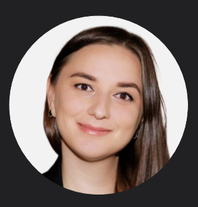
HACKEN

The Hacken 2025 Half Year Web3 Security Report

Halfway through 2025 — $3.1B lost

The biggest hack ever, largest smart contract exploit, worst DeFi quarter in years, and the first Uniswap V4 breach.

hacken.io



Yevheniia Broshevan
Hacken Co-Founder & CBDO

X linkedIn

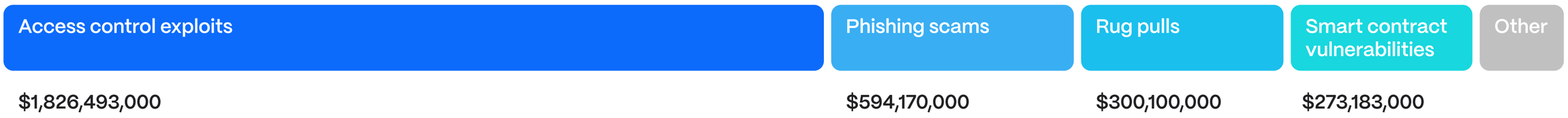
"2025 has been a wake-up call. In just two quarters, $3.1 billion was lost to access control failures, DeFi vulnerabilities, and social engineering. As blockchain reaches enterprise scale and regulations advance, cybersecurity becomes a core business function. Projects that invest in resilience and security build trust, meet compliance, and protect digital innovation."

Web3 Security Highlights Halfway Through 2025

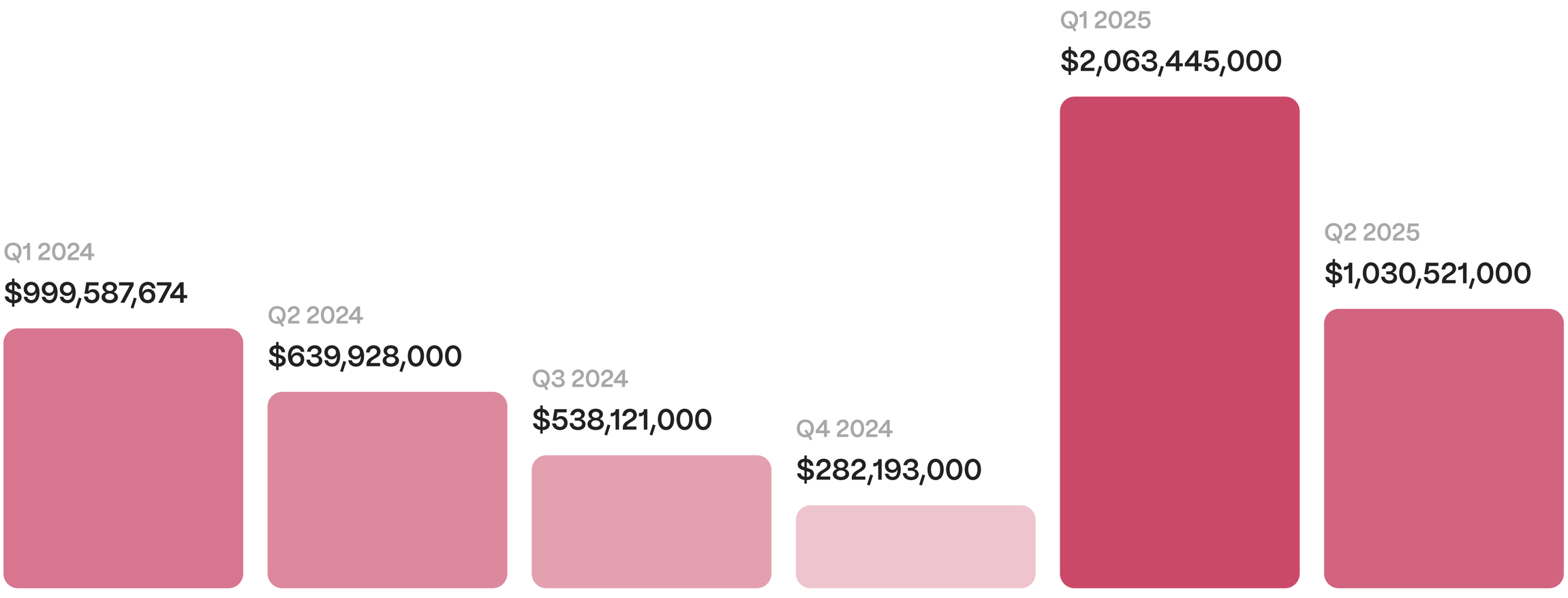
1. $3.1 billion lost from the beginning of the 2025 across all Web3 platforms, more than in 2024!
2. Nearly $600 million (≈19%) went to phishing and social engineering schemes
3. DeFi saw its worst quarter since 2023, a single overflow bug cost Cetus $223 million in under 15 minutes.
4. Attackers found the first big hole in a Uniswap V4 hook, draining $12 million from Cork Protocol.

2025 Half Year Total Value Stolen By Attack Type

Total 2025 loss: $3,093,946,000



Crypto losses per quarter in 2024, 2025



Introduction

This half-year Web3 security report looks at what happened in the first two quarters of 2025 and compares it both with each other and with the full year of 2024. So far this year we've seen over $3.1 billion in losses from smart-contract bugs, access-control oversights, rug pulls and scams due to phishing and social engineering. That already tops last year's $2.85 billion, a rise of more than six percent. The Bybit hack in Q1, which stole nearly $1.5 billion, was an outlier, but even without it projects suffered heavy hits across the board, and the mix of loss types hasn't shifted dramatically from past patterns of 2024.

This report presents a categorized breakdown of the 2025's incidents, identifies trends, and highlights a growing need for operational maturity across DeFi protocols and CeFi platforms.

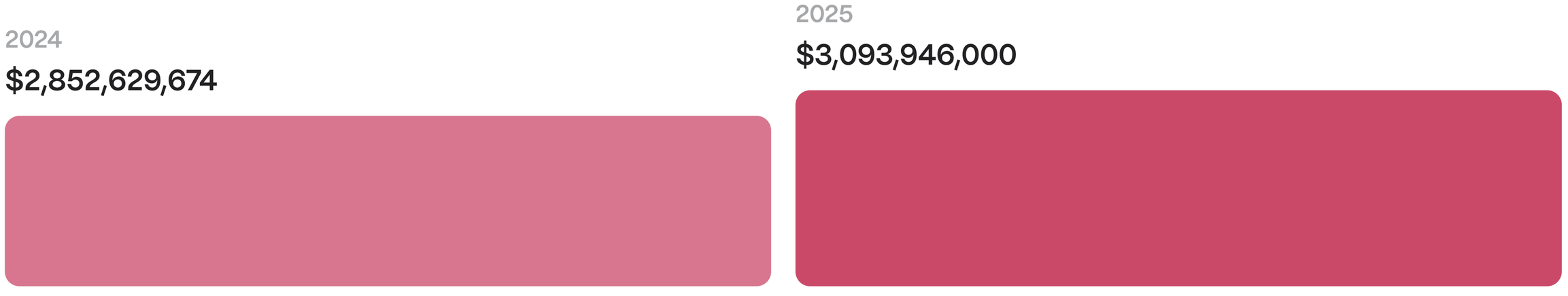
Key Trends In Crypto Hacks

In these first six months of 2025, access-control exploits have dominated, accounting for about 59% of total losses (roughly $1.83 billion) drained from both centralized and decentralized platforms. Smart-contract vulnerabilities made up around eight percent, with $263 million lost in the first half, including the $223 million Cetus exploit that marked DeFi's worst quarter since early 2023 with 300m drained across all the hacks.

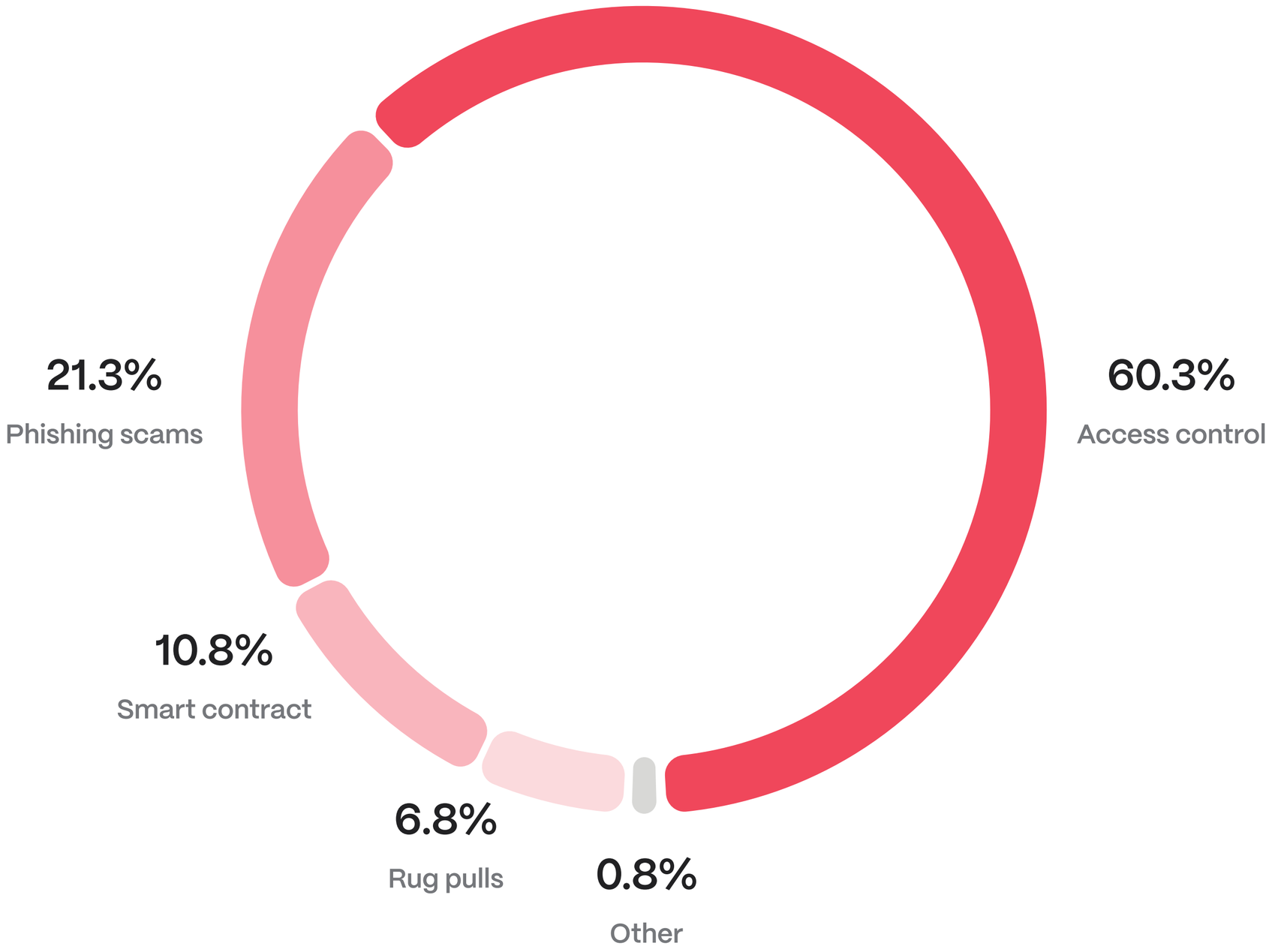
Phishing and social-engineering scams also set new records. In late April, a scammer tricked one person into handing over $330 million worth of Bitcoin, and phone-based schemes pretending to be Coinbase support cost users over $100 million only in this year alone after a data leak exposed contact details.

In 2025 so far we have witnessed:

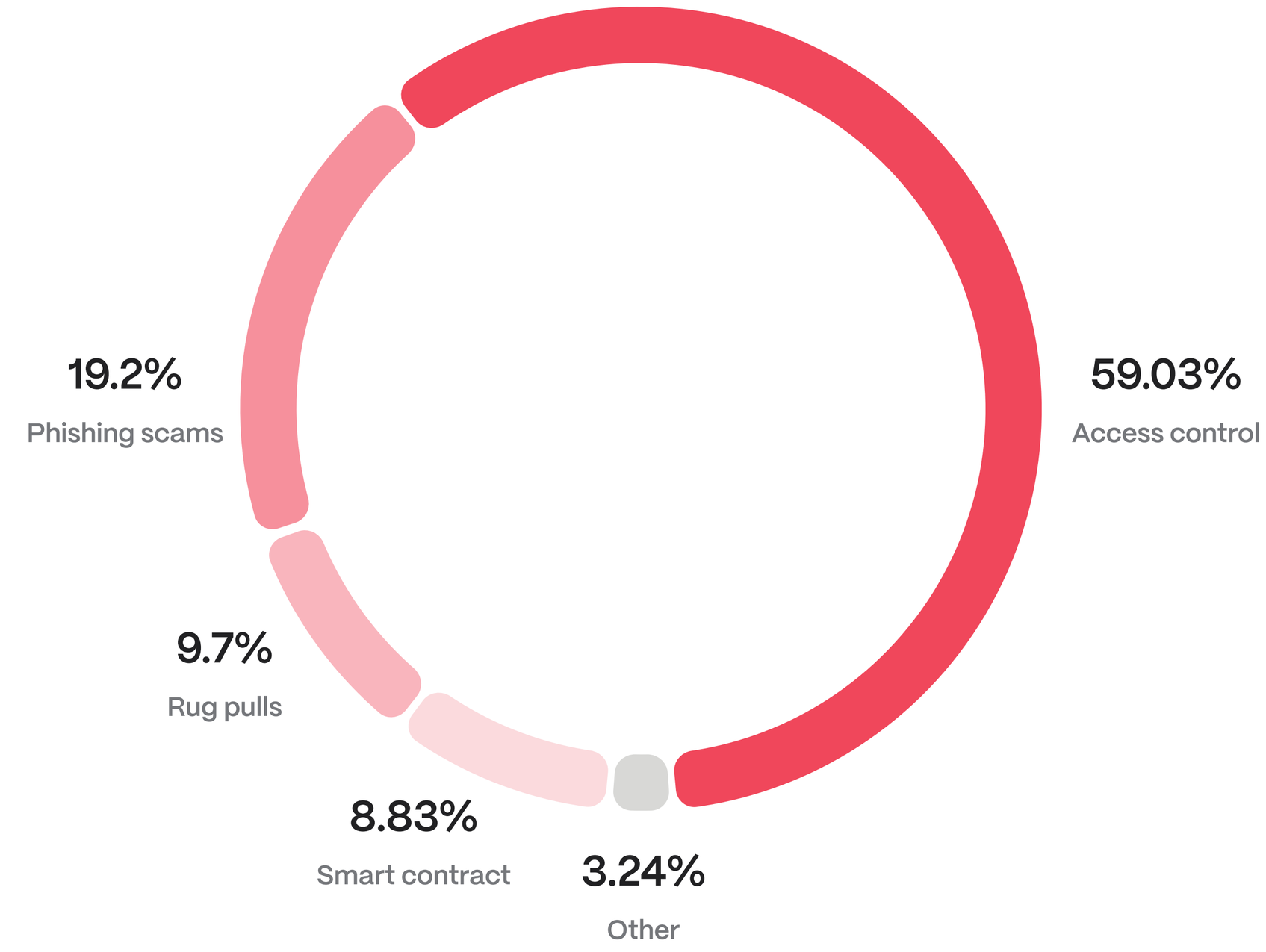
- biggest hack ever (ByBit, 1.465b)
- biggest hack due to smart contract vulnerability exploit (Cetus, 223m)
- biggest theft of single individual (elderly US individual, 330.7m)
- biggest rug pull ($LIBRA, 300m)
- first major exploit due to vulnerability in Uniswap V4 hook (Cork, 12m)
- exploit after longest time passed since deployment – more than 2 years (1inch's Settlement, 5m)



2024


21.3%
Phishing scams
60.3%
Access control
10.8%
Smart contract
6.8%
Rug pulls
0.8%
Other

2025


19.2%
Phishing scams
59.03%
Access control
9.7%
Rug pulls
8.83%
Smart contract
3.24%
Other

Access Control Exploits

In the first half of 2025, operational security flaws led to roughly $1.83 billion being stolen across both DeFi and CeFi platforms. Almost all of that (about $1.63 billion) occurred in the first quarter, making up 83% of Q1's total losses. The largest exploit of Q1 2025 – the $1.46B Bybit hack – was a direct result of a compromised signer interface (Safe{Wallet}), allowing attackers to propose and propagate a malicious transaction.

The malicious proposal manipulated the Safe's delegate call setup to seize control of the wallet. Within days, the Infini protocol lost another $50 million when a former developer simply withdrew all funds from the system in one go.

By contrast, the second quarter was much quieter on access control failures, with under $200 million drained (less than 20% of that quarter's losses). Still, several notable cases underline how a single over-powered role or key can wreak havoc in minutes.

- On UPCX, attackers hijacked the ProxyAdmin owner account, pushed through a malicious implementation upgrade, and called the built-in withdrawByAdmin function to drain 18.4 million UPC tokens (around $70 million).

- At KiloEx, a missing permission check in the MinimalForwarder contract let an attacker skew oracle prices near zero, to open a leveraged position, spike the price back up, and close out for a profit on BNB Chain, Base and opBNB – the first major hack on opBNB – draining $7.5 million.

- In the Roar case, the rogue developer back-doored the staking contract by hard-coding their own wallet's user.amount in the constructor. That gave them withdrawal rights from day one which they capitalised as soon as liquidity was added to LP – $800 000 drained.

- A compromised admin key of zkSync allowed a single signer to drain the remaining unclaimed ZK airdrop tokens (about $5 million) because the so-called multisig was actually 1-of-1, giving one leaked private key total control.

- On June 18, 2025, Iran's largest crypto exchange, Nobitex, was breached in what looked like a politically motivated attack. Attackers stole over $90 million in BTC, ETH, DOGE, TRX and other assets, sending everything to "burner" addresses.

Hacken Recommends

Learn More ↗

Automated Incident Response

Hacken Extractor can automatically detect and prevent multisig exploits with its advanced Safe Multisig Monitor and TVL Monitor capabilities.

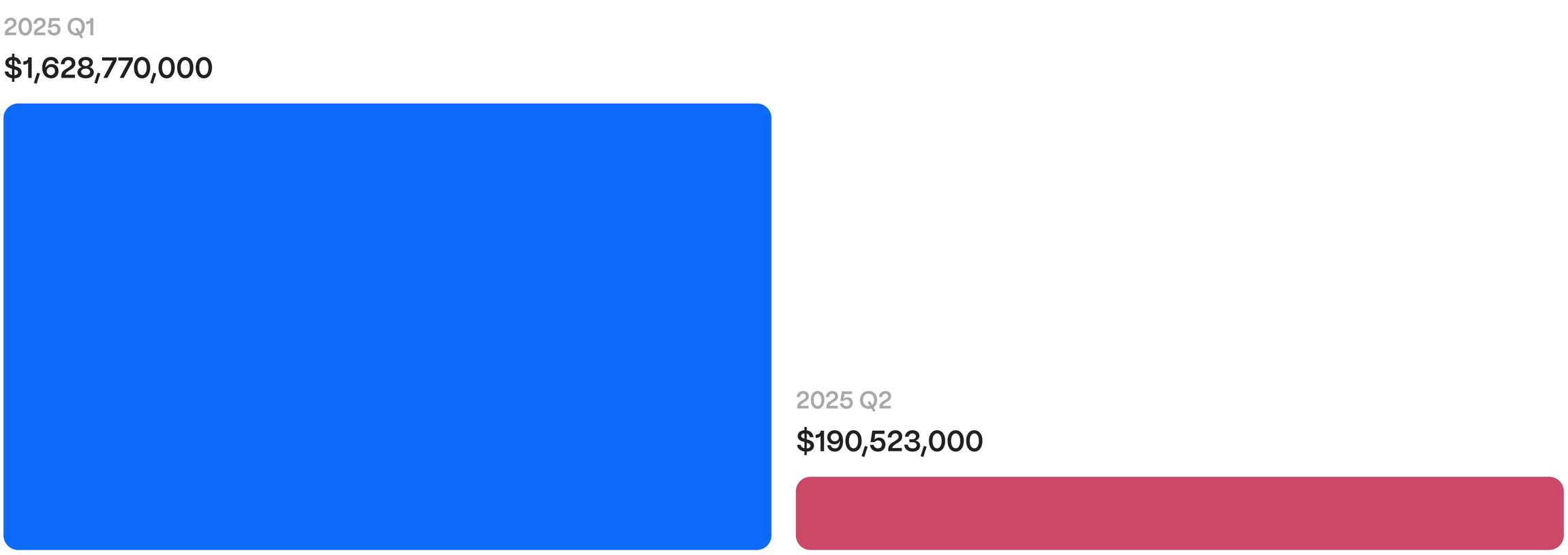
1

The Safe Multisig Monitor is purpose-built to track and validate transactions from Safe Multisig wallets, keeping a constant eye on key activities – retrieving signers, confirming signatures, and executing transactions. It verifies transaction hashes and signatures, flagging mismatches or anomalies with severity-based alerts.

2

Extractor's TVL Monitor watches for abnormal transfers, spotting irregular withdrawals or balance shifts that signal potential breaches.

Together, these detectors form a vigilant frontline, catching Access Control threats as they emerge. But Extractor goes further with automated prevention: it can limit or pause outflows, transfer ownership to a secure contract, initiate key rotation, remove compromised signers, or reassign proxy admin rights – all in real time.



Losses due to Access Control exploits in 2025

Implementation Challenges and the Path Forward

Six months into 2025, incidents involving compromised access controls continued to dominate Web3 security breaches, underscoring a critical point: attackers are no longer targeting only cryptographic primitives, but are increasingly exploiting human and process-level weaknesses to bypass technical safeguards. From blind signing attacks and private key leaks to sophisticated phishing campaigns, the landscape shows that access control in the crypto space remains one of the most underdeveloped and high-risk domains.

Case Landscape:
Business Impact of Access Failures

- **$330M Social Engineering Theft**
  An elderly U.S. victim was manipulated into transferring Bitcoin in one of the largest reported individual thefts. This reflects the emotional and trust-based manipulation used by attackers beyond pure technical exploits.

- **Trust Wallet Private Key Leak**
  A case of phishing and fake wallet app usage resulting in irreversible fund loss.

- **Coinbase Outsourcing Breach**
  A supply-chain access compromise led to data exposure potentially affecting millions.

- **Blind Signing Exploits**
  Users unknowingly authorize malicious transactions due to insufficient message transparency in wallet UIs.

- **North Korean Job Scams**
  Developer impersonation campaigns introducing malware and stealing credentials from target teams.

Collectively, these incidents highlight that half a billion dollars in crypto can be lost even when cryptography works perfectly. It is the human and procedural controls around access that are often weakest.

Dmytro Yasmanovych
Hacken Compliance Service Lead

linkedIn

"Your business goals matter. Our job is to help you reach them securely. Cybersecurity protects momentum. Using frameworks like CCSS & ISO/IEC 27001, along with structured team training, reduces risk and enables trust, scalability, and lasting customer confidence."

Strategic Gap: Where Access Control Breaks

The fragmented state of wallet and key access governance across the Web3 space often stems from:

- Lack of formal access control frameworks tailored for on-chain environments.
- Absence of third-party validation or auditing of wallet access processes.
- User-facing applications (wallets, DApps) lacking UX safeguards against social engineering and blind signing.
- Off-chain processes (e.g., HR onboarding/offboarding, vendor access, DevOps privileges) being ignored or inconsistently secured.

This is a systemic issue — not merely a user problem.

Hacken Recommends

Compliance For CASP/VASP Licensing: CCSS + ISO/IEC 27001

To address access control holistically, Hacken strongly recommends the implementation of:

1

Cryptocurrency Security Standard (CCSS)

to structure secure key generation, access segregation, and seed management across hot, warm, and cold wallets.

2

ISO/IEC 27001:2022

to operationalize governance and controls for off-chain access management, employee awareness, and incident handling.

Crypto exchanges, custodians, and infrastructure providers pursuing CASP/VASP licenses under MiCA, VARA, or Hong Kong SFC are increasingly required to demonstrate this dual-layered control.

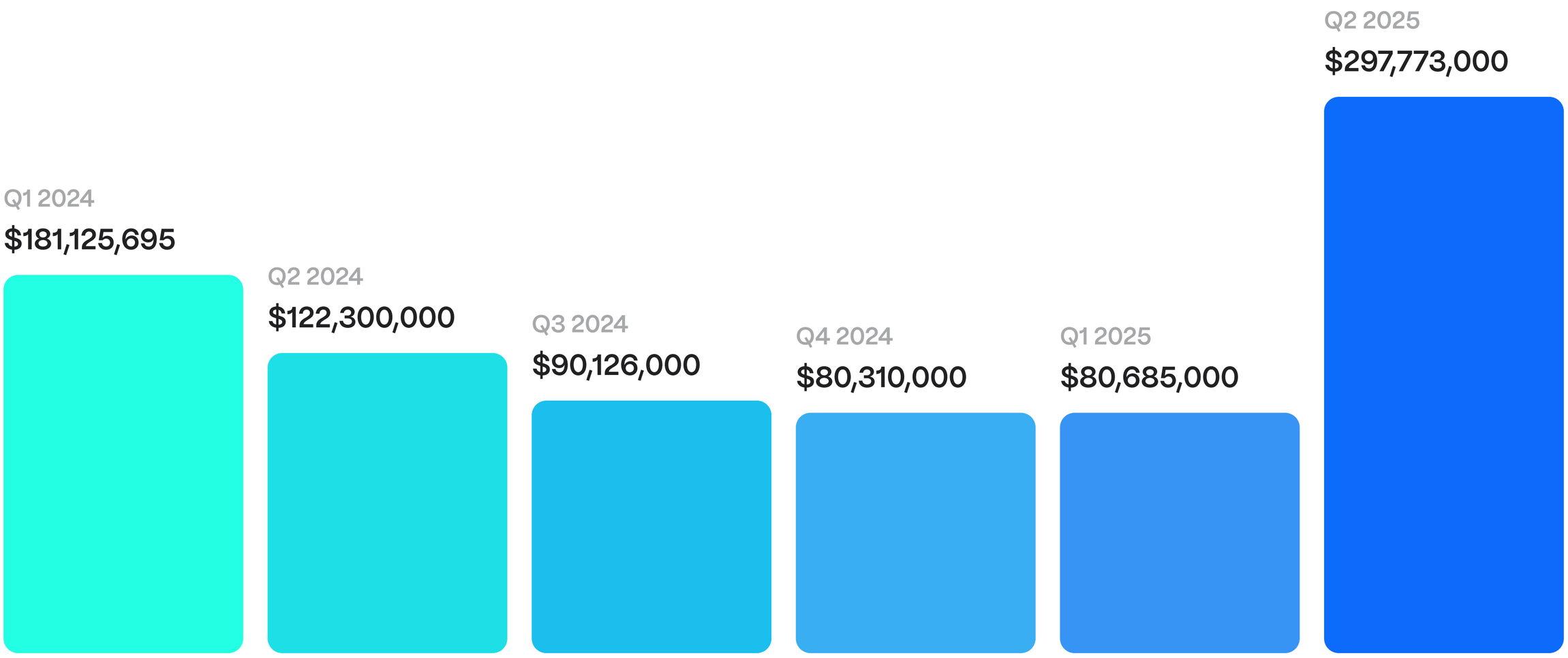
Hacken supports businesses in aligning with these and other regulatory standards to secure CASP/VASP licensing.

Learn More ↗

DeFi and Smart Contract Vulnerabilities

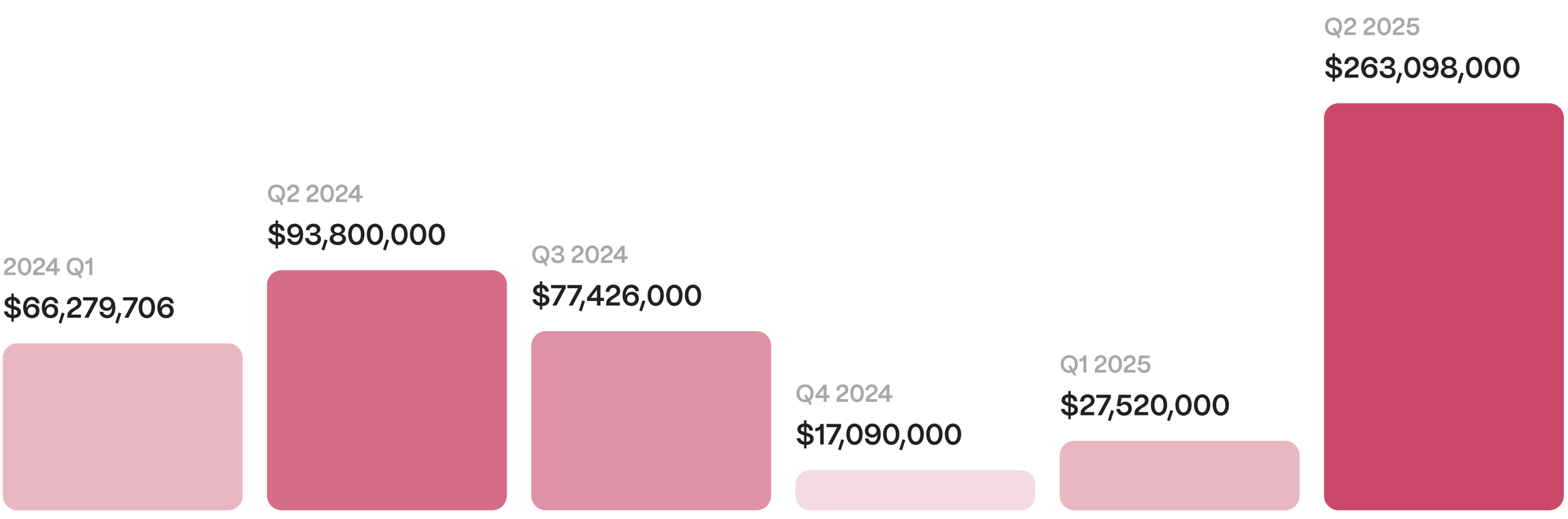
DeFi got hit with about 300m stolen – the worst quarter since 2023.

The standout was the Cetus hack in Q2, where $223 million was drained in just 15 minutes, making it DeFi's worst quarter since early 2023 and breaking a five-quarter downtrend in losses due to exploits. Earlier on, Q4 2024 and Q1 2025 were dominated by access-control failures, which drowned out most bug-based thefts. This quarter, however, access-control losses in DeFi fell to just $14 million (its lowest since Q2 2024's $28.5 million), while smart-contract exploits increased sharply.

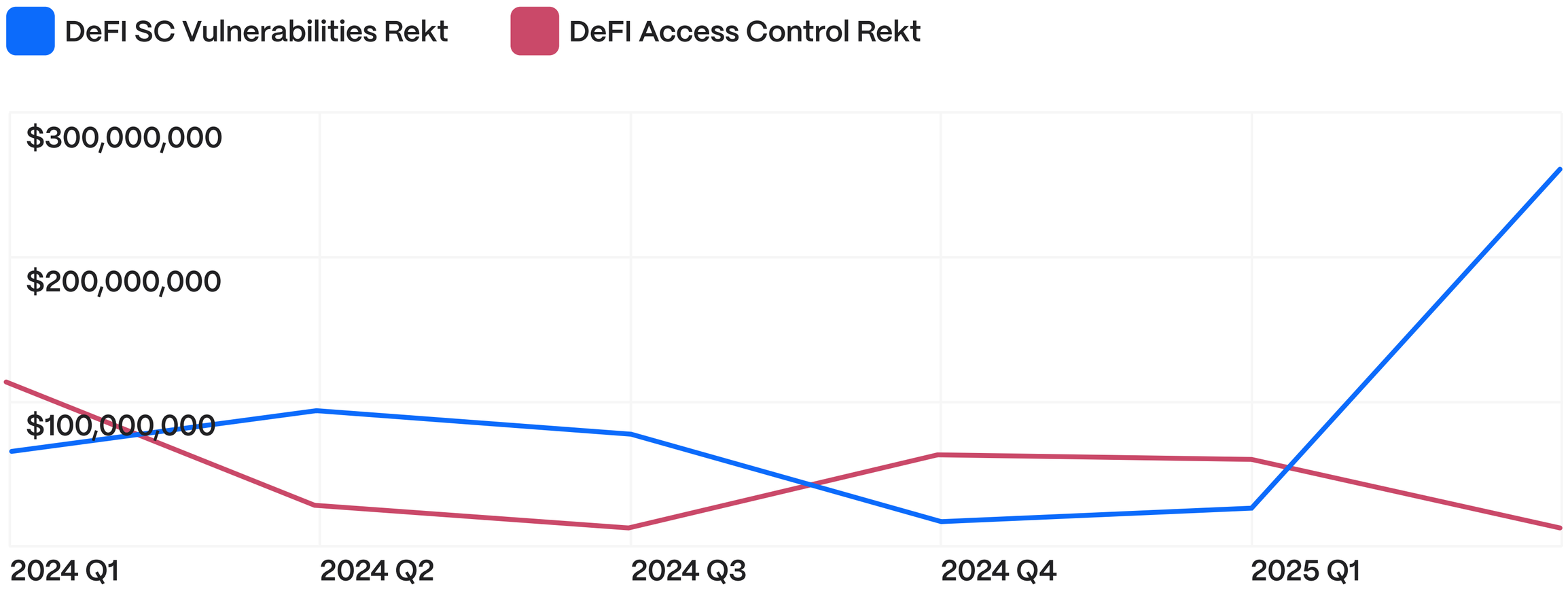


DeFi losses overall

Smart contract bugs accounted for $263M (8%) of all Web3 losses



DeFI SC Vulnerabilities Rekt



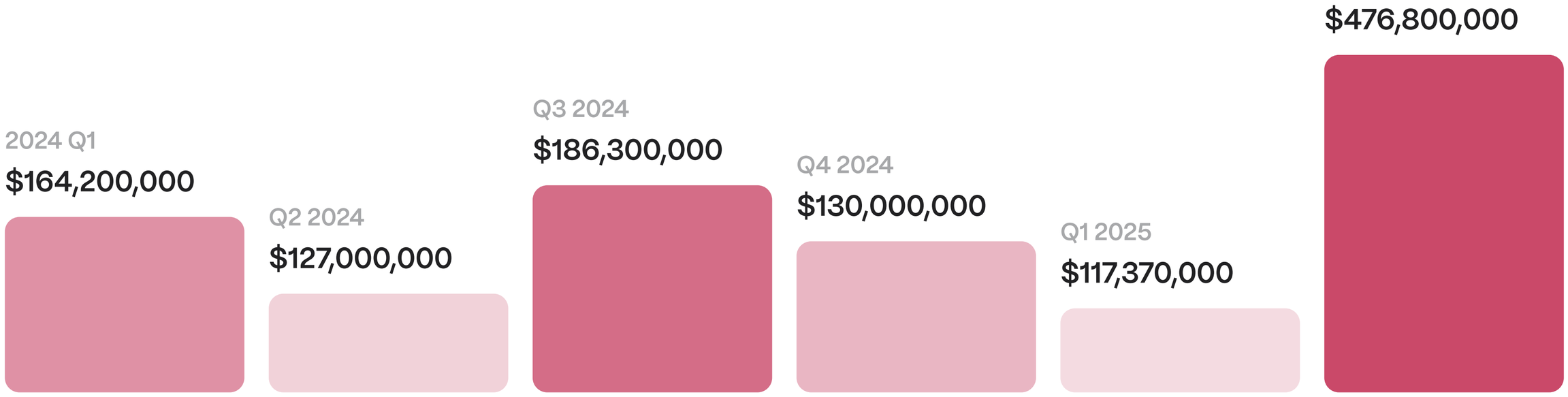
Cetus incident, by exploiting an overflow check in its liquidity calculation, the attacker took a flash loan, opened tiny-range positions (ticks 300 000–300 200), and then swept through 264 pools – starting with a $22 million haSUI pool and ending with a small $2 500 AXAI pool, draining $223 million. If there had been real-time TVL monitoring with auto-pause, up to 90 percent of those funds could have been saved.

Another major case was the Cork Protocol exploit, where attackers exploited the lack of permissions validation on who can call Uniswap's V4 beforeSwap hook. It was supposed to be called only by Uniswap's PoolManager, but the Cork team had modified default permissions. The attackers bought weETH8CT-2 tokens on the open market, then took advantage of a missing access check that let them inject custom data into CorkCall.

They split the token into fake_DS and fake_CT and then redeemed both for real RA tokens, draining 3 761 wstETH (around $12 million). In effect, the removed modifier turned a narrow hook into a free-for-all entry point.

Tremendous spike of losses due to Social Engineering

Phishing and social engineering made up about 20% of all Web3 losses in the first half of 2025, totaling roughly $600 million – already beating 2024's full-year losses.



The single biggest hit was a $330 million bitcoin theft from an elderly US holder, where complex social-engineering tactics convinced them to hand over wallet access. The attacker peeled the BTC through hundreds of wallets, mixed it into Monero (pushing its price up 50%), bridged some funds into Ethereum, and only a fraction of the stolen coins were ever frozen.

At the same time, high-net-worth Coinbase users have been hit by phishing, vishing and social-engineering since a data breach over long months. Callers posing as "Coinbase support" quoted real balances to gain trust and trick victims into revealing keys or passcodes, stealing over $100 million to then launder stolen money via mixers, OTC desks and DeFi.

Apart from this, unfortunately, as usual, people have fallen for fake wallet-permission requests, malicious token-approval prompts and wallet-draining scripts hidden in cloned dApps, browser extensions or GitHub/Bitbucket repos.

The advice for users to not become a victim of a phishing / social engineering attack:

- never pick up phone calls claiming to be support from your exchange
- avoid clicking links in branded SMS or chat messages
- open your exchange app or website directly to check alerts
- inspect email headers to confirm the sender's domain
- only accept help from people you already know and trust
- use an authenticator app or hardware key instead of SMS for 2FA
- store large balances in vaults or cold wallets, not in hot wallets
- keep your recovery phrases and keys out of plain files and folders

AI Security Highlights

1025% increase in AI-related exploits from 2023

98.9% of all AI-related exploits were tied to insecure APIs

5 major AI-related CVEs (Common Vulnerabilities and Exposures) added

34% of Web3 projects integrate AI agents in production

AI and LLM technologies are already woven into both Web2 and Web3 architectures, powering customer-facing chatbots, DeFi trading agents, code-review assistants, and more. This integration drives innovation but also expands the attack surface with new threat classes.

AI System Security Risks

- **Prompt Injection**

  Malicious inputs override LLM instructions, leading to data exfiltration or unauthorized transactions. OWASP lists this as the #1 LLM risk.

- **Training Data Poisoning**

  Subtle corruption of training data enables backdoors and model misclassifications.

- **Model Theft & Inference Attacks**

  Crafted queries can reconstruct proprietary model parameters, fueling intellectual property theft.

- **Supply Chain Compromises**

  Malicious or outdated dependencies in ML frameworks (e.g., BentoML, Langflow) open RCE vectors.

- **Agentic AI Exploits**

  Multi-agent coordination frameworks have been shown vulnerable to arbitrary code execution, even when individual agents resist direct prompt injection.

- **Model Hosting & Serialization Flaws**

  Insecure deserialization, improper sandboxing, and lack of input validation in inference servers remain rampant.

Notable AI-Related Incidents

- **Langflow RCE (CVE-2025-3248)**

  A critical, unauthenticated code injection flaw in Langflow's code-validation API (CVSS 9.8) saw active exploitation across ~1,050 exposed instances worldwide.

- **BentoML Deserialization (CVE-2025-32375)**

  Insecure deserialization in BentoML's runner allowed arbitrary code execution via crafted headers, patched in version 1.4.8.

- **Drupal AI Command Injection (CVE-2025-31692)**

  OS command injection in Drupal's AI module enabled unauthorized system commands on versions before 1.0.5.

- **MITRE Caldera RCE (CVE-2025-27364)**

  A zero-day in the adversary-emulation tool allowed remote code execution during agent compilation, underscoring the need to secure defensive platforms themselves.

- **Prompt Injection on Commercial LLMs**

  Researchers exploited hidden instructions to corrupt long-term memory in Google Gemini and other models, showing persistent manipulation risks.

- **"Vibe Hacking"**

  Jargon-free "vibe hacking" kits like WormGPT enable non-expert actors to generate sophisticated exploits, lowering the bar for large-scale malware campaigns.

New AI-Related CVEs

OWASP's GenAI Security Project was promoted to flagship status, publishing the Top 10 LLM Risks for 2025

CVE ID	Description	CVSS	Status
CVE-2025-3248	Langflow unauthenticated RCE	9.8	Patched
CVE-2025-32375	BentoML insecure deserialization → RCE	8.6	Patched
CVE-2025-31692	Drupal AI OS command injection	7.5	Patched
CVE-2025-27364	MITRE Caldera dynamic code generation RCE	10.0	Patched
CVE-2025-32756	Fortinet Admin API buffer overflow	9.0	Under Patch

Stephen Ajayi

DApp Audit Technical Lead, Hacken

linkedIn

"The promise of AI is massive, but so are the risks. By addressing AI-specific threats and embedding security throughout the AI lifecycle, businesses can innovate with confidence. Our AI System Security Audit helps teams build LLMs, agentic AI, and generative systems on strong security foundations from day one. "

Learn more

Key Mitigations for AI Risk

- **Adversarial Testing & Red Teaming**

  Employ OWASP GenAI Red Teaming guides to simulate prompt injections, data poisoning, and agentic exploit scenarios.

- **Pipeline Hardening**

  Sanitize inputs end-to-end, enforce sandboxing via WebAssembly or enclaves, and apply strict authentication on code-execution endpoints.

- **Supply Chain Hygiene**

  Pin and audit ML/LLM dependencies, maintain an SBOM, and integrate CISA KEV feeds for AI framework CVEs.

- **Context Protocols (MCP)**

  Adopt the Model Context Protocol to carry permissions, model version, and usage policies alongside each agentic AI call.

- **Runtime Monitoring & Explainability**

  Monitor model outputs and API patterns with AI-powered intermediaries; deploy anomaly detectors tuned for adversarial ML signatures.

- **Patch & Threat Intel**

  Prioritize high-severity AI CVEs, subscribe to MITRE ATLAS adversarial ML taxonomy, and leverage real-time intelligence from Recorded Future or Horizon3.

- **Training & Awareness**

  Conduct regular drills on AI-powered phishing, deepfake identification, and secure prompt practices to inoculate teams against emerging social-engineering tactics.

A New Era of AI Regulation

Traditional frameworks like ISO/IEC 27001, NIST CSF, and SOC 2 offer a strong foundation for general cybersecurity, but they were not designed to address AI-specific threats such as model hallucination, prompt injection, or adversarial data poisoning.

While they help establish baseline security hygiene (e.g., access controls, incident response), they must be augmented with AI-specific standards to achieve full-spectrum governance.

For example, ISO 27001 can ensure encrypted access to model files, but it won't require testing for biased model outputs. This is where emerging AI frameworks come in.

Key AI-focused regulations and frameworks now defining the compliance landscape include:

- **EU AI Act**

  A landmark risk-based regulation classifying AI systems and imposing transparency, data governance, risk assessments, and human oversight requirements for high-risk and foundation models. Companies targeting EU markets must prepare for **mandatory conformity assessments and CE marking** in the next 12–24 months.

- **NIST AI Risk Management Framework (AI RMF 1.0)**

  A lifecycle-based framework focused on trustworthy AI, emphasizing functions such as Govern, Map, Measure, and Manage. It helps organizations implement policies for risk-based AI governance and has quickly become a global reference point.

- **ISO/IEC 42001:2023**

  The first certifiable AI-specific management system standard. It mandates controls across the AI lifecycle (from design to decommissioning), ethical oversight, third-party vetting, and continuous improvement. Early adopters like Anthropic and Google DeepMind are already pursuing certification to demonstrate leadership.

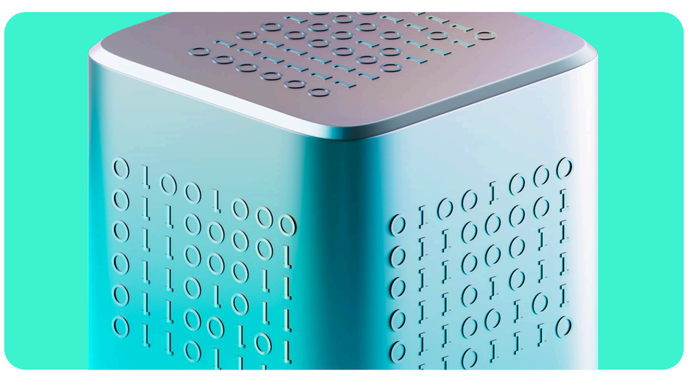
- **OECD AI Principles**

  Although non-binding, these form the ethical backbone for many regulatory efforts worldwide, emphasizing transparency, robustness, inclusivity, and accountability.

- **FINRA, FCA, and Sectoral Regulators**

  Financial, healthcare, and infrastructure regulators are now expecting AI-specific risk assessments, bias audits, and fraud prevention protocols attuned to generative AI threats.

Empowering Secure Digital Innovation for Web3 Businesses and Crypto Users



Discover Security Solutions

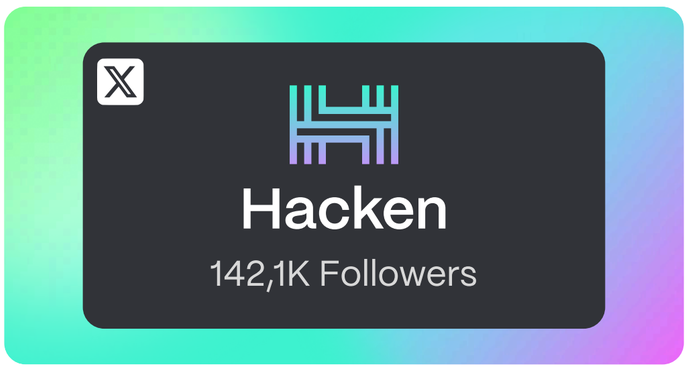
Your trusted blockchain security auditor. Learn how you can strengthen resilience, prevent exploits, and build trust with Hacken.

hacken.io

Access Educational Resources

Stay ahead of risks with Hacken's tools and resources—because knowledge is your first line of defense.

hacken.io/research



Support a Safer Web3

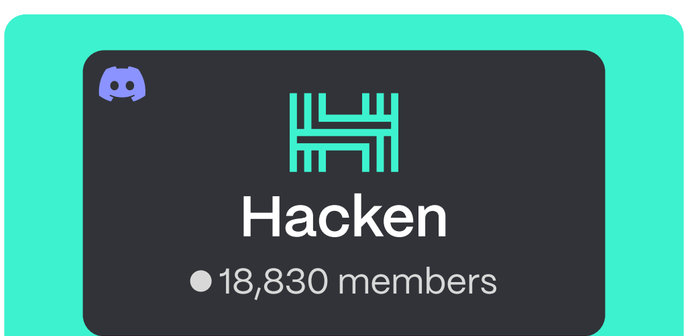
Join Hacken's security community. Stay updated, get involved, and advocate for blockchain security.

x.com/hackenclub

Subscribe to Hacken Digest

Get monthly Web3 security insights, exclusive webinars, and company updates — delivered straight to your email.

hacken.digest



Join HAI Discord Community

Master the art of DYOR and level up your crypto investment game with the strongest security-first community in Web3.

discord.gg/hacken

Making Web3 a safer place

About Hacken

Hacken is an end-to-end blockchain security & compliance partner for digital assets.

Our Story

Unlike traditional providers, Hacken was born on blockchain, combining deep Web3 expertise with enterprise-grade quality, AI-powered offensive security, and globally recognized certifications. Since 2017, Hacken has been trusted by 1,500 adopters to secure the new digital frontier.

Our Contribution

We bring top-tier, blockchain-native expertise and proven credibility to help organizations secure their infrastructure and meet modern digital asset regulations with confidence.

For media inquiries

marketing@hacken.io

Learn more

hacken.io X linkedIn

Authors: Rudytsia Y., Malanii O., Sheptytskyi A., Yasmanovych D., Ajayi, S.