More fertile ground for follow-on scams (fake recoveries, airdrops).
- Reinforces need for liquidity/price oracle hardening even for “small” projects.

NO LOGO AVAILABLE

April 2025

QuantMaster (DeFi Trading/Asset Management)

A DeFi trading and asset management project.

Amount Lost: $100K

How It Happened:

- Community reports alleged malicious code implanted by an employee.
- Internal investigation linked changes to a specific contributor/device history.
- Theft attributed to insider actions rather than an external exploit.
- Suspect reportedly identified (per public statements).

Root Cause

- Insider threat / SDLC failure (code review, permissions, and deployment controls failed to stop malicious changes).

Impact

- Direct loss and credibility hit.
- Engineering process overhaul pressure (review gates, least privilege).
- Increased scrutiny on contributor access and build integrity.
- Community trust erosion (“internal compromise” is hard to come back from).

NO LOGO AVAILABLE

April 2025

MEV Bot (Ethereum)

An MEV bot contract/address exploited due to control weaknesses.

Amount Lost: 116.7 ETH, ~$210K at the time

How It Happened:

- Bot/contract lacked strict access control on sensitive functions.
- Attacker invoked the vulnerable path to extract ETH.
- Funds moved out quickly after exploitation.
- Public reporting focused on the missing control rather than bot logic.

Root Cause

- Missing/weak access control in operational MEV infrastructure (common in "bot code" that wasn't built as adversarial-grade public software).

Impact

- Direct ETH loss to bit operator.
- Demonstrates that "infrastructure code" needs the same rigor as protocols.
- Increased caution around public MEV tooling.
- Copycat risk for similar bot contracts.

NEXT EARTH

April 2025

Next Earth (Polygon NFT/Metaverse Project)

NFT/metaverse-related project on Polygon.

Amount Lost: $17K

How It Happened:

- Attacker triggered a reentrancy condition.
- Re-entered vulnerable logic before state updates finalized.
- Extracted value through repeated calls.
- Public details focus on attack type rather than full code path.

Root Cause

- Reentrancy vulnerability (missing checks-effects-interactions discipline / missing reentrancy guard).

Impact

- Limited but real fund loss and contract risk.
- Mandatory patching + potential pauses.
- Reputation hit (reentrancy is considered "known class").
- Reinforces secure patterns even for smaller NFT projects.

RESONANCE // 2025

NOTABLE HACKS OF MAY

May 2025

Cetus Protocol (Sui DEX / Liquidity Provider)

A major DEX + liquidity hub in the Sui ecosystem.

Amount Lost: $220M - $230M

How It Happened:

- Attacker exploited a core math/validation flaw (reported as an MSB-check issue) to distort liquidity parameters.
- Used the distorted parameters to extract outsized value from pools.
- Large portion of stolen funds was frozen via coordinated response (validators/ecosystem).

Root Cause

- A contract-level validation/overflow-style weakness allowed parameter manipulation at extreme magnitudes, enabling pool extraction.

Impact

- Major liquidity and price dislocations across Cetus pairs.
- Ecosystem-wide incident response; ~$157M - $162M frozen (reported figures may vary).
- User trust hit; likely tightened audits/monitoring across Sui DeFi.

May 2025

Cork Protocol (DeFi Risk Infrastructure)

A DeFi protocol building risk-management primitives (Peg Stability Module + vault/hook automations).

Amount Lost: $12M

How It Happened:

- Attacker abused user-supplied data / hookData pathways to reach unintended states.
- Exploit path tied to beforeSwap logic and authorization/validation gaps in the hook flow.
- Liquidity was manipulated and redirected into unintended markets, enabling unauthorized redemptions.

Root Cause

- Insufficient validation + authorization edge cases in complex Uniswap-hook automation (and version/feature mismatches in upstream periphery expectations) created an exploitable path.

Impact

- ~3,761 wstETH equivalent value removed (as reported by sources).
- Markets paused; LPs contacted; long remediation + additional reviews planned.
- Wider concern for similar hook integrations across ecosystem.

May 2025

BitoPro (Centralized Exchange)

Taiwan-based crypto exchange.

Amount Lost: $11.5M

How It Happened:

- Abnormal hot-wallet outflows observed across multiple chains (Tron/EVM/Solana/Polygon noted).
- Funds dumped via DEX routes.
- Laundering trail reported via mixers/bridges (e.g., Tornado Cash; bridging into BTC via TORChain; further mixing).

Root Cause (Likely)

- Public reporting strongly suggests hot wallet compromise (exact intrusion vector not fully public).

Impact

- Significant exchange treasury/hot-wallet loss.
- Cross-chain incident response + attribution and tracing activity.
- Reputation and operational security scrutiny (wallet segregation, key mgmt).

May 2025

Mobius Token / MobiusDAO (BSC)

A BNB Chain token/project whose contracts were exploited shortly after funding.

Amount Lost: $2.15M - $2.16M

How It Happened:

- Attacker abused a minting/inflation bug caused by a multiplier error.
- Minted an enormous amount of MBU with negligible input, then swapped to stable assets.
- Drained value through market swaps after inflationary mint.

Root Cause

- A 1e18-style inflation/multiplier mistake in an unverified/vulnerable contract enabled effectively unbounded minting.

Impact

- Direct loss around $2.15M - $2.16M.
- Severe token economics damage (supply integrity broken).
- Post-incident pressure for verification, tests, mint controls, and audits.

Demex

May 2025

Nitron (Demex Lending Market)

Lending market on Demex.

Amount Lost: $950K

How It Happened:

- Attacker manipulated the oracle via a donation-based price/oracle attack.
- Targeted a deprecated dGLP vault pathway.
- Extracted value through mispriced collateral/borrow assumptions.

Root Cause

- Oracle design/guardrails around a deprecated vault were exploitable via donation-based manipulation, letting attackers bend pricing.

Impact

- >$950K user-fund loss reported; partial recovery reported later.
- Deprecated components became a live risk surface.
- Likely tightened oracle hardening + vault lifecycle controls.

May 2025

Malda (Linea Lending Protocol)

Lending protocol on Linea (reported exploit involved migration tooling).

Amount Lost: $285K

How It Happened:

- Exploit centered on Migrator.sol allowing a critical address (Comptroller) to be supplied dynamically.
- Attacker injected a malicious Comptroller, minted a synthetic position, then withdrew assets.
- Funds moved out and mixed/bridged (per postmortem and writeups).

Root Cause

- Trusting user-supplied contract addresses in a sensitive migrator path (instead of hardcoding/allowlisting) enabled hostile dependency injection.

Impact

- >$285K drained.
- Forced review of migration tooling, allowlists, and privilege boundaries.
- Adds pressure for "dangerous admin/migration" modules to get extra audits.

May 2025

Usual Protocol (Stablecoin/Vault System)

It's a protocol using a vault design around USD0 / USD0++ mechanics.

Amount Lost: $42.8K

How It Happened:

- Attacker exploited a price discrepancy between internal accounting and external DEX pricing.
- Vault allowed fixed 1:1 exchange between USD0++ and USD0 even when markets diverged.
- Crafted liquidity route/pool + transaction path to pull USD0 without expected backing, then sold externally for profit.

Root Cause

- Internal conversion assumptions (1:1 peg logic) didn't match market reality, enabling arbitrage via engineered routing.

Impact

- Direct protocol loss of ~$42.8K.
- Highlights risk of "fixed-rate" vault conversions without robust pricing checks.
- Likely tightened validation on swap paths and collateral receipt.

May 2025

Zunami Protocol (DeFi Stable Assets)

DeFi protocol issuing zunUSD / zunETH (collateral-backed assets).

Amount Lost: $500K

How It Happened:

- Collateral for zunUSD/zunETH was drained.
- Funds routed onward (reported sent to Tornado Cash).
- Team later suggested possibilities: deployer key compromise or malicious insider.

Root Cause

- Public info points to privileged-key/admin compromise (exact technical path not fully disclosed, but key control is central).

Impact

- ~$500K loss and collateral integrity damage.
- Likely depegs/risk premium on protocol assets.
- Reputational hit + renewed focus on key management and access controls.

May 2025

Coinbase (CEX)

Coinbase is the largest US-based crypto exchange.

Amount Lost: Affects fewer than 1% of users, with remediation expected to cost $180-400M; no funds or credentials DIRECTLY stolen, but social engineering losses previously tied to Coinbase exceed $300M annually.

How It Happened:

- Attackers recruited support agents overseas, bribing them to access internal systems and exfiltrate customer data. They then demanded a $20 million ransom, which Coinbase refused, instead offering a $20 million bounty for tips leading to the culprits.

Root Cause

- Insider threat; rogue support staff with access to sensitive user data (names, emails, addresses, masked SSNs, bank details, ID images).

Impact

- No passwords, private keys, or funds compromised.
- Coinbase will reimburse phishing victims.
- Stock dropped ~5-7%.
- Exchange plans tighter oversight, relocation of support, increased insider detection, and auto fraud prevention.

Incidents widely cited in May totals, but with limited public technical detail in mainstream summaries. ***These are named in multiple roundups, but the public "how/root-cause" details aren't consistently published in the broadly referenced sources.***

May 2025

Nexo (Digital Asset Wealth Management Platform)

Crypto wealth management platform offering financial products/services.

Amount Lost: $31.5K

How It Happened:

- Reported as a sandwich-style MEV attack hitting a contract flow.
- Attacker exploited a contract path that lacked access control, then captured value around trades.

Root Cause

- A contract function reportedly lacked proper access control / MEV-resistence assumptions, allowing sandwich extraction.

Impact

- Limited direct financial loss, but meaningful signal of MEV surface.
- Forces review of trade execution paths and permissioning.
- Potential user confidence impact despite small size.

May 2025

MapleStory Universe (Web3 Gaming Ecosystem)

Web3 gaming initiative associated with the MapleStory IP.

Amount Lost: $1.2M

How It Happened:

- No broadly published technical teardown surfaced in the mainstream summaries.

Root Cause (Likely)

- Likely a contract flaw / key compromise / infra-breach.

Impact

- >$1.2M loss reported in monthly tallies.
- Trust impact on gaming/web3 onboarding narrative.
- Typically leads to pauses, partner reviews, and stronger key/contract controls.

RESONANCE // 2025

NOTABLE HACKS OF JUNE

CoinMarketCap | June 2025

CoinMarketCap (Crypto Data Platform) - Frontend Compromise

Major crypto market-data and listing website.

Amount Lost: $21,624.47 (reported user losses; 76 accounts affected; reimburse promised)

How It Happened:

- Attackers compromised the site front-end to display malicious prompts/content.
- Users who interacted were funneled into scam flows (phishing/drainer-like behavior).
- Platform investigated and disclosed affected-user count and loss figure.

Root Cause

- Frontend/integration compromise (site-layer security failure, not an onchain exploit).

Impact

- Direct user losses; brand trust hit.
- Incident response + reimbursements.
- Reinforced risk of “trusted” crypto websites becoming attack delivery vectors.

June 2025

Nobitex (Centralized Exchange)

Iran-based centralized crypto exchange.

Amount Lost: $90M (some trackers cite $82M+ depending on methodology)

How It Happened:

- Attackers gained unauthorized access to internal systems / hot-wallet infrastructure.
- Funds were drained across multiple chains (multi-network impact).
- The group publicly claimed responsibility and threatened internal data / code leaks.

Root Cause

- A critical access-control failure (operational security breakdown enabling wallet/system compromise), not a smart-contract bug.

Impact

- Major hot-wallet loss across networks; severe trust hit.
- Potential exposure of internal data/source code (threatened).
- Exchange-wide incident response, wallet isolation/monitoring, reputational damage.

June 2025

ALEX Protocol / AlexLab (Bitcoin L2 / Bitcoin DeFi on Stacks)

Bitcoin DeFi stack offering lending/markets and onchain products (Stacks-based Bitcoin ecosystem).

Amount Lost: $8.37M (some analyses cite >$16M depending on accounting)

How It Happened:

- Attacker abused the protocol's self-listing / token verification logic.
- A malicious/fake token bypassed checks and obtained permissions needed to interact with vault logic.
- Multiple pools/vaults were drained (multi-asset impact).

Root Cause

- Broken verification + permissioning in listing/token validation (a logic + access-control design flaw that let malicious assets pass as "valid").

Impact

- Multiple asset pools drained; large protocol loss.
- Emergency pause/response; reimburse/compensation commitments discusses publicly.
- Reputation damage for Bitcoin DeFi security posture.

June 2025

Resupply (DeFi Stablecoin Protocol)

Decentralized stablecoin protocol (reUSD ecosystem / markets).

Amount Lost: $9.5M

How It Happened:

- Attacker manipulated the cvcrvUSD exchange rate via donation transactions to the controller contract.
- The distorted rate/invariant enabled extraction of value from the affected market.
- Large amount of reUSD was stolen before mitigation.

Root Cause

- Protocol accounting/oracle-style exchange-rate manipulation (insufficient validation on how "donations"/inputs affect price/exchange-rate logic).

Impact

- >$9.5M drained from the affected market.
- Contract/module paused; investigation and monitoring escalated.
- Confidence hit for the protocol's stablecoin mechanics.

June 2025

Force Bridge (Nervos Cross-Chain Bridge)

Cross-chain bridge tied to Nervos Network.

Amount Lost: $3.7M

How It Happened:

- Bridge was compromised and abnormal withdrawals occured across chains.
- Investigations found malicious code inside a Docker image used in Ethereum-related modules.
- Team paused bridge contracts while investigating.

Root Cause

- Supply-chain compromise (malicious/injected code in a locally built Docker image rathe than the public codebase).

Impact

- >$3.7M stolen from bridge liquidity.
- Bridge paused; cross-chain operations disrupted.
- Serious trust hit for bridge supply-chain hygiene.

Silo | June 2025
Silo Finance / Silo Labs (DeFi Lending)

DeFi lending/markets protocol (with experimental leverage modules).

Amount Lost: $542K (DAO-owned funds; users not impacted)

How It Happened:

- Exploit targeted an unreleased leverage feature contract deployed for testing.
- Attacker manipulated user-controlled inputs (notably swap args) to force unauthorized borrowing/extraction.
- Team isolated/paused the affected module.

Root Cause

- Unsafe parameter handling / insufficient validation in a non-production test module (peripheral contract risk).

Impact

- >$542K loss borne by DAO treasury.
- No user vaults/markets drained (oer disclosures).
- Highlighted risk of “testing on mainnet” with live funds.

HACKEN | June 2025
Hacken (Token / Bridge-Related Minting Role)

Web3 security firm with a native token (HAI) and bridge/minting setup.

Amount Lost: $250K (economic loss; token supply impact was far larger)

How It Happened:

- A private key tied to a minting role was exposed during architecture changes.
- Attacker minted ~900M HAI on Ethereum and BNB chain and sold into liquidity.
- Team revoked access/paused and moved toward migration response.

Root Cause

- Single-key access control failure (mint authority protected by a compromised key; insufficient compartmentalization/multisig hardening).

Impact

- HAI price crashed sharply (reported ~97%+ drawdown).
- Unauthorized supply inflation; ecosystem disruption for holders/liquidity pools.
- Bridge/mint controls paused; migration/response required.

June 2025

Meta Pool (Liquid Staking)

Liquid staking protocol; mpETH pool mechanics.

Amount Lost: $25K realized outflow (while exploit minted a much larger notional amount)

How It Happened:

- Attacker abused a minting logic weakness to mint mpETH without proper backing/invariants holding.
- Large notional mpETH was minted, but thin liquidity limited cash-out.
- Incident was noticed and mitigations/pauses were applied.

Root Cause

- Faulty mint/invariant enforcement in the mpETH pool logic (a contract logic bug enabling unbacked minting).

Impact

- Realized loss limited by liquidity, but trust impact high.
- mpETH pool integrity questioned; incident response and controls tightened.
- Liquid staking risk spotlighted (invariant bugs are catastrophic).

June 2025

Anome (DeFi Protocol on Base)

Base-native DeFi borrowing/lending style project.

Amount Lost: $120K

How It Happened:

- Attacker acquired an outsized amount of the project token cheaply.
- Supplied it as collateral where valuation checks were weak, enabling excessive borrowing.
- Borrowed repeatedly and drained available assets.

Root Cause

- Broken token valuation / price-validation allowing over-borrowing against effectively worthless collateral.

Impact

- ~$120K drained.
- Confidence hit for Base DeFi risk controls.
- Likely emergency pause + remediation (as typical for lending drains).

June 2025

Polyhedra (ZK-Project)

Polyhedra Network, a zk-focused DeFi protocol with its ZKJ token.

Amount Lost: Token value slumped over 80%, wiping out approximately $500 million in market cap

How It Happened:

- Attackers orchestrated large-scale withdrawals of liquidity provider (LP) tokens, triggering cascading dumps across both decentralized and centralized exchanges. This forced massive liquidations (~94M) in margin markets, sending ZKJ spiraling.

Root Cause

- A classic coordinated liquidity attack, not a smart-contract exploit. Exploiters used deep insight into shallow AMM pools and on-chain mechanics.

Impact

- ZKJ price dropped from ~$2 to $0.32 in minutes.
- Triggered a technical review and plans for deeper on-chain defense mechanisms.

June 2025

BedRock UniBTC (Liquid Staking Protocol)

Bedrock is a liquid staking protocol offering synthetic tokens like UniBTC and UniETH.

Amount Lost: Approximately $2 million was drained from the UniBTC liquidity pools

How It Happened:

- A former Fuzzland employee, who had internal access, inserted malware into engineering workstations. When a vulnerability in UniBTC's mint logic was revealed during an emergency call, the attacker exploited it using insider knowledge and drained funds.

Root Cause

- Insider threat + supply-chain attack: a compromised private key combined with overlooked vulnerability due to false-positive noise in security alerts.

Impact

- Fuzzland reimbursed Bedrock fully and engaged ZeroShadow, Seal 911, and SlowMist in joint investigations.
- Prompted internal security reforms and added monitoring safeguards.

Incidents widely cited in June totals, but with limited public technical detail in mainstream summaries. ***These are named in multiple roundups, but the public "how/root-cause" details aren't consistently published in the broadly referenced sources.***

June 2025

Hypersphere Partner Wallet Drain (Targeted Zoom Phishing)

A crypto VC ecosystem participant (personal wallets); not a protocol exploit, but a high-signal security incident.

Amount Lost: Not disclosed ("savings over several years" reported)

How It Happened:

- Social engineering via Telegram outreach to schedule a meeting.
- Victim pushed to use "Zoom Business" and install a malicious "update".
- Multiple wallets drained after compromise.

Root Cause

- Targeted malware delivery through meeting-software impersonation (classice "fake update" endpoint compromise).

Impact

- Multiple wallets drained; personal financial loss.
- Demonstrates rising risk of offchain compromise → onchain theft.
- Reinforces need for endpoint hardening for teams and KOLs.

June 2025

CoinTelegraph (Crypto Media) - Frontend Compromise

Major crypto news publisher/site.

Amount Lost: Not disclosed publicly.

How It Happened:

- Front-end compromise triggered a persistent "airdrop" style pop-up.
- Pop-up behavior suggested a phishing/drainer delivery attempt.
- Users were warned to exercise caution.

Root Cause (Likely)

- Public reporting points to a website/frontend compromise; deeper entry point (ad scripts, CDN, third-party tags) not confirmed.

Impact

- High risk of user wallet compromise via malicious UI.
- Trust damage for a crypto media domain.
- Users advised to avoid interacting during the incident window.

RESONANCE // 2025

NOTABLE HACKS OF JULY

GMX | July 2025

GMX (Perps DEX on Arbitrum)

A decentralized perpetuals trading protocol on Arbitrum.

Amount Lost: $42,000,000 (later returned; bounty paid)

How It Happened:

- Attacker exploited how GMX's keeper/leverage execution interacted with global short average price updates.
- Used reentrancy + position mechanics to manipulate GLP pricing.
- Redeemed inflated GLP to extract profit.
- Negotiated return of funds for a $5M bounty.

Root Cause

- A design/logic vulnerability in how global short metrics and keeper-executed leveraged actions were accounted for, enabling price/position state manipulation under reentancy.

Impact

- Temporary loss/exposure of ~$42M.
- Protocol reputation hit; renewed scrutiny on perps pricing/state logic.
- Funds mostly/fully recovered after negotiation + bounty.

July 2025

Kinto (Arbitrum-based Project)

A modular exchange platform in the Arbitrum ecosystem.

Amount Lost: $1,550,000 (ETH + USDC)

How It Happened:

- Attacker exploited a bug enabling unlimited minting of K tokens.
- Minted ~110,000 K, then attacked Morpho vault + Uniswap v4 pool.
- Resulted in asset loss and major K price volatility.

Root Cause

- A contract vulnerability that allowed unauthorized/unbounded minting, which was then weaponized against liquidity/vault integrations.

Impact

- $1.55M direct loss.
- Severe token price volatility and liquidity disruption.
- Highlighted composibility risk: mint bugs cascading into vault/pool drains.

PUNDI AI

July 2025

Pundi AI (Token Project on Ethereum)

A token project (AI branding) with swap/mint flows on Ethereum.

Amount Lost: $6,570,000 (team said ~87% recovered; remaining covered by team)

How It Happened:

- Exploit resulted in unauthorized minting of 1M tokens.
- Rooted in a token swap contract weakness, abused via front-running duing deployment (per team).
- Asset freezes + recovery actions reclaimed most value.

Root Cause

- A deployment/front-running + swap contract vulnerability that allowed the attacker to mint/realize value before protections were effectively in place.

Impact

- Multi-million dollar hit; partial recovery.
- Forced remediation + compensation commitment by project team.
- Likely downstream volatility/market confidence damage.

July 2025
Arcadia Finance (DeFi Project on Base)

A DeFi protocol focused on onchain asset management/liquidity management on Base.

Amount Lost: $3,500,000

How It Happened:

- Attacker exploited a contract vulnerability to drain funds.
- Losses realized through onchain transactions over the exploit window.
- Post-incident, ecosystem partied documented claim/response steps (e.g., coverage claims).

Root Cause

- Public reporting describes a smart-contract exploit (permission/validation issues around trusted execution paths) that enabled unauthorized withdrawals from user accounts.

Impact

- ~$3.5M drained.
- Claims/coverage workflows triggered for insured users.
- Reinforced need for strict validation of "trusted"" contract call paths.

Incidents widely cited in July totals, but with limited public technical detail in mainstream summaries. ***These are named in multiple roundups, but the public "how/root-cause" details aren't consistently published in the broadly referenced sources.***

July 2025
CoinDCX (Centralized Exchange)

A major Indian centralized crypto exchange.

Amount Lost: $44,200,000

How It Happened:

- Onchain investigator flagged the suspected drain; exchange later confirmed.
- Company described it as a "sophisticated server breach" affecting corporate funds.
- Public technical breakdown of initial access + kill chain was not fully disclosed in the same level as DeFi postmortems.

Root Cause (Likely)

- Publicly characterized as server/security breach (exact exploit path not fully detailed in public writeups).

Impact

- $4.2M loss headline for the month.
- Exchange credibility + security posture scrutiny.
- Operational response + user reassurance cycle.

July 2025

BigONE (Centralized Exchange)

A centralized cryptocurrency exchange.

Amount Lost: $27,000,000

How It Happened:

- Reported as a supply-chain attack.
- Attacker breached production network and altered server logic tied to account management/risk controls.
- Enabled unauthorized withdrawals; no private key leakage noted.

Root Cause

- Supply-chain / production environment compromise allowing tampering with critical backend controls rather than direct key theft.

Impact

- >$27M lost.
- Demonstrated high blast-radius of compromised backend/risk systems.
- Reinforced need for build/deploy integrity + prod segmentation.

July 2025

SuperRare (NFT Market on Base)

A curated NFT marketplace protocol/ecosystem.

Amount Lost: $900,000

How It Happened:

- Attacker exploited a weakness in a function that missed a permission check.
- Triggered unauthorized withdrawals.
- Limited public technical depth beyond the missing authorization guard.

Root Cause

- A missing authorization/permission check on a withdrawal-related path.

Impact

- ~$900K drained.
- Marketplace/user trust impact.
- Necessitated emergency patches + access control review.

July 2025
Alien Base (DEX on Base)

A decentralized exchange on Base.

Amount Lost: $38,000

How It Happened:

- Reported as a protocol attack with relatively small loss.
- Public info is mostly monitoring alerts; limited postmortem depth.

Root Cause (Likely)

- Listed as an attack (specific exploit vector not richly documented in public sources).

Impact

- Smaller but real loss; demonstrates long-tail exploit volume.
- Likely forced code review + mitigations.

July 2025
WOO X (Centralized Exchange)

A centralized crypto trading platform.

Amount Lost: $14,000,000

How It Happened:

- Described as a targeted phishing attack.
- Compromised a team member device, leading to access into the development environment.
- Resulted in fund losses (public detail stops short of full internal timeline).

Root Cause

- Credential/device compromise via phishing leading to elevated access (dev environment exposure).

Impact

- $14M hit.
- Security process tightening around endpoints and dev systems.
- Market confidence impact around operational security.

RESONANCE // 2025

NOTABLE HACKS OF AUGUST

August 2025

Bitcoin Holder (Private Wallet)

A long-time BTC holder (individual/custody wallet), not a protocol.

Amount Lost: $91.4M (in BTC)

How It Happened:

- Attackers reportedly impersonated hardware-wallet “support” / ran a targeted social-engineering flow.
- Victim was tricked into performing actions that enabled the attacker to take control and move BTC.
- Funds were then transferred out on-chain and dispersed.

Root Cause

- A human-layer compromise (high-trust support impersonation) rather than a protocol bug; attackers won by getting the victim to authorize/enable access.

Impact

- Massive loss concentrated in a single wallet.
- Reinforced “support impersonation” as a top theft vector.
- Likely laundering/peel-chain activity post-theft.

NO LOGO AVAILABLE

August 2025

D3X AI (BSC Token)

Token/project on BSC with an exchange function tied to on-chain spot pricing.

Amount Lost: $158.9K

How It Happened:

- Contract exchange() relied on spot price from a UniswapV2-style pair.
- Attacker manipulated the pair price (thin liquidity / controlled swaps).
- Extracted value using the distorted rate.

Root Cause

- Oracle/design flaw: spot-price dependency without TWAP/robust oracle defenses, enabling classic price manipulation.

Impact

- Direct treasury/pool loss.
- Demonstrated ongoing prevalence of "spot-price orcale" mistakes on BSC.
- Likely liquidity stress and token price shock post-incident.

BtcTurk

August 2025

BtcTurk (Turkish CEX)

Major Turkish centralized exchange.

Amount Lost: $48M - $54M

How It Happened:

- Exchange detected unusual hot-wallet outflows across multiple chains and paused deposits/withdrawals.
- Incident attributed in reporting to compromised private keys again (repeat pattern vs prior year).
- Attacker drained hot wallets; cold storage was stated/assumed largely unaffected.

Root Cause

- Hot-wallet key exposure / operational key management failure (off-chain security), enabling direct unauthorized transfers.

Impact

- Large treasury loss (exchange-side), hush reputational damage.
- Deposits/withdrawals disruption during response.
- Renewed scrutiny on exchange key custody controls.

ODIN·FUN | August 2025

ODIN.FUN (Memecoin Launchpad)

Bitcoin-nbased memecoin launchpad + trading/AMM system.

Amount Lost: $7M (~58.2 BTC)

How It Happened:

- Attacker manipulated AMM pricing by using worthless/low-value tokens to distort pool valuation.
- Artificially inflated token value and then withdrew BTC based on manipulated prices.
- Platform froze operations during investigation; partial recovery was discussed publicly.

Root Cause

- AMM/business-logic weakness allowing value extraction via price manipulation and flawed valuation assumptions.

Impact

- Platform halt/freeze and user trust hit.
- Significant BTC-denominated loss and recovery efforts.
- Became a reference case for AMM manipulation risk outside typical EVM DEXes.

August 2025

BetterBank (PulseChain DeFi Lending)

PulseChain DeFi platform with reward/bonus token mechanics.

Amount Lost: $5M (with ~$2.7M reportedly returned, per later reporting)

How It Happened:

- Attacker used flash-loan/liquidity operations, then created fake liquidity pairs.
- Exploited reward logic to mint/loop rewards (ESTEEM/FAVOR mechanics) and inflate extractable value.
- Swapped and cashed out portions; some proceeds bridged and mixed (per analysis).

Root Cause

- Reward/bonus logic failed to validate legitimate pools/routes, enabling reward farming via fake pools; plus a loopable conversion path that amplified the exploit.

Impact

- Pool liquidity drained; protocol paused and planned relaunch with patched contracts.
- Rartial recovery after attacker returned a chunk.
- Highlighted how “low severity” audit findings can become multi-million losses.

August 2025

CrediX / Credix (Sonic DeFi Lending)

DeFi lending protocol on Sonic (bridging to Ethereum involved).

Amount Lost: $4.5M

How It Happened:

- Attacker gained control of an admin/multisig/bridge-related wallet (reported).
- Minted tokens/unbacked collateral and drained protocol liquidity pools.
- Funds were then bridged out toward Ethereum; “negotiation” was claimed publicly.

Root Cause

- Access control failure / signer compromise enabling privileged minting + pool draining.

Impact

- Liquidity loss and protocol stoppage.
- Community suspicion escalated after team presence disappeared shortly after.
- Users left with unresolved reimbursement uncertainty (per reporting).

August 2025

NumaVault (Sonic DeFi Vault)

Vault contract component in a DeFi system on Sonic.

Amount Lost: $320K

How It Happened:

- Attacker manipulated the vault and triggered liquidations of victim accounts.
- Extracted extra tokens not entitled to, then swapped across pools.
- Funds were subsequently mixed to obfuscate flows.

Root Cause

- Protocol logic flaw around vault/liquidation mechanics enabling abusive liquidation/value extraction.

Impact

- Direct vault losses and affected user positions.
- Emergency response + heightened scrutiny of Sonic DeFi deployments.
- Typical post-exploit laundering behavior (mixing).

August 2025

Coinbase (CEX)

Centralized exchange; incident involved a corporate/fee collection wallet (not customer funds).

Amount Lost: $300K - $550K

How It Happened:

- Wallet mistakenly granted broad ERC-20 approvals to a permissionless swap/settlement contract.
- MEV actors/bots detected the approvals and pulled many different tokens from the wallet.
- Coinbase revoked allowances and migrated wallets afterward.

Root Cause

- Operational misconfiguration; approvals granted to the wrong contract surface, allowing permissionless extraction without “breaking” code.

Impact

- Treasury/fee-wallet loss; customer funds stated unaffected.
- Became a widely-cited example of “approvals are permissions, not safety.”
- Reinforced the need for approval minimization and contract-allowlist policies.

August 2025

Equilibria Finance (DeFi Auto-Compunder)

DeFi yield/auto-compounding system (ePENDLE auto-compounder on Ethereum, per disclosure).

Amount Lost: 13.36 ETH ($62.5K)

How It Happened:

- Attacker used flash loans (Balancer) to acquire ePENDLE.
- Staked into stk-ePENDLE, then repeatedly transferred stk-ePENDLE across addresses.
- Each transfer triggered reward claims, draining unclaimed rewards from the contract.

Root Cause

- Configuration/logic mistake: stk-ePENDLE not enforced as non-transferable, enabling repeatable reward-claim triggers.

Impact

- Reward pool depletion and contract patching requirements.
- Limited direct loss size, but high signal on “transfer hooks / rewards triggers” risk.
- Trust impact on strategy vault users.

August 2025

0x2d98...6695 (Individual Wallet, Not a Protocol)

Individual wallet theft (not a protocol exploit).

Amount Lost: $3.05M (USDT)

How It Happened:

- Victim was deceived into signing/granting malicious approvals.
- Attacker immediately pulled USDT out of the wallet.
- Funds moved away rapidly post-drain.

Root Cause

- Approval phishing: user authorized a spender that had no legitimate need for that allowance.

Impact

- Large single-wallet stablecoin loss.
- Highlights why “approve” is often the real theft moment.
- Typical post-theft dispersal behavior.

August 2025

Private Wallet (Individual, Not a Protocol)

Individual wallet drain using newer transaction patterns.

Amount Lost: $1.54M

How It Happened:

- Victim signed a fraudulent batch transaction.
- Batch included token transfers + NFT approval operations.
- Attacker used permissions to extract assets.

Root Cause

- Signature/transaction deception: user approved a bundle whose effective actions were not understood at signing time.

Impact

- High-value personal loss.
- Shows scammers adapting quickly to new transaction UX patterns.
- Increased demand for transaction simulation and “what you sign” tooling.

RESONANCE // 2025

NOTABLE HACKS OF SEPTEMBER

VENUS | September 2025

Venus Protocol (DeFi Lending on BNB Chain)

Major lending/borrowing protocol (money market) on BNB chain.

Amount Lost: $13M

How It Happened:

- Victim was lured via Telegram → Zoom social engineering.
- They approved a malicious transaction granting attacker delegate/borrow + redeem rights.
- Attacker used flash loans + their funds to reshape debt/collateral and siphon value.
- Venus force-liquidated attacker positions (price/position mechanics) and recovered funds.

Root Cause

- User approval abuse (permit/delegation) via high-quality phishing; protocol wasn't "exploited" so much as the user's authority was weaponized.

Impact

- Temporary ~$13M exposure, later recovered.
- Highlights "signature = authorization" risk for whales.
- Increased scrutiny around delegation/permissions UX.

September 2025

OlaXBT (AI Trading Platform)

Ai-driven crypto market intelligence and trading product.

Amount Lost: $2M

How It Happened:

- Attackers compromised/abused multisig wallets, enabling unauthorized withdrawals.
- ~32M AIO tokens were withdrawn without authorization.
- Team triggered incident response and claimed mitigation/resolution.

Root Cause

- Multisig operational/security failure (compromise or unsafe configuration) allowing unauthorized token movements.

Impact

- Direct treasury/token loss.
- Emergency response + user trust hit.
- Likely tightened wallet controls and monitoring post-incident.

September 2025

Bunni (DEX on Uniswap)

DEX liquidity protocol built around Uniswap v4-style hooks/custom liquidity logic.

Amount Lost: $8.4M

How It Happened:

- Attacker exploited a rounding/precision error in custom liquidity math.
- Used flash loans + 44 carefully-sized withdrawals to repeatedly extract excess value.
- Bunni paused contracts across networks and shipped a patch.
- Team attempted recovery via on-chain negotiation/bounty offer.

Root Cause

- A protocol-logic precision bug (rounding) that became extractable under adversarial sequencing and flash liquidity.

Impact

- ~$8.4M drained from pools/LPs.
- Emergency pause affected trading/liquidity availability.
- Reinforced need for adversarial math reviews + invariant testing.

SwissBorg | September 2025

SwissBorg (Centralized Wealth App / Exchange)

Centralized crypto wealth platform with Earn/Staking products.

Amount Lost: $41.5M

How It Happened:

- Attack leveraged third-party / supply chain weakness (reported as the core vector).
- Staking/Earn-related accounts (notably Solana Earn) were targeted with auth/control abuse.
- Unauthorized transactions drained funds from affected staking flows.
- SwissBorg paused Solana staking and coordinated investigation/compensation.

Root Cause

- Not "one smart contract bug", but it was dependency/infrastructure compromise enabling attacker control over sensitive staking operations.

Impact

- ~$41.5M theft.
- Limited user subset impacted (reported as <1%), but large absolute loss.
- Earn/staking product disruption + forced compensation plan.

September 2025

Nemo Protocol (DeFi Protocol on Sui)

Yield optimization / DeFi platform on Sui.

Amount Lost: $2.4M

How It Happened:

- Malicious/rogue code path introduced and later exploited.
- Exploit abused a function incorrectly exposed + a "read-only" query that could mutate state.
- Funds were drained and bridged out (reported via Wormhole/CCTP to ETH).
- TVL collapsed as users rushed to withdraw after disclosure.

Root Cause

- Bad SDLC / internal controls: unaudited or improperly reviewed code plus a critical access/state-mutation flaw.

Impact

- ~$2.4M loss.
- Reported TVL drawdown (~$5M) due to panic withdrawals.
- Reputation damage for Sui DeFi security posture.

September 2025

Evoq Finance (DeFi Project on BNB Chain)

BNB Chain based DeFi protocol.

Amount Lost: $450K

How It Happened:

- Attacker obtained owner private key.
- Ownership transferred to attacker-controlled address.
- Proxy upgraded via upgradeAndCall to malicious implementation.
- Treasury + approval-based drains executed.

Root Cause

- Privileged key compromise + upgradeable proxy abuse (admin power became the exploit).

Impact

- ~$450K stolen.
- Trust hit for upgradeable proxy patterns without strong governance.
- Likely triggered key rotation + admin hardening.

September 2025

Kame Aggregator (DeFi Project on Sei)

Aggregator/router for swaps on Sei.

Amount Lost: $1.32M (partially recovered; net reported ~$360K)

How It Happened:

- Design flaw: swap() allowed arbitrary executor calls without validation.
- Attacker used a malicious multicall/proxy to drain users who had unlimited approvals.
- Copycats repeated the same pattern after first disclosure.
- Negotiation/bounty + refunds recovered most funds (~96% refunded reported).

Root Cause

- Router design that effectively became a token-stealing primitive once arbitrary external execution was permitted and users had standing approvals.

Impact

- 830 users affected; ~$1.32M gross impact reported.
- User guidance: revoke approvals immediately.
- Major reputational hit for “approval-based” security model.

September 2025

Shibarium Bridge (Bridge / L2 Ecosystem)

Bridge component in the Shuba Inu / Shibarium ecosystem.

Amount Lost: Reported range ~$2.4M - $4.1M

How It Happened:

- Attacker used flash loans to acquire enough governance/validator influence (BONE).
- Validator/signing manipulation enabled fraudulent checkpoints/withdrawals.
- Assets drained from bridge liquidity.
- Team paused/froze parts of the system and began tracing/mitigation.

Root Cause

- Validator/bridge access-control weakness where temporary voting power + key/signature issues could translate into unauthorized bridge actions.

Impact

- Multi-million dollar drain; market shock for ecosystem tokens.
- Bridge downtime/constraints during recovery.
- Renewed focus on validator key hygiene + bridge security.

September 2025

Yala (BTC-focused DeFi + Stablecoin)

BTC-focused DeFi protocol; includes a stablecoin (YU) and cross-chain components.

Amount Lost: $7.64M

How It Happened:

- Attacker abused temporary deployment keys used during an authorized bridge deployment.
- Backdoor later activated to mint large amounts of tokens (OFRU/YU mechanics).
- Funds moved cross-chain and laundered (Tornade Cash referenced).
- Protocol compensated users (1:1 swap mechanism referenced) and planned token cleanup.

Root Cause

- Key management + cross-chain trust assumptions: privileged deployment artifacts enabled an attacker-controlled bridge path and token minting.

Impact

- ~$7.64M drained.
- YU briefly depegged; confidence hit.
- Compensation + remediation burden on treasury/liquidity.

NO LOGO AVAILABLE

September 2025

NewGold Protocol (BSC DeFi Project)

DeFi project for gold-backed/tokenized gold narrative on BSC.

Amount Lost: $2.0M

How It Happened:

- Flash loans manipulated DEX reserves used for pricing.
- Oracle weakness let attacker bypass purchase limits/cooldowns (via routing tricks).
- Attacker accumulated tokens, then dumped and bridged out.
- Laundered via bridge to Ethereum + Tornado Cash.

Root Cause

- DEX-reserve-based oracle design without robust manipulation resistance.

Impact

- ~$2M loss; token value drawdown (88% mentioned).
- Confidence collapse immediately post-launch.
- Highlights danger of launching with weak oracle assumptions.

UXLINK

September 2025

UXLINK (Web3 Social Platform)

Web3 social platform + infrastructure provider.

Amount Lost: $11.3M direct extracted in one writeup. $28.0M total impact (including ~$17M attributed to mint/dillution).

How It Happened:

- Attackers abused delegateCall/admin controls to replace multisig admins / reduce threshold.
- Drained stablecoins + ETH/WBTC and dumped tokens.
- Minted a large quantity of additional tokens (reported 1-2B) and sold part of it.
- Funds converted to ETH and laundered (Tornado Cash referenced).

Root Cause

- Broken admin/multisig safety model (insufficient guardrails like timelocks/guardians + exploitable privileged call paths).

Impact

- Multi-million loss + token price shock from dumping/minting.
- Exchange freezes recovered only a portion (some deposits flagged/frozen).
- Announced 1:1 swap / supply cleanup approach (per reporting).

Seedify | September 2025

Seedify (Launchpad/Incubator)

Web3 incubator + launchpad; SFUND token.

Amount Lost: $1.8M

How It Happened:

- Attacker obtained a developer private key.
- Used bridge permissions to mint unauthorized SFUND on Avalanche.
- Bridged tokens across chains, drained liquidity, sold into deeper venues (BNB Chain mentioned).
- Exchanges coordinated: blacklists/pauses and bridge shutdown.

Root Cause

- Key compromise on privileged bridge infrastructure; bridge mint controls were effectively "admin = mint".

Impact

- ~$1.8M stolen + SFUND price disruption.
- Cross-chain bridge trust damaged.
- Forced infra security review and incident coordination.

September 2025

GriffinAI (GAIN Token Project)

DeFi/AI-token project with GAIN token; used cross-chain messaging (LayerZero).

Amount Lost: $3.5M realized drain in detailed exploit analysis. $36M "impact" mentioned in news (likely includes dilution/market effects).

How It Happened:

- Compromised admin/privileged wallet or misconfigured trusted peer.
- Attacker set a malicious trusted endpoint and minted billions of tokens cross-chain.
- Dumped on PancakeSwap / OTC, converted to ETH.
- Laundered via bridges + Tornado Cash.

Root Cause

- Cross-chain security failure where trusted-peer validation + admin key hygiene wasn't strong enough to prevent unauthorized minting.

Impact

- Massive supply distortion and price crash (87% cited).
- Exchange trading halts to contain damage.
- Re-issuance/snapshot style recovery plans discussed publicly.

Hypervault | September 2025

HyperVault (Hyperliquid Ecosystem DeFi)

Yield/DeFi vault product on Hyperliquid ecosystem.

Amount Lost: $3.6M

How It Happened:

- Large "abnormal withdrawals" detected on-chain.
- Funds bridged to Ethereum and swapped into ETH.
- Deposited into Tornado Cash for laundering.
- Project socials/website disappeared, reinforcing rug-pull hypothesis.

Root Cause

- Not a code exploit; classic operator exit scam pattern (custody/controls centralized).

Impact

- Direct depositor losses (~$3.6M).
- Hyperliquid ecosystem confidence hit.
- Reinforces due diligence needs for new yield vaults.

September 2025

HyperDrive (Hyperliquid Ecosystem DeFi)

Lending/DeFi protocol on Hyperliquid ecosystem.

Amount Lost: $782K

How It Happened:

- Attacker exploited arbitrary call capability in route/market logic.
- Drained specific pools/markets (Primary + Treasury USDT0 markets cited).
- Team paused markets and deployed a patch.
- Users reportedly compensated for impacted positions.

Root Cause

- Smart contract vulnerability in router permissions/execution that allowed repeated abusive calls.

Impact

- ~$782K drained.
- Temporary pause/disruption of markets.
- Increased scrutiny on Hyperliquid ecosystem risk after multiple incidents.

dTRINITY | September 2025

dTRINITY / dLEND (DeFi Lending)

dLEND is a lending product in the dTRINITY ecosystem.

Amount Lost: $56K

How It Happened:

- Attackers abused prior approvals via a swap adapter / approval path.
- Collateral siphoned from wallets with exposure (team said internal wallets).
- Vulnerable feature disabled quickly.

Root Cause

- Approval handling/adapter design allowed misuse of allowances (effectively "approved token = transferable under exploit path").

Impact

- Limited loss ($56K) and reportedly no user funds impacted.
- Fast mitigation reduced contagion.
- Another reminder: approvals are an attack surface.

---

sbicrypto | September 2025

SBI Crypto (Japanese Crypto Firm)

Crypto business under Japan's SBI group (reporting describes compromise of crypto assets and laundering flow).

Amount Lost: $21M

How It Happened:

- Wallet compromise led to unauthorized outflows (reporting attributed to compromise rather than smart contract bug).
- Funds routed through swap/bridge hops and obfuscation paths.
- Public attribution/links discussed by analysts.

Root Cause (Likely)

- Likely key management failure (hot wallet/private key exposure) rather than on-chain logic.

Impact

- ~$21M direct loss.
- Compliance/incident response escalation (exchange-grade severity).

Incidents widely cited in September totals, but with limited public technical detail in mainstream summaries. ***These are named in multiple roundups, but the public "how/root-cause" details aren't consistently published in the broadly referenced sources.***

NO LOGO AVAILABLE

September 2025

Aqua (Solana-based Project)

Solana project/token promoted pre-launch; alleged team exit.

Amount Lost: 21.77K SOL ($4.65M reported)

How It Happened:

- Team allegedly drained liquidity/treasury and cut communications.
- Social channels restricted/disabled; presence degraded immediately after.
- On-chain investigators flagged flows consistent with a rug pull.

Root Cause

- Centralized control over liquidity + lack of enforced lockups/withdrawal constraints.

Impact

- Token holders left with severe losses.
- Trust hit for "audited" marketing narratives around new tokens.

NO LOGO AVAILABLE

September 2025

Unnamed Protocol/Entity (EOA Token Theft)

Reported as a significant ETH-chain theft event (not tied to a clearly named protocol publicly).

Amount Lost: $3.0M

How It Happened:

- Funds stolen and rapidly swapped to ETH.
- Split across intermediary wallets to evade tracing.
- Laundered via Tornado Cash.

Root Cause (Likely)

- Public reporting can't conclusively pin this to one exploit class (described as wallet / smart contract / flash-loan related).

Impact

- $3M theft + visibility into laundering patterns.
- Reinforces mixer-based cashout reality for attackers.

NO LOGO AVAILABLE

September 2025

NPM “qix” (Not a Crypto Project)

Software supply-chain incident impacting crypto users/devs via compromised packages.

Amount Lost: Not consistently quantified in public writeups

How It Happened:

- Attacker phished package owner and published backdoored versions.
- Malware swapped wallet addresses to attacker-controlled addresses.
- Intercepted Ethereum/Solana transaction flows in affected environments.

Root Cause

- Maintainer account takeover + trust in dependency distribution pipelines.

Impact

- Broad blast radius potential (depends on who imported the package).
- Reinforces SBOM + dependency pinning + maintainer hardening.

September 2025

THORChain (Not a Protocol Hack)

Personal compromise of a high-profile web3 founder (not a THORChain protocol exploit per se).

Amount Lost: $1.2M - $1.35M

How It Happened:

- Attacker used a hijacked Telegram account and deepfake video call.
- Victim ran malicious code.
- Private keys extracted → funds drained.

Root Cause

- Human-targeted compromise (social engineering) leading to device/key exfiltration.

Impact

- Multi-million personal loss.
- Signals “deepfake ops” becoming mainstream against crypto leadership.

CORE | September 2025

Corepound (Core DAO Ecosystem DeFi)

A DeFi project on Core DAO chain.

Amount Lost: $400K

How It Happened:

- Project operators allegedly withdrew funds and disappeared (rug pull classification).
- Limited additional post-mortem/public transparency.

Root Cause

- Governance/custody centralization with insufficient safeguards.

Impact

- Direct depositor losses.
- Reputation damage for ecosystem discovery projects.

September 2025

Unnamed Wallet (Crypto Whale)

Whale wallet drain via permit/approval signature.

Amount Lost: >$6.0M

How It Happened:

- Whale signed a malicious permit.
- Attacker used transferFrom to drain tokens without a “normal-looking” on-chain approval transaction.

Root Cause

- Signature-based authorization misuse (phishing); “no gas approval” makes it harder to notice.

Impact

- Multi-million wallet drain.
- Reinforces the danger of signing permits blindly.

RESONANCE // 2025

NOTABLE HACKS OF OCTOBER

October 2025

Garden Finance (Cross-Chain Protocol)

Cross-chain protocol used to move/swap assets across networks via solvers/relayers.

Amount Lost: ~$10.8M - $11M

How It Happened:

- Attacker compromised a single solver in Garden's solver networks.
- Using the solver position, the attacker drained funds across multiple chains/flows routed via the solver.
- Garden paused/shur down its app and began incident response while funds were moved out.

Root Cause

- Solver-level security failure (i.e., compromise of a trusted execution/relayer component) rather than a simple single contract big, highlighting the fragility of "off-chain trust points" inside cross-chain designs.

Impact

- Direct user/protocol losses in the ~$11M range.
- Temporary shutdown/pausing of Garden's app/operations.
- Renewed scrutiny on solver/relayer operational security for cross-chain systems.

October 2025

Hyperliquid (Crypto Ecosystem)

Perps-focused ecosystem/network where a user's private key compromise led to a large theft (not a core-protocol contract bug).

Amount Lost: ~$21M

How It Happened:

- A user wallet/private key was leaked/compromised.
- Attacker used the stolen key to authorize withdrawals/transfers without "hacking" the chain itself.
- Funds were drained rapidly and moved out.

Root Cause

- Access-control failure at the key-management layer (private key compromise), not an exploitable flaw in Hyperliquid's smart contracts.

Impact

- ~$21M stolen from the affected account.
- Re-put "opsec/key security" at the center of loss drivers (even when contracts are fine).

October 2025

Astera (DeFi Lending on Linea)

Lending protocol on Linea, impacted by a "liquidity index inflation" style exploit.

Amount Lost: ~$821,856 to "over $880,000"

How It Happened:

- Attacker executed a liquidity index inflation / accounting manipulation against specific pools.
- Manipulated index led to collateral/value being overstated.
- Overvaluation enabled borrow/drain cycles across impacted minipools.

Root Cause

- Weakness in protocol accounting/index mechanics (insufficient checks to prevent index manipulation or to circuit-break abnormal movements).

Impact

- Losses ~8% of TVL (per reporting), across multiple pools.
- Coordinated response with Linea/security partners to contain impact.
- Highlighted that "non-price" accounting primitives can be as dangerous as oracles.

October 2025
Abracadabra.Money (DeFi Lending)

Cross-chain lending protocol behind MIM stablecoin; uses “cauldrons” as lending markets.

Amount Lost: ~$1.7M - $1.79M

How It Happened:

- Exploit hit a cauldron set (reporting points to older/deprecated cauldron versions).
- A solvency check was bypassed, enabling extraction beyond safe collateral constraints.
- Attacker drained funds; DAO paused affected contracts and acted to stabilize MIM.

Root Cause

- Smart contract logic flaw around solvency enforcement-security assumptions didn’t hold under crafted inputs/flows, allowing collateralization constraints to be bypassed.

Impact

- ~$1.7M+ stolen.
- Abracadabra paused impacted contracts and performed stabilizing actions.
- Yet another major incident added to historical exploit baggage for the protocol.

October 2025
402Bridge (x402 Ecosystem Protocol)

Cross-layer payment/bridge-like protocol in the x402 ecosystem; users granted token approvals to interact.

Amount Lost: ~$17,693 USDC (commonly cited)

How It Happened:

- A private key compromised backend/admin wallets.
- Contract ownership was transferred to an attacker-controlled address. Attacker invoked transferUserToken to pull USDC from wallets that had granted approvals.
- Stolen USDC was swapped and bridged out.

Root Cause

- Centralized key-management/back-end design error (admin keys exposed) plus an approvals model that made user funds pullable once admin control was lost.

Impact

- 200+ users affected (per reporting) with ~$17.7k confirmed stolen.
- Protocol paused operations and urged users to revoke approvals.
- Became a cautionary tale for “approval + backend admin key” architectures.

NO LOGO AVAILABLE

October 2025

Sharwa.Finance (DeFi Protocol on Arbitrum)

Arbitrum-based DeFi project whose contracts were exploited.

Amount Lost: ~$146K - $147K

How It Happened:

- Attacker exploited a smart contract weakness (postmortem/analysis references contract-level compromise).
- Funds were drained from protocol-controlled balances.
- Team investigated and published/participated in analysis and response steps.

Root Cause

- A contract logic/security flaw (insufficient validation/guardrails) that allowed an attacker to execute value-extracting calls the protocol didn't anticipate.

Impact

- ~$147K stolen.
- Service disruption and incident-response overhead for the team/community.
- Reinforced need for deeper pre-launch testing and post-launch monitoring.

October 2025

Astra Nova (AI Crypto Project)

Crypto-AI project where a third-party market maker account compromise triggered heavy token dumping.

Amount Lost: ~$10M - $10.2M

How It Happened:

- A third-party market maker account was compromised.
- Attacker gained control and liquidated a large amount of RVV on the market.
- Proceeds were swapped into USDT; some funds were reportedly moved to exchanges.

Root Cause

- Third-party operational security failure (custody/access controls at a market maker) rather than a core smart-contract exploit, showing how "launch infrastructure" can be a single point of failure.

Impact

- ~8.6% of supply reportedly dumped; major price crash (~75% intraday in some reporting).
- Team stated core contracts weren't compromised; initiated buyback/response actions.
- Investor trust hit + insider-suspicion discourse due to "MM compromise" narrative.

October 2025

BNB Chain (X Account Compromise, Not Protocol)

Official BNB chain social account hijacked to push a fake rewards/voting campaign linking to drainer/phishing infra.

Amount Lost: ~$8,000 (reported)

How It Happened:

- Attacker gained control of the verified BNB Chain X account.
- Posted phishing links/contracts disguised as official rewards/vote campaign.
- Victims clicked/connected wallets; funds drained via malicious contract.

Root Cause

- Social account security failure (account takeover) + classic "urgent reward" phishing social engineering.

Impact

- ~$8K stolen across victims (most from one larger victim).
- Short-lived but high-signal risk because official channels are trusted by default.
- Reinforced need for multi-channel verification + stronger social-account protections.

October 2025

Typus Finance (DeFi Protocol)

A DeFi protocol offering yield strategies/aggregations (notably impacted by oracle issues).

Amount Lost: ~$3.44M

How It Happened:

- Attacker targeted Typus's custom price/oracle mechanism.
- Oracle manipulation (or inadequate validation) enabled mispricing of assets used in the strategy flow.
- Mispricing was leveraged to drain protocol funds (classic "borrow/drain" via incorrect valuations).

Root Cause

- Oracle / access-control weaknesses in how Typus accepted or enforced price updates; insufficient protective checks and/or guardrails allowed manipulated prices to become actionable for value extraction.

Impact

- ~$3.44M stolen from the protocol.
- Emergency response/triage; heightened focus on oracle hardening.
- Demonstrated continued "oracle manipulation" as a top DeFi failure mode.

Incidents widely cited in October totals, but with limited public technical detail in mainstream summaries. ***These are named in multiple roundups, but the public "how/root-cause" details aren't consistently published in the broadly referenced sources.***

October 2025

GMGN (Trading/Analytics App)

A crypto trading and analytics platform; users were targeted via phishing/social engineering.

Amount Lost: ~$10.3K - $700K (not confirmed)

How It Happened:

- Attackers lured users into a fake GMGN login/verification flow.
- Victims provided credentials/session tokens (or signed malicious requests).
- Attackers used that access to drain wallets/execute unauthorized transfers.

Root Cause

- Social engineering + weak user-side security hygiene (and potentially insufficient anti-phishing/login hardening around session tokens).

Impact

- Multiple users drained; total losses reported inconsistently across sources.
- Trust hit for GMGN brand; users pushed to rotate credentials and tighten security.
- Demonstrates how "account compromise" can look like a protocol hack to users.

October 2025

DoodiPals (NFT Project)

NFT project impacted by a reported private key leak leading to fund loss.

Amount Lost: ~$171K

How It Happened:

- Sensitive key material leaked/compromised.
- Attacker used the key to access wallets/treasury assets.
- Funds moved out to attacker-controlled addresses.

Root Cause

- Operational security failure around private key storage/handling.

Impact

- ~$171K lost.
- Community trust hit; forced security reset and wallet rotations.
- Highlights recurring "key leak" pattern in NFT teams.

NO LOGO AVAILABLE

October 2025

TokenHolder (BSC Project)

A BSC project flagged for “insufficient function access control” leading to losses.

Amount Lost: ~$26,000

How It Happened:

- Exploiter abused a function lacking proper access restrictions.
- Unauthorized calls enabled value extraction.
- Funds moved out (details not public).

Root Cause

- Missing/incorrect access control on sensitive contract functions.

Impact

- ~$26k stolen.
- Limited technical disclosure publicly available.
- Another example of “basic authZ” failures in small-cap contracts.

NO LOGO AVAILABLE

October 2025

Squid (Base & Optimism)

Project labeled “Squid” impacted on Base and Optimism; public detail is sparse.

Amount Lost: ~$90,000

How It Happened:

- Reported as an “exploit/other” category incident across Base/Optimism.
- Funds drained (mechanics not broadly published).
- Post-incident response details not consolidated publicly.

Root Cause (Likely)

- Not enough public technical detail to conclusively classify beyond “exploit/other”.

Impact

- ~$90k lost.
- Likely localized user/protocol impact; limited broader ecosystem contagion reported.
- Demonstrates the long tail of mid-size exploits that get little deep-dive coverage.

NO LOGO AVAILABLE

October 2025

OracleBNB (A BNB Chain Token)

BNB Chain token/project flagged for a rug pull (liquidity pulled + socials wiped).

Amount Lost: ~$43K to $80K

How It Happened:

- Token saw sharp spike in trading activity.
- Liquidity was abruptly drained / exit-scam style sell-off occurred.
- Project deleted/wiped social presence shortly after.

Root Cause

- Project-level fraud/exit scam (not a "hack" of a third party), enabled by centralized control of liquidity/LP tokens.

Impact

- Investors left holding near-worthless tokens post-liquidity removal.
- Loss estimates vary based on how drained liquidity is measured.
- Adds to memecoin-era "rug pull" baseline risk on BSC.

October 2025

VeloraDEX (Velora/ParaSwap Ecosystem)

VeloraDEX (Velora/ParaSwap Ecosystem)

User report alleging theft via previously granted allowance/approval tied to an older router vulnerability ("AugustusV6").

Amount Lost: ~20,107.8 USDC (single user claim)

How It Happened:

- User previously approved a router/contract allowance during an earlier swap.
- Attacker later leveraged that lingering approval to pull USDC from the wallet.
- User filed a governance/forum refund request describing the drain.

Root Cause

- Residual approvals + router/allowance safety failure mode: once an allowance exists, a later exploit path can turn it into a "delayed drain".

Impact

- ~$20.1K USDC allegedly stolen from a single wallet.
- Public dispute/claims process opened (forum/governance).
- Reminder: approvals are long-lived attack surface; revoke aggressively.

RESONANCE // 2025

NOTABLE HACKS OF NOVEMBER

Balancer | November 2025

Balancer v2 (DeFi AMM / Liquidity Protocol)

A major on-chain liquidity protocol powering pools and routing across multiple networks.

Amount Lost: ~$121M - $128.6M

How It Happened:

- Attacker targeted ComposableStablePool style pools and repeatedly executed carefully sized swaps.
- Exploited precision/rounding behavior in invariant math to extract value while staying within constraints.
- Drained liquidity across multiple chains in a short window, then bridged/rotated assets.

Root Cause

- A rounding/precision issue in Balancer v2 pool math (invariant/accounting paths) that could be amplified via repeated interactions, letting an attacker "shave" value from pools at scale.

Impact

- Large multi-chain liquidity drain; downstream protocols/pools exposed via composability.
- Emergency responses, pool pauses, and ecosystem-wide monitoring/escalations.
- Triggered deeper reviews of stable-math assumptions and invariant edge cases.

November 2025

Berachain BEX (DEX on Berachain)

Berachain's native DEX (BEX), closely tied to Balancer-style pool mechanics.

Amount Lost: ~$12.8M stolen, later recovered/returned (per reports)

How It Happened:

- Balancer v2 exploit conditions impacted BEX's pool logic.
- Funds were taken during the broader Balancer incident window.
- Chain/team executed emergency actions (network halt / hard-fork style response reported) to contain/recover.

Root Cause

- Inherited exposure to the Balancer v2 vulnerability class via shared/compatible pool mechanics and composibility assumptions.

Impact

- Immediate disruption to BEX operations and user confidence.
- Incident-response playbook stress test (halts, recovery coordination).
- Funds reported returned, reducing net user loss.

---

moonwell

November 2025

Moonwell (DeFi Lending Market)

A lending/borrowing protocol on Base.

Amount Lost: ~$1M stolen and ~$3.7M bad debt reported

How It Happened:

- Oracle malfunction/mispricing overvalued wrsETH collateral.
- Attacker deposited minimal collateral and borrowed outsized assets against it.
- Repeated borrowing/withdrawing created realied loss play protocol bad debt.

Root Cause

- Incorrect oracle pricing for a collateral asset led to inflated collateral valuation and under-collateralized borrowing.

Impact

- Direct loss plus significant bad debt on the affected market.
- Emergency parameter changes/pauses and post-incident governance response.
- Renewed scrutiny on oracle dependencies and asset onboarding.

November 2025

DIMO (DePIN Project on Ethereum)

A DePIN-style project for vehicle/telematics data with an ERC-20 token.

Amount Lost: ~30M DIMO token (~3% supply); USD value reported around ~$1M, and no user funds were claimed impacted

How It Happened:

- A privileged/admin path was abused to enable token movement.
- ~30M DIMO was withdrawn/bridged/sold after the compromise.
- Teams/partners flagged abnormal activity and moved to contain.

Root Cause

- Public reporting points to a compromised privileged key / admin upgrade path abuse enabling unauthorized token extraction.

Impact

- Sudden token supply/market shock risk.
- Forced incident response around admin controls and bridge/key hygiene.
- Public reassurance emphasized “no user funds” in some summaries.

NO LOGO AVAILABLE

November 2025

DRLVaultV3 (USDC-WETH Rebalance Vault)

A vault strategy contract that swaps between USDC and WETH.

Amount Lost: Not clearly stated in the primary technical writeup; some secondary reporting estimated ~$98K, and the attacker address was tagged as whitehat, implying likely recovery.

How It Happened:

- Attacker flash-borrowed large USDC, pushed pool price by buying WETH aggressively.
- Triggered the vault’s swap function to trade at the manipulated price.
- Unwound price manipulation and captured profit from the vault’s “bad” execution.

Root Cause

- The vault computed minimum-out (slippage) on-chain using the same pool state that could be manipulated in-transaction., nullifying protection.

Impact

- Demonstrated classic “slippage based on manipulable quote” design risk.
- Likely recoverable if whiteahat coordination holds.
- Reinforces best practice: min-out derived off-chain or from robust oracle/TWAP.

Polymarket | November 2025

Polymarket (Prediction Market on Polygon)

A prediction market where users trade on event outcomes.

Amount Lost: >$500K reported from user theft in the campaign

How It Happened:

- Attackers posted obfuscated phishing links in market comment sections.
- Victims clicked, landed on lookalike pages, and logged in.
- Malicious scripts/credential theft enabled subsequent wallet/account draining.

Root Cause

- User-targeted phishing enabled by surface area in comments + social engineering, not a core smart contract flaw.

Impact

- Direct user losses and fear around platform social surfaces.
- Likely increases moderation, link filtering, and anti-phishing UX controls.
- Reputational hit despite protocol contracts not necessarily being exploited.

November 2025

Hyperliquid (Perp DEX)

A decentralized derivatives venue with a shared liquidity vault (HLP/Hyperliquidity).

Amount Lost: ~$4.9M

How It Happened:

- Attacker coordinated positions around POPCAT with leverage and market structure tactics.
- Manipulated price dynamics/marking mechanics to force vault losses.
- Exited positions, leaving the liquidity vault with bad debt/loss.

Root Cause

- Price manipulation / market-strucuture exploitation where liquidity/risk controls were insufficient to withstand adversarial positioning in a thin or gameable market.

Impact

- Direct losses to liquidity backstop.
- Temporary restrictions/changes to risk parameters are typical after such events.
- Elevated debate on oracle/mark prices, per-market caps, and adversarial trading assumptions.

NO LOGO AVAILABLE

November 2025

GANA Payment (DeFi Payment/Staking Project)

A BSC/BNB chain project described as a DeFi payments platform.

Amount Lost: ~$3.1M

How It Happened:

- Attacker gained control over a critical contract/admin pathway.
- Abused an unstake/withdraw capability to extract funds/liquidity.
- Funds were consolidated and partially routed through laundering paths per reporting.

Root Cause

- Reporting strongly suggests privileged access compromise or deployer/admin misuse (key management failure) rather than a purely permissionless logic bug.

Impact

- Material user liquidity loss and trust collapse.
- Intensified scrutiny of admin controls, timelocks, and key custody practices.
- Response often includes contract pauses and postmortem/bounty negotiations.

November 2025

Yearn Finance (DeFi Yield Protocol)

A long-running DeFi yield protocol; incident focused on specific yETH pool.

Amount Lost: ~$9M

How It Happened:

- Attacker deposited a trivial amount (famously “dust-level”) into the pool.
- Exploited a flaw to mint an astronomically large amount of yETH.
- Swapped the illegitimately minted yETH into real assets (LSTs), draining value.

Root Cause

- Analyses describe an accounting/cache/storage desynchronization that enabled effectively “infinite mint” under edge conditions.

Impact

- Direct pool drain and immediate reputational shock.
- Asset recovery efforts and contract/pool review.
- Reinforced need for invariant/accounting fuzzing and edge-case simulations.

November 2025

Aerodrome + Velodrome (DEX on Base and Optimism)

Two major DEXs (aerodrome on Base; Velodrome on Optimism).

Amount Lost: ~$700K confirmed in multiple reports, while some estimates suggested higher in the early hours

How It Happened:

- Attackers executed a DNS/domain hijack (domain registrar / DNS control).
- Users were redirected to lookalike front-ends that prompted malicious interactions.
- Wallet drainers stole funds from users who signed/approved transactions.

Root Cause

- Web2 infrastructure compromise (domain/DNS control plane), not the DEX smart contracts).

Impact

- User wallet losses; urgent “do not use main domain” advisories.
- Domain migrations, registrar hardening, and improved monitoring.
- Reinforced need for decentralized front-ends / signed builds / domain protections.

November 2025

Port3 Network (BNB Chain Project)

A web3/AI-related project whose token supply and bridge path were abused.

Amount Lost: Reported very differently: some reporting frames it as multi-million “impact”, while cash-out described includes dumps yielding much smaller realized proceeds.

How It Happened:

- Attacker exploited a CATERC20 cross-chain solution weakness.
- Minted ~1B fake PORT3, then dumoed a portion for BNB and burned the rest.

Root Cause

- Bridge/cross-chain mint validation failure (insufficient verification of mint/burn or message authenticity in the cross-chain path).

Impact

- Severe token price shock (reports of >80% crash).
- Trust damage around bridging and token integrity.
- Likely forced bridge suspension and contract upgrades/audits.

November 2025

BasisOS “Agentic FoF” (AI-Project on Base)

An AI-managed on-chain vault/strategy product under BasisOS.

Amount Lost: ~$531K

How It Happened:

- Vault was compromised and funds moved out.
- Team paused vault operations and restricted withdrawals while investigating.
- Reporting indicates an internal malicious actor was suspected/claimed.

Root Cause

- Public reporting points to insider threat / privileged access misuse, not a purely external contract bug.

Impact

- Immediate vault suspension and user withdrawal disruption.
- Governance/trust hit; stronger internal controls likely required.
- Sparked debate on Ai-vault operational security and custody.

November 2025

Upbit (South Korena CEX)

One of South Korea’s largest centralized exchanges.

Amount Lost: Commonly reported ~$30M+

How It Happened:

- Unauthorized withdrawals were detected from a Solana-related hot wallet.
- Exchange suspended deposits/withdrawals and initiated security checks.
- Authorities and regulators began investigations shortly afte disclosures.

Root Cause (Likely)

- Public reporting includes claims of a weakness enabling private-key interfencing (still not fully verified publicly end-to-end).

Impact

- Temporary halt of exchange services and operational disruption.
- Increased regulatory scrutiny and law enforcement involvement.
- Renewed focus on hot-wallet architecture and key-management isolation.

Incidents widely cited in November totals, but with limited public technical detail in mainstream summaries. *These are named in multiple roundups, but the public "how/root-cause" details aren't consistently published in the broadly referenced sources.*

November 2025

World Liberty Financial (WLFI) (EVM Project)

A token/project referenced in incident trackers.

Amount Lost: Not cleanly disclosed as "stolen funds". Reports describe a defensive action where 166.67 WLFI tokens ($22.14M) were burned, tied to a mnemonic/phishing incident.

How It Happened:

- Mnemonic/seed exposure via phishing/social engineering was reported.
- Team executed emergency actions (including token burn/containment measures).
- Public details focus on containment more than full attacker workflow.

Root Cause (Likely)

- Credential/seed compromise (human + operational security failure)

Impact

- Major trust event; emergency token actions are highly disruptive.
- Users pushed to rotate wallets/credentials.
- Long tail of reputational and governance fallout.

November 2025

NOFX AI (Trading Bot)

An open-source automated trading system used by some CEX/DEX traders.

Amount Lost: Not publicly quantified

How It Happened:

- Vulnerabilities exposed wallet private keys and exchange API credentials.
- Affected users' credentials were abused for theft attempts/incidents.
- Exchanges and responders revoked keys for impacted users where possible.

Root Cause (Likely)

- Sensitive key material exposure via software design/implementation flaws in the toolchain.

Impact

- Users forced to rotate API keys and wallets; automation credentials revoked.
- Tooling-trust hit for automated trading stacks.
- Stronger push toward secret isolation and "no private keys in app memory/logs."

RESONANCE // 2025

NOTABLE HACKS OF DECEMBER

Goldfinch | December 2025

Goldfinch (Onchain Private Credit)

DeFi private credit protocol; issue centered on an old contract + user approval state.

Amount Lost: ~$330,000

How It Happened:

- Old contract contained a vulnerability enabling unauthorized pulls against approvals.
- Specific user (deltatiger.eth) had not revoked authorization in time.
- Attacker exploited and siphoned funds.
- ~118 ETH was sent into Tornado Cash (reported).

Root Cause

- Legacy contract vulnerability + persistent token approvals.

Impact

- Loss was user-specific, but exposed approval hygiene risks.
- Push for routine approval revocation and monitoring.

December 2025

Private Wallet (Whale Gnosis Safe)

A whale wallet (Gnosis Safe) drained after single-key control was compromised.

Amount Lost: ~$27,300,000

How It Happened:

- Wallet configured effectively as 1-of-1, so a single compromised key meant full control.
- Attacker drained assets and laundered chunks via Tornado Cash-style patterns (reported).
- Attacker retained control of the wallet after the drain.
- An active leveraged position was reportedly left open, adding risk.

Root Cause

- Operational security failure; key compromise + unsafe multisig configuration (single point of failure).

Impact

- Massive loss from wallet security, not protocol code.
- Highlights why “multisig” isn’t safety if it’s 1-of-1 in practice.
- Secondary market risk via lingering leveraged exposure.

December 2025

babur.sol (Private Solana Wallet)

A high-value wallet tied to a .sol identity reportedly drained via key compromise.

Amount Lost: ~$22M - $27M

How It Happened:

- Victim’s keys/endpoint believed compromised (malware/phishing suspected).
- Assets were rapidly moved/swapped across venued/chains.
- Funds then dispersed to reduce traceability.

Root Cause

- Endpoint/key theft rather than a smart-contract vulnerability.

Impact

- Reinforces “OPSEC > onchain security” for whales.
- Shows attacker playbook: fast swaps + dispersal.

December 2025

Trust Wallet (Multi-Chain Wallet)

Major wallet provider; incident impacted users of a specific extension version.

Amount Lost: ~$8,500,000

How It Happened:

- A malicious modification was introduced into Trust Wallet's internal codebase (analytics logic).
- The legitimate PostHog library was abused to redirect analytics to an attacker-controlled server.
- Users running the affected extension version were drained.
- Extension was rolled back and upgrades + compensation process initiated.

Root Cause

- Compromised internal code path / build pipeline weakness (malicious code in first-party logic, not just a 3rd party package).

Impact

- ~2,520 addresses reportedly affected.
- Trust hit to wallet extension supply chain and update integrity.
- Triggered emergency versioning/rollback + user compensation workflows.

December 2025

Unleash Protocol (Story Protocol Ecosystem)

DeFi protocol deployed on the Story ecosystem.

Amount Lost: ~$3,900,000

How It Happened:

- Attacker abused multisig / governance privileges.
- Executed an unauthorized contract upgrade.
- Transferred user assets (e.g., WIP/USDC/WETH and related assets) to external addresses.
- Assets were then moved cross-chain/off-platform.

Root Cause

- Privilege compromise: attacker gained or misused upgrade authority (admin/governance controls).

Impact

- Protocol operations suspended; investigation/audit launched.
- Users warned not to interact with contracts.
- Ecosystem impact contained (Story itself reported unaffected).

December 2025

Flow (L1 / Execution Layer)

Flow foundation / Flow network.

Amount Lost: ~$3,900,000

How It Happened:

- Attacker exploited a vulnerability in the Flow execution layer.
- Moved ~$3.9M off-network before response finalized.
- Validators coordinated and halted operations to contain damage.
- Incident reported as not affecting existing balances/deposits.

Root Cause

- Core execution-layer bug (protocol-level vulnerability rather than an app contract issue).

Impact

- Network halt / emergency coordination event.
- Reputational damage for protocol security posture.
- User custody/deposits reportedly remained intact.

December 2025

USPD (Ethereum Stablecoin)

USD-pegged stablecoin system issuing USPD.

Amount Lost: ~$1,000,000

How It Happened (summary)?

During deployment, attacker used Multicall3 to pre-initialize proxy and seizer admin privileges.

Malicious implementation was disguised while forwarding calls to audited logic.

After a dormancy period, attacker upgraded proxy and executed exploit.

Minted ~98M USPD and transferred out ~232 stETH.

Root Cause

Proxy initialization/admin takeover (“CPIMP” pattern: an operational/deployment flaw where ownership was captured before legitimate initialization.

Impact

Inflationary mint + collateral drain event.

Public attacker addresses disclosed; tracing + bounty offered.

Demonstrated how “audited code” can be bypasses by proxy control.

December 2025

Aevo (Ethereum DeFi Project)

Aevo (formerly Ribbon ecosystem) legacy DOV vaults.

Amount Lost: ~$2,700,000

How It Happened:

- A vulnerability introduced during a smart-contract upgrade impacted legacy vaults.
- Attacker abused oracle/administrative behavior (writeups describe proxy-admin/oracle manipulation dynamics).
- Drain executed from the affected legacy vaults.
- Funds dispersed afterward.

Root Cause

- Upgrade-induced vulnerability + unsafe admin/oracle control surface on legacy contracts.

Impact

- Losses isolated to legacy vaults; newer Aevo infra said not impacted.
- Highlighted "legacy surface area" risks even after protocol migrations.
- Reimbursement plans and comms became contentious (publicly discussed).

December 2025

Yearn Finance V1 (Ethereum-based Project)

Yearn legacy V1/iEarn vault contract (TUSD).

Amount Lost: ~$293,000 (~103 ETH after conversion)

How It Happened:

- Vault strategy misconfigured (tracking a different underlying exposure than the vault asset).
- Attacker used a large Morpho flashloan to manipulate accounting.
- "Donated" assets the vault didn't recognize, crushing denominator and inflating shares.
- Cashed out via Curve pool dynamics, extracting value and converting to ETH.

Root Cause

- Configuration error in legacy contract strategy/adapter assumptions enabling accounting manipulation under flashloan leverage.

Impact

- Direct loss + downstream pricing stress to connected liquidity venues.
- Renewed attention on "immutable legacy contracts" as modern targets.
- Emphasized need to sunset/drain old vaults, not just "move on".

December 2025
Futureswap (DeFi Protocol)

Governance-controlled DeFi protocol.

Amount Lost: ~$830,000

How It Happened:

- Attacker created a malicious governance proposal.
- Used flash loans to temporarily acquire enough voting power.
- Proposal passed, granting the attack contract privileges.
- Attack contract transferred tokens from user balances/allowances.

Root Cause

- Weak governance protections against flashloan voting and privilege escalation.

Impact

- Direct loss + governance credibility hit.
- Demonstrated need for vote-locks, timelocks, quorum rules, and anti-flashloan voting design.

NO LOGO AVAILABLE

December 2025
OG Foundation (OG Ecosystem)

OG ecosystem foundation; rewards distribution contract.

Amount Lost: ~$520,000

How It Happened:

- Targeted attack led to breach of the reward contract.
- Emergency withdrawal function was exploited to extract tokens/ETH/USDT value.
- Reported lateral movement tied to internal services after a Next.js CVE was exploited (as described).
- Tokens bridged and funds dispersed via Tornado Cash patterns.

Root Cause

- Operational compromise + exposed emergency controls (attack chain included infra weakness and privileged function abuse).

Impact

- Multiple services affected; core chain and user funds reported safe.
- Loss of reward funds + ecosystem disruption.
- Incident response required across infra + smart contract surfaces.

Incidents widely cited in December totals, but with limited public technical detail in mainstream summaries. *These are named in multiple roundups, but the public "how/root-cause" details aren't consistently published in the broadly referenced sources.*

December 2025

Debot (Wallet)

Wallet/app where user keys were reportedly compromised.

Amount Lost: ~$255,000 (and theft was reported as ongoing at the time)

How It Happened:

- User private keys tied to Debot were reportedly compromised.
- Attacker drained funds across affected addresses.
- Project disputed "core wallet compromised" claims but acknowledged impacted addresses.
- Compensation process executed for claims (reported).

Root Cause (Likely)

- Key compromise (exact initial vector not fully public).

Impact

- Direct user losses + reputational damage.
- Compensation precedent set (100% commitment claimed).

NO LOGO AVAILABLE

December 2025

MSCST (BSC Project)

A BSC contract exploited via price manipulation + reward logic abuse.

Amount Lost: ~$130,000

How It Happened:

- Attacker used a flashloan to manipulate a PancakeSwap pool price.
- Exploited releaseReward() lacking ACL.
- Extracted value by abusing reward/price assumptions.
- Exited with profits.

Root Cause

- Missing access control + price-dependent reward logic.

Impact

- Loss of >$130K.
- Demonstrates recurring BSC pattern: weak ACL + AMM price reliance.

December 2025

Private User (EVM-based)

A user drained after signing a malicious permit.

Amount Lost: ~$563,590

How It Happened:

- Victim phished into signing an onchain permit (or equivalent approval signature).
- Attacker used trhe granted allowance to transfer tokens.
- Funds moved out quickly after signature execution.

Root Cause

- Signature phishing (human-layer exploit).

Impact

- Reinforces “don’t sign what you don’t parse”.
- Demand for wallet-level signature simulation + spend-limit tooling.

December 2025

Private User (EVM-based)

Another poisoned-history case similar to the $50M incident.

Amount Lost: ~$81,000

How It Happened:

- Attacker sent dust transaction from a lookalike address.
- Victim copied address from history.
- Sent funds to attacker-controlled address.

Root Cause

- Transaction-history trust + lookalike addresses.

Impact

- Shows scalability: same technique hits both whales and retail.

December 2025

Rari Capital (Ethereum-based Project)

Defunct/legacy DeFi contracts still holding value, exploited via implementation/control weakness.

Amount Lost: ~$2,000,000

How It Happened:

- Investigators observed anomalous borrowing activity.
- Attacker interacted with protocol without posting collateral (reported).
- Preliminary analysis pointed to a hijacked/vulnerable implementation path.
- Extraction occurred before widespread flagging.

Root Cause

- Legacy contract maintenance gap + implementation control weakness.

Impact

- Reminder that “inactive” protocols remain targets if funds remain.
- Pushes ecosystem toward draining/sunsetting old deployments.

December 2025

ZEROBASE (BSC Ecosystem Project)

Product whose frontend was impersonated to trick users into approvals.

Amount Lost: Largest single loss ~$123,000 (total not fully disclosed)

How It Happened:

- Malicious contract (“Vault”) impersonated ZEROBASE frontend.
- Users were tricked into authorizing USDT spending.
- Attacker drained funds from approved wallets.
- Funds moved onward (reported to an Ethereum address).

Root Cause

- Frontend compromise / UI trust break → approval phishing.

Impact

- Hundred of addresses affected (reported).
- Community urged to revoke approvals (revoke.cash etc.).
- Illustrates “wallet drain without protocol bug” via UI compromise.

RESONANCE // 2025

EMERGING THREAT VECTORS

1. Address Poisoning (Transaction History Manipulation)

Examples:

- $50M address poisoning victim (December 2025)
- Multiple retail wallet losses across Ethereum and BSC (throughout 2025)

Why it's alarming:

- Requires zero smart contract interaction and bypasses all audits.
- Exploits human behavior + wallet UX assumptions.
- Scales from retail to whales with the same technique, making it one of the most cost-effective attack vectors for criminals.

2. Privileged Key & Multisig Compromise (Admin Takeovers)

Examples:

- Unleash Protocol
- USPD Stablecoin
- DIMO
- Evoq Finance
- Seedify

Why it's alarming:

- Turns "admin features" into instant kill switches.
- Multisigs are often misconfigured (1-of-1, weak signer hygiene).
- One compromised key can bypass years of secure smart-contract engineering.

3. Wallet-Level Attacks (Not Protocol Hacks)

Examples:

- babur.sol (~$22–27M)
- Hyperliquid whale loss (~$21M)
- Multiple private wallet drains across Q3–Q4

Why it's alarming:

- The largest dollar losses of 2025 came from wallet compromises, not DeFi bugs.
- Malware, fake Zoom calls, deepfakes, and fake installers are now standard attacker tools.
- No on-chain mitigation once keys are exposed.

4. Approval Abuse & Permit-Based Drains

Examples:

- Kame Aggregator
- dTRINITY / dLEND
- VeloraDEX user case
- Multiple airdrop-related drains (DexMaxAI, ZEROBASE)

Why it's alarming:

- Old approvals act as time bombs.
- Permit signatures remove the "approval transaction" warning entirely.
- Users rarely understand the scope and duration of what they sign.

5. Governance Attacks (Flashloan Voting & Proposal Abuse)

Examples:

- Futureswap
- Mango-style governance patterns resurfacing in smaller DAOs

Why it's alarming:

- Flash liquidity can rewrite protocol rules in minutes.
- Many DAOs still lack vote delays, quorum protection, or vote escrow.
- Governance has become an attack surface, not a safeguard.

6. Oracle & Pricing Manipulation (Still Not Solved)

Examples:

- Moonwell (Base)
- Typus Finance
- NewGold Protocol
- Astera

Why it's alarming:

- Oracles remain one of the most exploited DeFi primitives.
- Even "trusted" oracles fail when edge cases, LSTs, or new assets are introduced.
- Attackers repeatedly extract value without breaking protocol invariants.

7. Upgradeable Contract Abuse (Proxy & Initialization Attacks)

Examples:

- USPD (CPIMP proxy takeover)
- Aevo legacy vaults
- Multiple BSC proxy exploits

Why it's alarming:

- Exploits often lie dormant for weeks or months before activation.
- Audited logic is irrelevant if proxy control is compromised.
- Upgrade paths are increasingly targeted during deployment, not runtime.

8. Supply Chain Attacks (Wallets, Libraries, Frontends)

Examples:

- Trust Wallet extension compromise (~$8.5M)
- NPM / React-related crypto site injections
- Shai-Hulud-style package compromises

Why it's alarming:

- One compromised dependency can impact thousands of users instantly.
- These attacks bypass on-chain security entirely.
- Web3 still heavily relies on Web2 build and distribution pipelines.

9. Frontend & Domain Hijacking

Examples:

- Aerodrome + Velodrome DNS hijack
- ZEROBASE frontend impersonation
- PEPE website compromise

Why it's alarming:

- Users trust frontends more than contracts.
- A compromised domain turns a safe protocol into a wallet drainer.
- DNS and hosting security is still treated as secondary in Web3.

10. Bridge & Cross-Chain Trust Exploits

Examples:

- Yala Protocol
- Seedify bridge exploit
- Shibarium bridge incident
- NoOnes Solana bridge loss

Why it's alarming:

- Bridges combine key risk, oracle risk, and message validation risk.
- Attackers increasingly exploit deployment keys and trusted peers, not code bugs.
- Cross-chain exploits remain high-impact with low recovery rates.

RESONANCE // 2025

SECURITY RECOMMENDATIONS

1. Kill Single Points of Failure in Key Management

- Use true multisig setups (minimum 2-of-3 or 3-of-5) with signers on separate devices and networks.
- Store signing keys on hardware wallets only; never on daily-use laptops or cloud backups.
- Rotate admin keys periodically and after every team change, incident, or device replacement.

2. Treat Approvals as Live Explosives

- Grant minimal approvals (exact amounts, not infinite) and revoke them after use.
- Regularly audit approvals using tools like revoke dashboards and automate alerts for new approvals.
- For projects, design contracts to avoid long-lived allowances and prefer pull-based patterns.

3. Harden Upgrade & Proxy Paths (Not Just Logic)

- Use timelocks (24–72 hours minimum) on all upgrades and admin actions.
- Separate deployment keys from upgrade keys, and destroy deployment keys after launch.
- Monitor proxy admin addresses in real time and alert on any ownership or implementation change.
- **4. Assume Frontends Will Be Attacked**
- Treat frontend, DNS, and hosting as part of the security perimeter.
- Use domain locks, registrar-level protections, signed builds, and subresource integrity (SRI).
- Always provide users with on-chain contract verification paths (read-only contract UIs).

5. Build for Humans, Not Just Contracts

- Never rely on users copying addresses from history; encourage address books and whitelists.
- Wallets and apps should show full address verification prompts for high-value transfers.
- Educate users: "If you didn't type or whitelist it, don't send to it."

6. Lock Down Governance Against Flash Attacks

- Enforce vote delays, snapshot voting, and minimum proposal lifetimes.
- Use vote escrow / stake duration requirements to neutralize flashloan voting.
- Alert on governance proposals that modify permissions, upgrades, or transfer rights.

7. Use Oracles Like Adversaries Exist (Because They Do)

- Never rely on single-source or spot-price oracles, especially from AMMs.
- Use TWAPs, circuit breakers, deviation thresholds, and multi-oracle aggregation.
- Apply stricter controls for new assets, LSTs, and exotic collateral.

8. Segment Risk: Separate Users, Treasuries, and Ops

- Never mix treasury wallets, ops wallets, and user-facing wallets.
- Limit blast radius: one wallet = one purpose.
- Monitor for abnormal flows between internal wallets and pause immediately when detected.

9. Assume Supply Chain Compromise Is Inevitable

- Pin dependencies, audit updates, and monitor for unexpected package changes.
- Restrict who can publish builds and require multi-party review for releases.
- For wallets and apps, treat updates as security-critical events, not routine pushes.

10. Make Incident Response a First-Class Feature

- Prepare a runbook: pause switches, comms templates, law enforcement contacts, exchange liaisons.
- Set up real-time alerts for abnormal withdrawals, upgrades, governance actions, and approvals.
- Practice incident simulations; speed of response often determines whether a $100K loss becomes $100M.

RESONANCE // 2025

CLOSING THOUGHTS

The events of 2025 make one reality impossible to ignore: Web3 is no longer being broken by unknown threats, but by familiar ones that keep repeating. From admin key compromises and unsafe upgrades to phishing, approval abuse, and address poisoning, attackers consistently exploited the same weaknesses across different ecosystems, chains, and user profiles. The scale of losses was not driven by technical sophistication alone, but by gaps in operational discipline, security ownership, and user experience design. In many cases, the underlying smart contracts functioned exactly as written; the failures happened in how they were governed, accessed, deployed, or trusted.

As Web3 moves into 2026, the path forward is clear but demanding. Security can no longer be treated as an audit milestone or a post-incident response; it must be an ongoing operational practice spanning code, infrastructure, governance, and human behavior. Reducing losses will not come from more complex technology, but from better defaults, safer assumptions, and systems designed with adversarial reality in mind. The lessons of 2025 are already written in losses; whether the ecosystem chooses to learn from them will define whether the next year is remembered for progress... or repetition.

Resonance Security provides best-in-class full-spectrum cybersecurity solutions for SMBs, Institutions, and Web3.

Our Specialties & Services

- **Modular cybersecurity platform** for companies, Web3, AI, and individuals
- **Continuous monitoring tools** for domain changes, vulnerability scans, leak detection, and phishing tests
- **Offensive services** like pentesting, config reviews, and smart contract audits
- **Defensive support** including 24/7 SOC, incident response, and forensics
- **Cybersecurity training and CISO-as-a-Service** for teams and enterprises
- **PulseCheck**, an instant security assessment tool to see where you stand

Our Certifications

Our Differentiators

- Unified **offense + defense** in one platform
- Built for **Web3, AI, and emerging tech** environment
- Simple for **both technical and non-technical users**
- **Hands-on support** from expert engineers
- Full coverage across **code, cloud, and devices**
- Backed by **global security experts**

Our In-House Cybersecurity Tools

EQUALIZER
Seamless phishing campaign simulator to test team resilience

Reverb
Customized vulnerability scanner for your exposed assets

TUNER
24/7 data leak and credential monitoring and notification tool

HARMONY
Real-time domain monitoring tool to flag changes across web assets

Our Happy Clients

AVALANCHE · primex · near · chiliz · Velvet · PAKT · freename · kulipa

PhishGuard by RESONANCE
Protect your inbox against phishing attacks

PulseCheck [SCAN ME] →
Think you're secure enough?
Take a free PulseCheck assessment and find out.

CONTACT US

Check us out at
www.resonance.security

+1 (646) 713 0881
support@resonance.security

RESONANCE