A global leader in blockchain threat intelligence

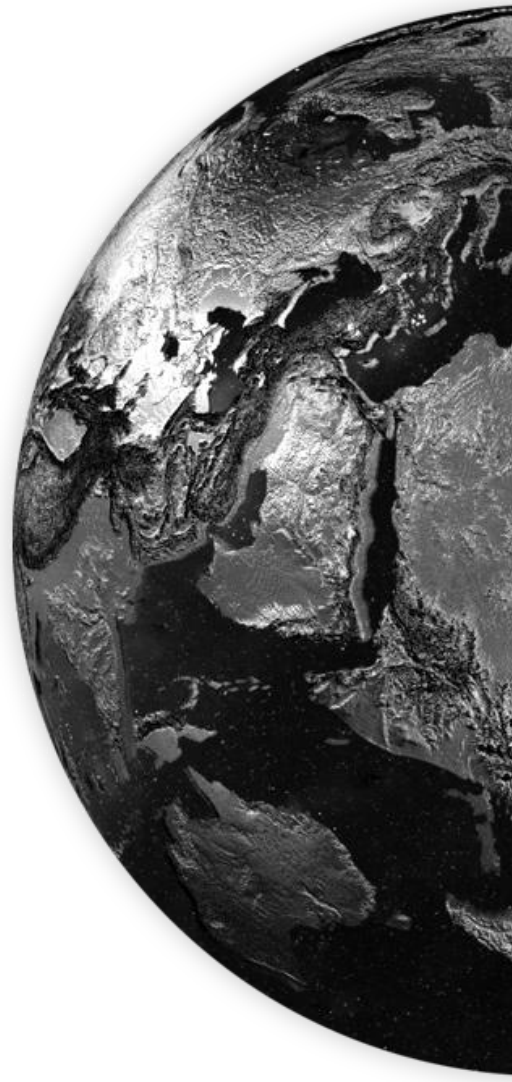
About SlowMist

SlowMist is a **threat intelligence** firm specializing in blockchain ecosystem security, established in January 2018. The firm was founded by a team with over ten years of network security experience. Our goal is to make the blockchain ecosystem as secure as possible for everyone. We are now a renowned international blockchain security firm that has worked on various well-known projects such as HashKey Exchange, OSL, MEEX, BGE, BTCBOX, Bitget, BHEX.SG, OKX, Binance, Amber Group, Crypto.com, etc.

SlowMist was awarded the “Cyber Security Excellence Contribution Award” at the Cyber Security Professionals Awards 2025, presented by the Hong Kong Police Force (CSTCB). In addition, our AML tracking and analytics platform MistTrack received the Gold Award in FinTech (RegTech: Regulatory and Risk Management) at the HKICT Awards 2025. **Our extensive work in cryptocurrency crime investigations has been cited by international organizations and government bodies, including the United Nations Security Council and the United Nations Office on Drugs and Crime.**

SlowMist's security solutions include services such as SlowMist AI, security auditing, Blockchain Threat Intelligence (BTI), and defense deployment, complemented by a suite of SaaS security products, including the cryptocurrency AML tracking and analytics platform (MistTrack), the AML compliance engine for large institutions (SlowMist KYT), fake deposit vulnerability scanning, Web3 threat intelligence and dynamic security monitoring (MistEye), and the hacked incident database (SlowMist Hacked). We have partnerships with leading domestic and international firms such as Akamai, Bitdefender, RC², TianJi Partners, IPIP, etc.

By delivering comprehensive security solutions customized for individual projects, we help identify and mitigate risks. Our team has discovered and disclosed several high-risk blockchain vulnerabilities, contributing to greater awareness and improved security standards across the blockchain ecosystem.



Services and Products

Blockchain Security Audit

Provide security services for CEX, DEX, DeFi, GameFi, NFT, Wallets, Blockchains

Red Teaming

Evaluate personal, organizational, supply chain, office, and physical security risks

Security Monitoring

MistEye, the meticulously developed system that provides comprehensive dynamic security monitoring services for Web3 projects

Blockchain AML

An AML/CFT compliance solution that employs on-chain analytics to trace illicit funds

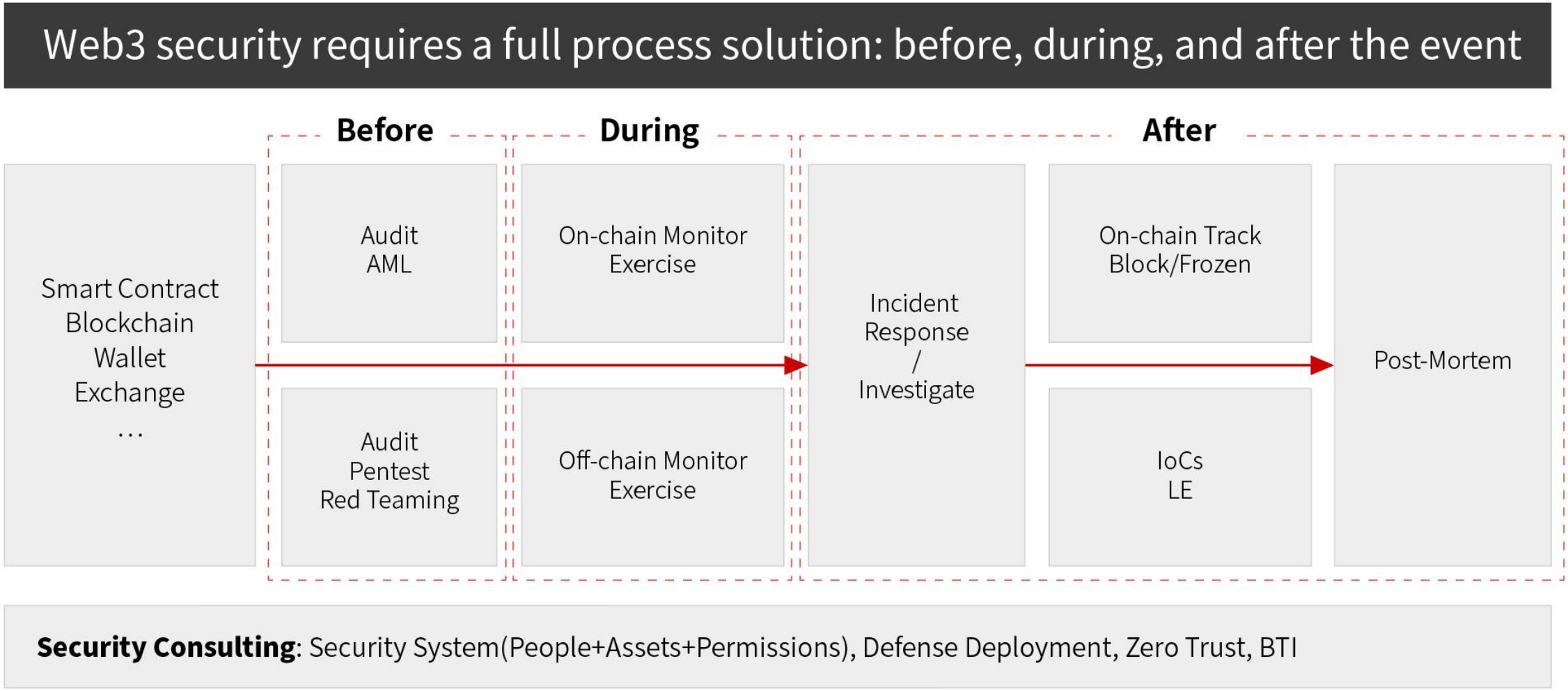
Incident Response Service

Designed to help Web3 projects respond quickly and effectively to security incidents and threats, while providing on-chain tracing services for stolen digital assets.

Security Consulting

Provide technical, risk management and emergency response support, along with recommendations for improvements

How SlowMist Delivers Full–Lifecycle Protection



Compliant Security Audit Services

With the new virtual asset policies, the blockchain sector embraces fresh opportunities, marking Web3 industry as the innovation frontier for entrepreneurs and builders. To safeguard user assets, rights, and market stability, compliance is an inevitable trend, with regulatory oversight on the cryptocurrency industry maturing. Since its establishment, SlowMist has been embracing compliance and regulation, offering compliance security audit services. SlowMist's security team continually translates frontline security capabilities into corresponding compliance check items, providing compliance security audit services for outstanding projects within the Web3 industry.

Customer Sample

HASHKEY HK EXCHANGE
OSL
MEEX
BGE
DFX
BTCBOX
Bitget
BHEX | SG
YAX
WhaleFin HK WhaleFin Markets Limited
RD Technologies

Compliant Security Audit Services

Adhering to compliance policies is crucial for project stakeholders from a policy perspective. It ensures that the platform complies with FinCEN, HKSFC and other regulatory regulations, reducing legal risks and fostering a positive reputation. Moreover, compliance policies safeguard user data privacy, uphold stringent security standards, mitigate various risks, and showcase social responsibility. Ultimately, they build trust, attract users, and fortify the project's integrity within the market.

- Demonstrating the Team’s Due Diligence
- Enhancing User Trust in the Project
- Better Protection of User Data
- Streamlining Processes and Improving Services
- Achieving Secure Internal Controls and Efficient Management

Compliant Security Audit Services

SlowMist has provided compliance security audit reports to numerous cryptocurrency trading platforms, earning regulatory approvals:

- In **2020**, a report for **BTCBOX** was submitted to **Japan's Financial Services Agency**, securing a license.
- In **2020**, a report for **Bitget** was acknowledged by the **U.S. FinCEN** during its licensing process.
- In **2021**, a report for **BHEXSG** was submitted to the **Monetary Authority of Singapore**, successfully obtaining a license.
- In **2023**, a report for **HashKey Exchange** was submitted to **HKSFC**, securing a license.
- We are serving more customers.

Customer Sample

HASHKEY HK EXCHANGE BTCBOX Bitget BHEX | SG

HKSFC Compliant Security Audit Services

SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

Following the HKSFC's latest requirements and the international OWASP standards, SlowMist has organized a checklist for HKSFC-compliant security audits. By deeply analyzing HKSFC's circulars and guidelines and leveraging years of blockchain security experience, SlowMist has developed a HKSFC-compliant security audit framework, also aligning with OWASP international standards for Web, iOS, and Android, ensuring project compliance with HKSFC while adapting to OWASP standards, encompassing:

- HKSFC’s 23 Compliance Requirements
- OWASP Web’s 13 Compliance Requirements
- OWASP Android’s 7 Compliance Requirements
- OWASP iOS’s 7 Compliance Requirements
- Over 170 security audit items compiled by SlowMist

Customer Sample

HASHKEY HK EXCHANGE　OSL　MEEX　BGE　YAX　WhaleFin HK WhaleFin Markets Limited

Blockchain AML Solution

SLOWMIST AML https://aml.slowmist.com

Industries Served

SlowMist has served thousands of clients, spread across more than a dozen major countries and regions. We have successfully intercepted more than a billion dollars in funds in terms of AML and have actively participated in promoting the safety standards for blockchain at the local, national, and international levels.

Web3 Industry

Promoting industry compliance, helping to establish trust, and protecting businesses from the harm of financial crimes.

Financial institutions

Helping traditional financial institutions improve their anti-money laundering capabilities in the direction of cryptocurrencies.

Regulatory units

Assisting in the formulation of industry standards, establishing secure markets and maintaining financial stability.

Compliance departments

Helping to discover, analyze blockchain financial risks and prevent cryptocurrency-related crimes.

Blockchain AML Solution

SLOWMIST AML https://aml.slowmist.com

SlowMist has been deeply involved in cryptocurrency anti-money laundering for many years, and has a complete and effective set of solutions in compliance, investigation, audit, etc.

Compliance

- Meeting regulatory requirements
- Address risk identification
- Threat intelligence network
- Build an anti-money laundering alliance

Investigation

- Emergency response
- Hacker profile
- Intercept stolen funds
- Recovering stolen funds

Audit

- HKSFC's 23 Compliance Requirements
- OWASP's 27 Compliance Requirements
- Over 170 security audit items compiled by SlowMist

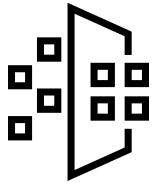
Products and Services

- MistTrack KYT
- MistTrack Investigation
- Malicious Address Library
- Case Evaluation
- Case Tracking
- Case Report

Blockchain AML Solution

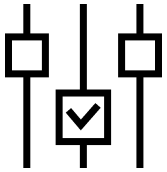
SLOWMIST KYT https://kyt.slowmist.com

A professional, real-time AML engine designed for institutional compliance teams, focused on deep risk fund screening and flexible risk configuration



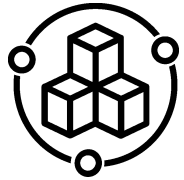
Penetrative Deep Screening

Supports 10-layer fund link analysis, precisely penetrating complex transaction networks to identify hidden risks.



Flexible Configuration & Automated Risk Control Loop

Customizable risk screening rules tailored to various business scenarios. Real-time automated work tickets are triggered upon risk detection, significantly reducing manual screening costs.



Enterprise–grade Internal Control & Integration

Supports granular Role-Based Access Control (RBAC) and high-performance API integration, meeting the high standards of institutional compliance teams for security, stability, and scalability.

Blockchain AML Solution

MISTTRACK BY SLOWMIST

https://misttrack.io

On 21 November 2025, at the Hong Kong ICT Awards 2025, SlowMist's crypto AML tracing platform MistTrack won the Gold Award in FinTech (RegTech: Regulatory and Risk Management)!

HONG KONG ICT AWARDS 2025 香港資訊及通訊科技獎

中华人民共和国香港特别行政区政府 数字政策办公室

10K +
Known Entities

500K +
Threat Intelligence Addresses

400M +
Labeled Wallet Addresses

90M +
Risky Addresses

AML Screening

Real-time detection of wallet address risk levels, identifying sanctioned and blacklisted addresses to ensure transaction safety.

- Real-time Risk Assessment
- Sanction List Screening
- Blacklist Identification
- Risk Level Classification

Transaction Monitoring

24/7 continuous monitoring of transaction activity, automatically identifying suspicious patterns and detecting potential money-laundering behavior.

- 24/7 Real-time Monitoring
- Suspicious Pattern Recognition
- Automated Alert System
- Transaction Path Analysis

Crypto Tracing & Investigation

In-depth tracking of fund flows and reconstruction of complete transaction chains, providing detailed evidence for compliance investigations.

- Fund Flow Tracing
- Transaction Chain Analysis
- Evidence Collection & Organization
- Investigation Report Generation

Blockchain AML Solution

Malicious Address Library

https://aml.slowmist.com/malicious-address-library.html

The SlowMist threat intelligence engine utilizes a comprehensive approach to data collection, combining data cleaning and integration with advanced artificial intelligence technology to extract precise data from vast datasets. This engine covers relevant content from various sources, including the dark web and hundreds of exchanges worldwide, and it tracks over 100,000 malicious wallet addresses for popular cryptocurrencies such as BTC, ETH, EOS, XRP, TRX, and USDT.

Benefit

Exchange

Mitigate money laundering and policy risks with ease

Wallet

Assist users in preventing fraud and safeguarding digital assets

Asset Management Platform

Verify assets sources, prevent disputes, and protect the platform's reputation

MistEye Security Monitor

https://misteye.io

MistEye's security monitoring is dedicated to serving Web3 security consultation clients. By conducting real-time surveillance of specific domains, smart contracts, and wallet addresses, it preemptively uncovers potential risks for projects and aids in promptly mitigating these risks.

MistEye is equipped to support the following types of security monitoring:

- On-chain: Monitoring for abnormal transactions.
- On-chain: Oversight of wallet/contract assets.
- On-chain: Scrutiny of smart contracts.
- Off-chain: Ensuring Web3 component security through timely updates.
- Off-chain: Monitoring of front-end code.
- Off-chain: Surveillance of domain information.
- Off-chain: Alerting on new component vulnerabilities, PoCs, and APT intelligence.

SlowMist AI

SLOWMIST AI

Security for AI & Crypto · AI for Security
https://slowmist.ai

Security for AI & Crypto

AI agents face supply chain poisoning (malicious Skills/MCPs), prompt injection, and privilege escalation; crypto protocols face contract exploits and on-chain asset fraud. With ADSS (AI Development Security Solution) as the governance foundation, MistEye as the threat-perception retina, MistTrack as the on-chain risk-control immune system, and MistAgent as the deep-analysis brain, we build a five-layer progressive digital fortress securing the full Agent lifecycle.

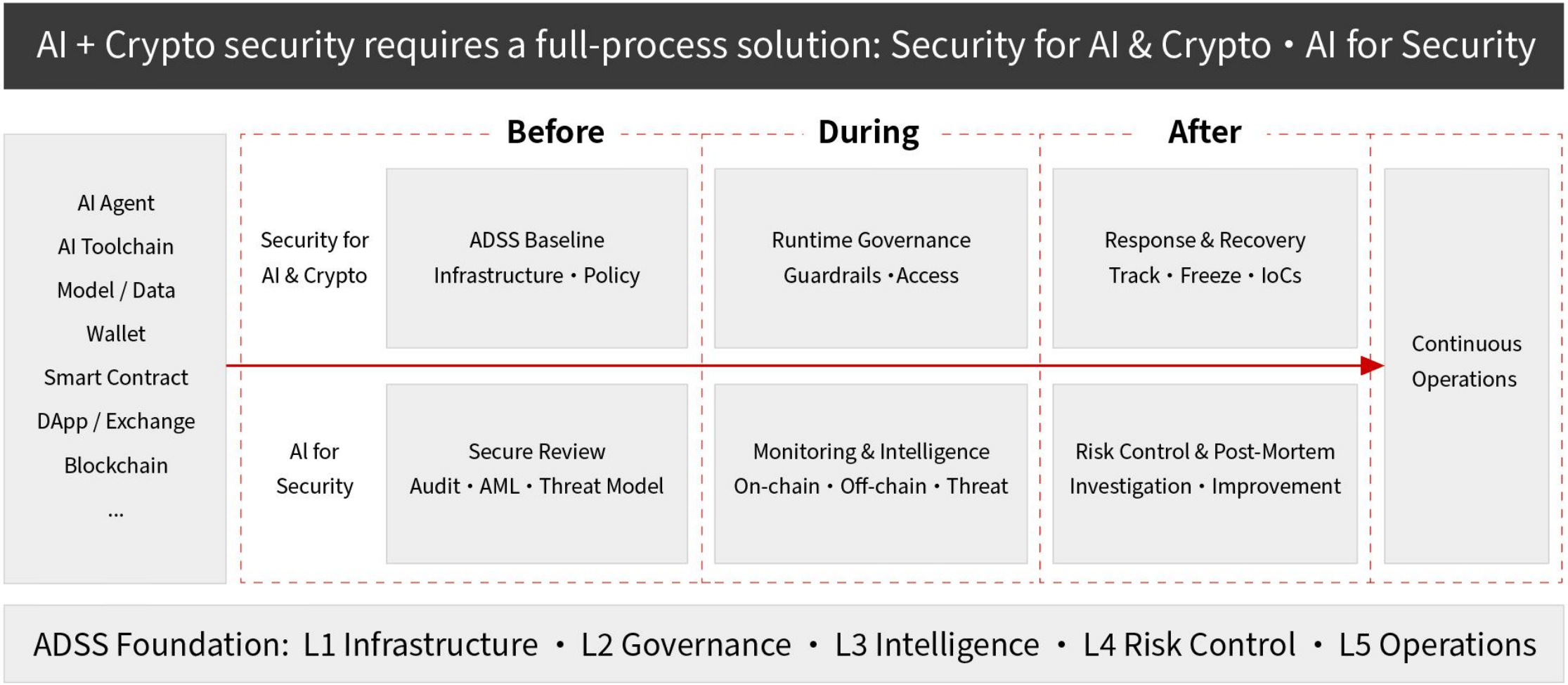
- **AI Agent Security Solution**
- **MCP Security Checklist**
- **Smart Contract Auditing**
- **On-chain Threat Monitoring**

AI for Security

We harness AI to transform security — MistAgent runs 20+ LLMs in parallel with RAG-enhanced detection across thousands of historical audit reports, MistEye delivers 24/7 AI-driven IOC correlation and threat intelligence, and MistTrack traces funds across 19 chains against 400M+ labeled addresses for intelligent AML compliance. All three inject into Agent workflows as Skills for scalable, intelligent defense.

- **Multi-LLM Auditing Engine**
- **AI-Powered Threat Intelligence**
- **Intelligent Fund Tracing**
- **Automated Compliance (AML)**

AI + Crypto Security in Practice

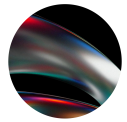


Open Source / Public Report

Web3 Project Security Handbook
https://www.slowmist.com/redhandbook/

Crypto Asset Tracing Handbook
https://github.com/slowmist/Crypto-Asset-Tracing-Handbook

Blockchain Dark Forest Selfguard Handbook
https://darkhandbook.io



SlowMist Blockchain Security and AML Annual Report
https://www.slowmist.com/report/

HackingTime
https://ht.slowmist.io/

SlowMist Knowledge Base
https://github.com/slowmist/Knowledge-Base

Technical Research Report on AML and Compliance Pathways for Stablecoins
https://www.slowmist.com/report/SlowMist-2025-Stablecoin-AML-Compliance-Tech-Report-CN.pdf

Open Source / Public Report (AI)

1、SlowMist Agent Security Skill
https://github.com/slowmist/slowmist-agent-security

2、Misteye Security Check
https://github.com/slowmist/MistEye-Skills

3、MistEye DepScan
https://github.com/slowmist/MistEye-DepScan

4、MistTrack Skills
https://github.com/slowmist/misttrack-skills

5、OpenClaw Security Practice Guide
https://github.com/slowmist/openclaw-security-practice-guide

6、MCP Security Checklist: A Security Guide for the AI Tool Ecosystem
https://github.com/slowmist/MCP-Security-Checklist

7、MasterMCP
https://github.com/slowmist/MasterMCP

Vulnerabilities Discovered by SlowMist

Our team members were able to discover a number of zero-day exploits in the blockchain ecosystem

2026-07-18: xAI Grok-Build-CLI RCE via folder-trust bypass

2026-07-18: Sui False Top-up Vulnerability

2026-07-16: xAI Grok-Build-CLI RCE via cargo check

2026-07-16: xAI Grok-Build-CLI & Claude Code CLI RCE via bypassPermissions

2026-07-07: EVM Callcode False Top-up Vulnerability

2026-07-07: Dogecoin Timelock False Top-up Vulnerability

2025-03-17: Avalanche False Top-up Vulnerability

2025-01-11: Web3 Wallet eth_sign Detection Bypass Vulnerability

2024-07-31: TonConnect SDK Origin Forgery Vulnerability

2024-03-19: Web3 Wallet Privacy-Violating Vulnerability

2023-09-21: Web3 Wallet Origin Spoofing Vulnerability

2023-09-19: Web3 Wallet URL-Open-RCE Vulnerability

2023-07-09: WalletConnect web3modal Origin Forgery Vulnerability

2023-07-09: MetaMask SDK Origin Forgery Vulnerability

2022-04-08: Blockbook False Top-up Vulnerability

2022-04-07: UTXO False Top-up Vulnerability (Affected tokens: BTC/LTC/DOGE/BCH/BSV/BHD/CPU/DFI/BTCV/BXC/ZCL)

2021-11-26: TRON Token False Top-up Vulnerability

2021-08-26: Solana False Top-up Vulnerability

2021-04-19: NEM False Top-up Vulnerability

2020-11-14: Filecoin False Top-up Vulnerability

2020-07-07: BTC RBF False Top-up Vulnerability

2020-05-22: ETH False Top-up Vulnerability

2019-08-13: Monero (XMR) Locked Transfer Attack

2019-04-18: New Kind of Public Chain Attack: Alien Attack

2019-03-11: EOS DApp False Top-up Vulnerability

2019-02-25: IOST False Top-up Vulnerability

2018-12-28: XRP False Top-up Vulnerability

2018-10-15: EOS DApp Deposit "False Notification" Vulnerability

2018-09-18: TradingView XSS 0day Vulnerability

2018-07-09: Ethereum Token False Top-up Vulnerability

2018-06-28: USDT False Top-up Vulnerability

2018-05-28: EOSIO P2P DOS Vulnerability

2018-03-20: Billions of Tokens Theft Case cause by ETH Ecological Defects

Our Professional Certifications

Recovering

In June 2021, we successfully aided Poly Network in recovering over $610 million worth of cryptocurrencies

More recovering is happening:

SlowMist Security Team has helped multiple projects recover losses, including: Lendf.me, Socket Protocol, Hope Lend Protocol, and others.

cna

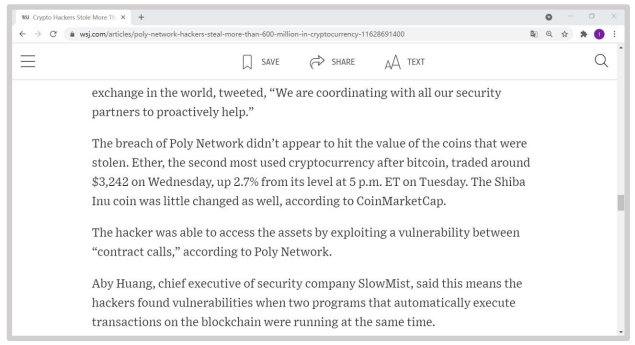
THE WALL STREET JOURNAL.

REUTERS®

THE BLOCK

Forbes

Bloomberg

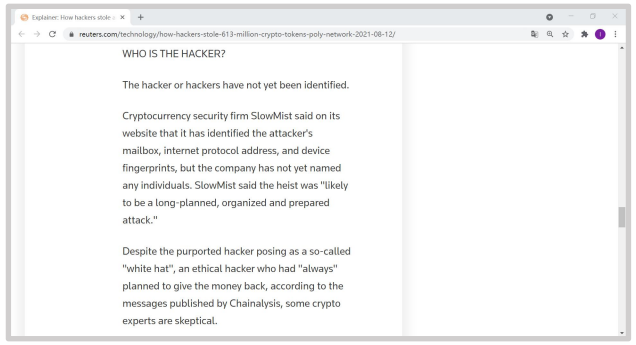


exchange in the world, tweeted, "We are coordinating with all our security partners to proactively help."

The breach of Poly Network didn't appear to hit the value of the coins that were stolen. Ether, the second most used cryptocurrency after bitcoin, traded around $3,242 on Wednesday, up 2.7% from its level at 5 p.m. ET on Tuesday. The Shiba Inu coin was little changed as well, according to CoinMarketCap.

The hacker was able to access the assets by exploiting a vulnerability between "contract calls," according to Poly Network.

Aby Huang, chief executive of security company SlowMist, said this means the hackers found vulnerabilities when two programs that automatically execute transactions on the blockchain were running at the same time.

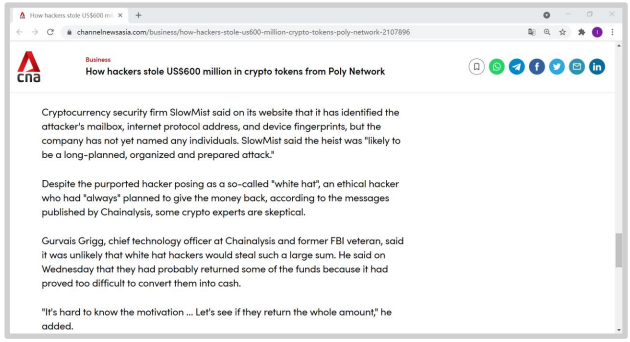


WHO IS THE HACKER?

The hacker or hackers have not yet been identified.

Cryptocurrency security firm SlowMist said on its website that it has identified the attacker's mailbox, internet protocol address, and device fingerprints, but the company has not yet named any individuals. SlowMist said the heist was "likely to be a long-planned, organized and prepared attack."

Despite the purported hacker posing as a so-called "white hat", an ethical hacker who had "always" planned to give the money back, according to the messages published by Chainalysis, some crypto experts are skeptical.



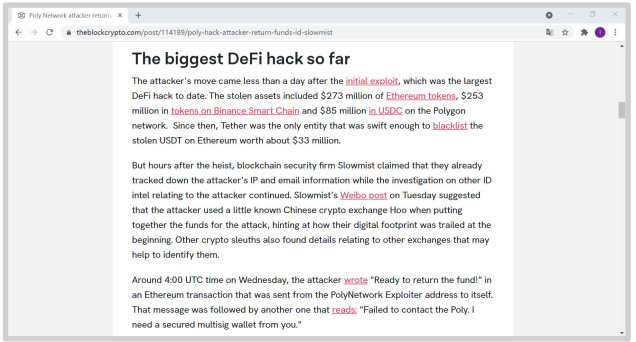
How hackers stole US$600 million in crypto tokens from Poly Network

Cryptocurrency security firm SlowMist said on its website that it has identified the attacker's mailbox, internet protocol address, and device fingerprints, but the company has not yet named any individuals. SlowMist said the heist was "likely to be a long-planned, organized and prepared attack."

Despite the purported hacker posing as a so-called "white hat", an ethical hacker who had "always" planned to give the money back, according to the messages published by Chainalysis, some crypto experts are skeptical.

Gurvais Grigg, chief technology officer at Chainalysis and former FBI veteran, said it was unlikely that white hat hackers would steal such a large sum. He said on Wednesday that they had probably returned some of the funds because it had proved too difficult to convert them into cash.

"It's hard to know the motivation ... Let's see if they return the whole amount," he added.

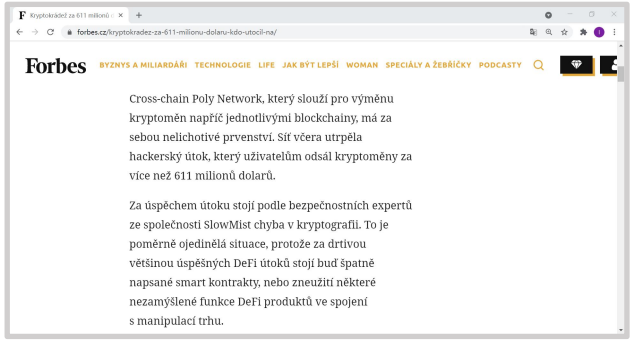


The biggest DeFi hack so far

The attacker's move came less than a day after the initial exploit, which was the largest DeFi hack to date. The stolen assets included $273 million of Ethereum tokens, $253 million in tokens on Binance Smart Chain and $85 million in USDC on the Polygon network. Since then, Tether was the only entity that was swift enough to blacklist the stolen USDT on Ethereum worth about $33 million.

But hours after the heist, blockchain security firm Slowmist claimed that they already tracked down the attacker's IP and email information while the investigation on other ID intel relating to the attacker continued. Slowmist's Weibo post on Tuesday suggested that the attacker used a little known Chinese crypto exchange Hoo when putting together the funds for the attack, hinting at how their digital footprint was trailed at the beginning. Other crypto sleuths also found details relating to other exchanges that may help to identify them.

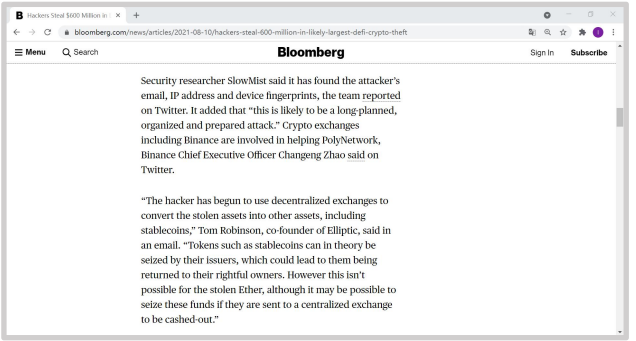
Around 4:00 UTC time on Wednesday, the attacker wrote "Ready to return the fund!" in an Ethereum transaction that was sent from the PolyNetwork Exploiter address to itself. That message was followed by another one that reads: "Failed to contact the Poly. I need a secured multisig wallet from you."



Forbes

Cross-chain Poly Network, který slouží pro výměnu kryptoměn napříč jednotlivými blockchainy, má za sebou nelichotivé prvenství. Síť včera utrpěla hackerský útok, který uživatelům odsál kryptoměny za více než 611 milionů dolarů.

Za úspěchem útoku stojí podle bezpečnostních expertů ze společnosti SlowMist chyba v kryptografii. To je poměrně ojedinělá situace, protože za drtivou většinou úspěšných DeFi útoků stojí buď špatně napsané smart kontrakty, nebo zneužití některé nezamýšlené funkce DeFi produktů ve spojení s manipulací trhu.



Bloomberg

Security researcher SlowMist said it has found the attacker's email, IP address and device fingerprints, the team reported on Twitter. It added that "this is likely to be a long-planned, organized and prepared attack." Crypto exchanges including Binance are involved in helping PolyNetwork, Binance Chief Executive Officer Changeng Zhao said on Twitter.

"The hacker has begun to use decentralized exchanges to convert the stolen assets into other assets, including stablecoins," Tom Robinson, co-founder of Elliptic, said in an email. "Tokens such as stablecoins can in theory be seized by their issuers, which could lead to them being returned to their rightful owners. However this isn't possible for the stolen Ether, although it may be possible to seize these funds if they are sent to a centralized exchange to be cashed-out."

Acknowledged / Cited

SlowMist's related security research has been cited or acknowledged by the United Nations, the U.S. Department of the Treasury, the U.S. Securities and Exchange Commission, NCDIT, etc.

United Nations

https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

https://documents.un.org/doc/undoc/gen/n24/032/68/pdf/n2403268.pdf

https://home.treasury.gov/system/files/136/Illicit-Finance-Risk-Assessment-of-Non-Fungible-Tokens.pdf

https://www.sec.gov/Archives/edgar/data/1823144/000110465921147443/tm2134804d1_ex99-1.htm

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

https://it.nc.gov/documents/cybersecurity-newsletters/2023/esrmo-newsletter-december-2023/download

Honors

Recent Honors and Recognitions of the SlowMist Team (See more at https://www.slowmist.com/honor.html)

2026-07-01: With the support of the InMist Lab Threat Intelligence Network, SlowMist helped clients, partners, and victims of publicly disclosed hacks freeze or recover approximately $5.16 million in stolen assets during the first half of 2026.

2026-06-29: SlowMist's MistTrack - Cryptocurrency Tracking and Anti-Illicit Finance Platform & Solution Suite received the Best FinTech Innovation Award at the HKMA/HKT Global Innovation Awards 2025/26.

2026-06-16: SlowMist received the Blockchain Security Champion Award in the Top 100 New-Quality Digital Security Specialists.

2026-04-21: The SlowMist Security Team was interviewed by Techub News to share insights on the Kelp DAO rsETH x LayerZero incident.

2026-03-30: The founder of SlowMist was interviewed by Odaily.

2026-03-27: The founder of SlowMist delivered a keynote titled "Security Challenges and Defensive Innovations in the AI and Crypto Ecosystem" at the 1st Agentic AI Innovation & Security Forum.

2026-03-11: SlowMist founder Cos was interviewed by Tencent News on the topic of AI Agents.

2026-01-30: SlowMist Limited Partner & CISO was awarded the Merit Award in the Cyber Security Audit & Consulting Sector at the Cyber Security Professional Awards 2025 (CSPA 2025).

2026-01-30: SlowMist Limited was honored with the Cyber Security Excellence Contribution Award at the Cyber Security Professional Awards 2025 (CSPA 2025).

2025-12-30: With substantial support from partners in the InMist Intelligence Network, SlowMist successfully assisted clients, partners, and publicly hacked entities in freezing approximately $19.29 million in funds in 2025.

2025-11-21: MistTrack was awarded the Gold Award in FinTech at the HKICT Awards 2025.

Partners and Clients

Official Website
https://slowmist.com

Email
team@slowmist.com

X (Twitter)
@SlowMist_Team

GitHub
https://github.com/slowmist

Medium
https://slowmist.medium.com