SLOWMIST SLOWMIST AML MISTTRACK MISTEYE

Cyber Tempest: Rebuilding the Firewall in 180 Days

“在黑客风暴中心，唯有极速成长，方能抵御破坏。”

23pds@SlowMist.com

About Me

23pds@SlowMist

Partner & CISO of SlowMist
Veteran Security Researcher
Wall of Fame: Apple、Microsoft、 OpenSea、
Yubico、Axie、Auth0、Cloudflare、Grab.. etc

@im23pds

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. Customers served: 90 + ; Cumulative recovered assets: $1,000,000,000 +

Security Consulting

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

Incident Response Service

Aiming to help Web3 projects quickly and effectively respond to security incidents and threats

SLOWMIST

1. Real-World Web2 Attack Cases in the Web3 Industry

2. The Current State of Offense and Defense from a Red Teamer's Perspective

3. Full-Lifecycle Protection Solutions for Web3

SLOWMIST

1 Real-World Web2 Attack Cases in the Web3 Industry

2 The Current State of Offense and Defense from a Red Teamer's Perspective

3 Full-Lifecycle Protection Solutions for Web3

Real- World Web2 Attack Cases in the Web3 Industry

Common Focus:

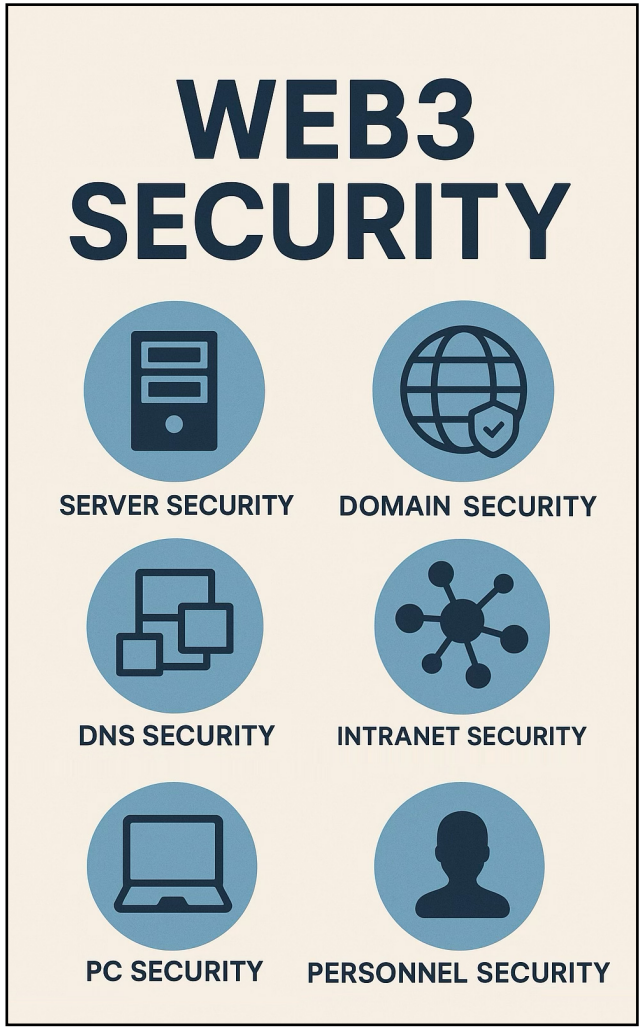
Web3 security discussions often center on smart contracts and blockchain vulnerabilities.

Broader Landscape:

Web2 elements also play a crucial role and are frequently targeted by attackers.

Web2 Attack Vectors in Web3 Industry

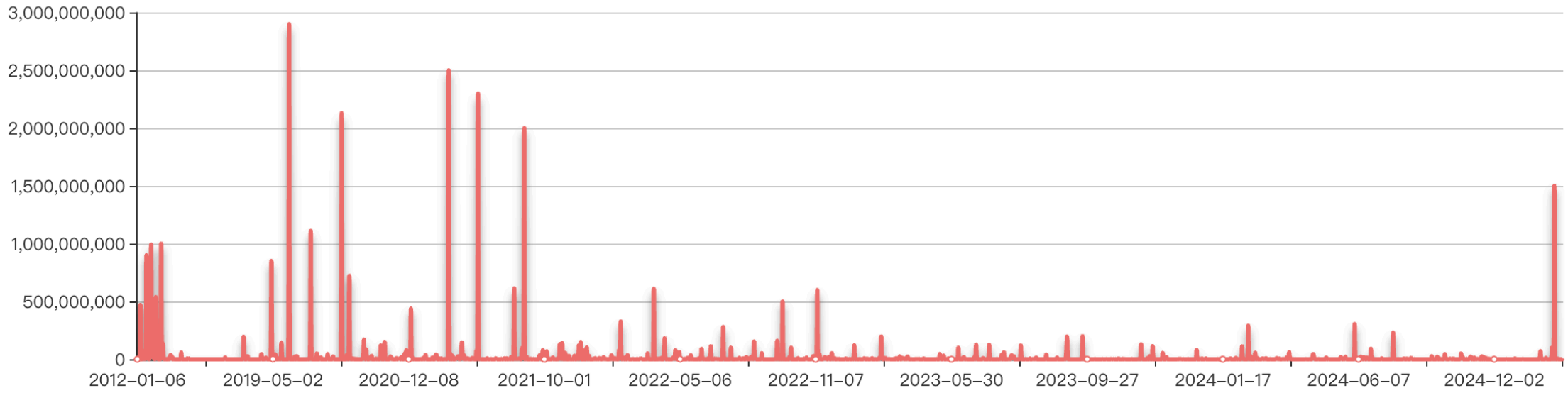
- Targeting user credentials through fake websites, emails or malicious programs.
- Manipulating insiders or users to gain access to sensitive information.
- Exploiting weaknesses in Web2 components like APIs, databases, and user interfaces.
- Attacks on servers, hosting providers, and DNS to disrupt services or hijack transactions.
- Stealing cryptocurrency private keys or seed phrases.
- Deceiving users into providing signature authorizations, and more.



Overview of Industry Losses

Total hack event(s) 1850 ;

The total amount of money lost by blockchain hackers is about $ 35,240,507,673.24 ;

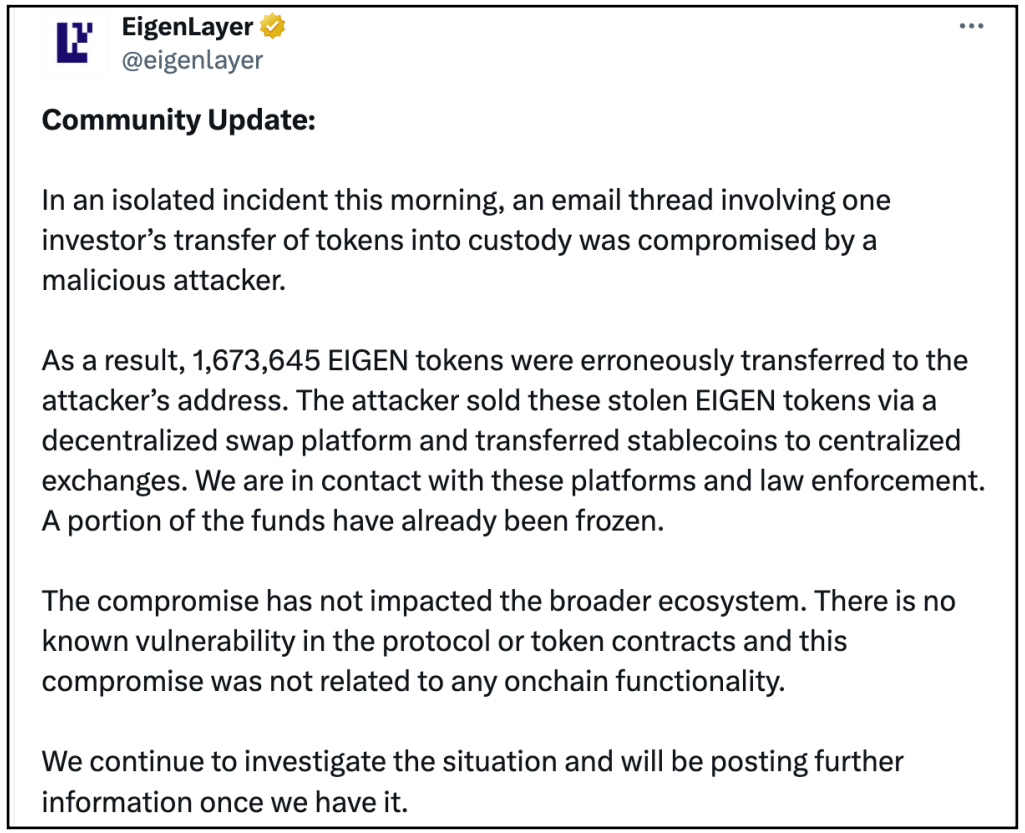


https://hacked.slowmist.io

APT Case Study: Real-World Incident (01)

Incident Overview

Loss Details: Senior executives and institutions within the company were targeted in a phishing attack, resulting in a loss exceeding **1.6 million Eigens tokens**.



EigenLayer
@eigenlayer

Community Update:

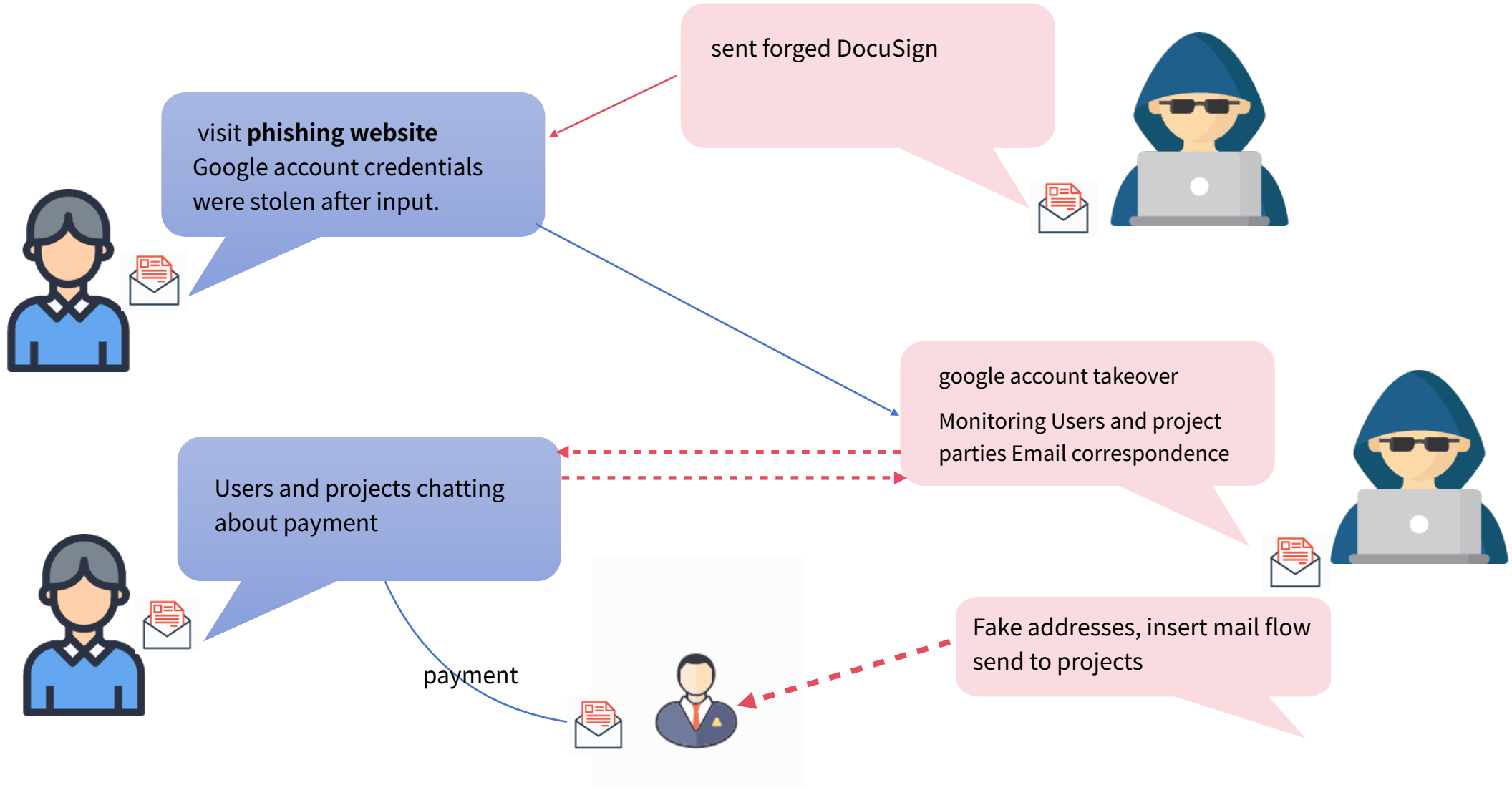
In an isolated incident this morning, an email thread involving one investor's transfer of tokens into custody was compromised by a malicious attacker.

As a result, 1,673,645 EIGEN tokens were erroneously transferred to the attacker's address. The attacker sold these stolen EIGEN tokens via a decentralized swap platform and transferred stablecoins to centralized exchanges. We are in contact with these platforms and law enforcement. A portion of the funds have already been frozen.

The compromise has not impacted the broader ecosystem. There is no known vulnerability in the protocol or token contracts and this compromise was not related to any onchain functionality.

We continue to investigate the situation and will be posting further information once we have it.

APT Case Study: Real-World Incident (01)



APT Case Study: Real-World Incident (01)

Incident Overview

TTPs (Tactics, Techniques, and Procedures):

- **Tactics:** Phishing combined with social engineering, targeting senior executives and institutions by impersonating the trusted DocuSign brand.
- **Techniques:** Deployment of phishing websites to steal Google credentials and exploitation of compromised email accounts to send fraudulent messages.
- **Procedures:** A multi-stage attack chain involving initial phishing emails, credential theft, account takeover, and subsequent theft of cryptocurrency assets.

APT Case Study: Real-World Incident (01)

Lessons Learned

Prevention: Enable MFA for critical accounts. Train staff via phishing simulations. Deploy AI email filters to block suspicious senders. Monitor logins and transactions.

Response: Isolate compromised accounts immediately. Enforce multi-approval for fund transfers. Conduct security drills to test protocols.

Other: Update training with emerging threats. Use enterprise email security tools. Set strict account security baselines.

APT Case Study: Real-World Incident (02)

Incident Overview

Since June 2024, the Lazarus Group has launched a state-sponsored APT campaign targeting cryptocurrency exchanges. Attackers embedded malicious code in fake open-source projects (e.g., financial tools), exploiting PyYAML for remote control. Multiple exchanges were compromised, though some attacks were blocked due to triggered security alerts.

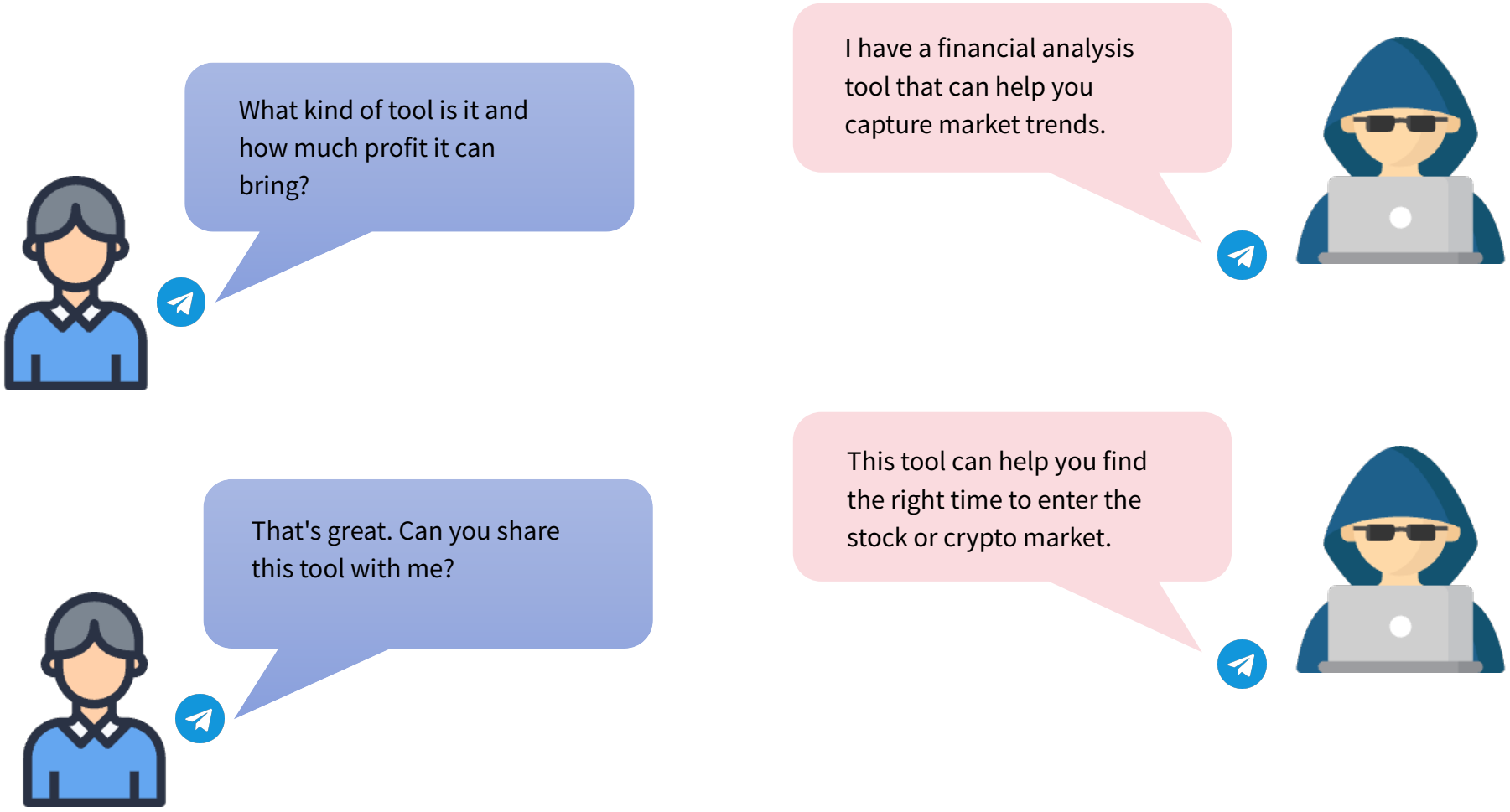
Loss Details:

Over 2 billion USD

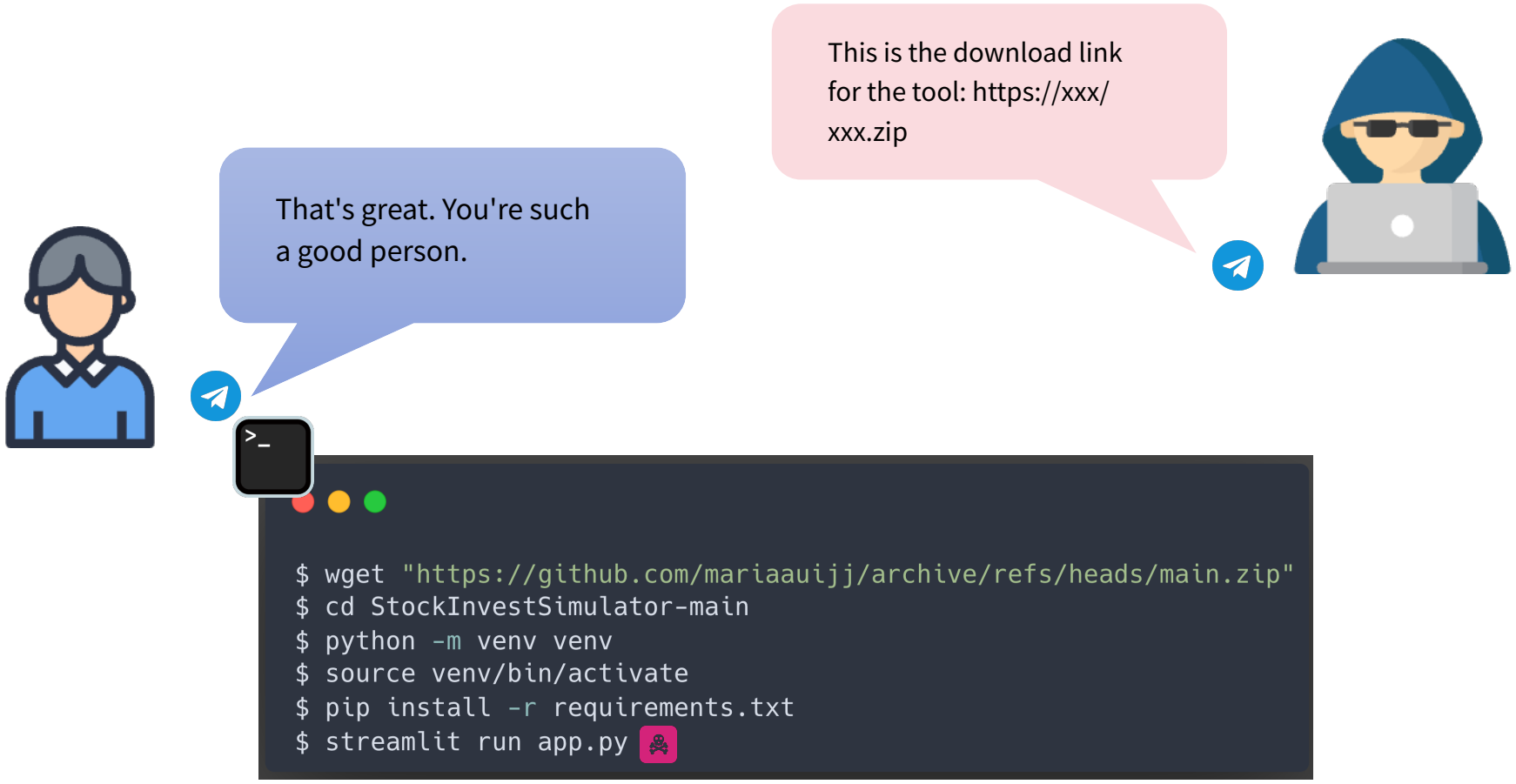
Intelligence:

- https://slowmist.medium.com/cryptocurrency-apt-intelligence-unveiling-lazarus-groups-intrusion-techniques-a1a6efda7d34
- https://www.validin.com/blog/bybit_hack_infrastructure_hunt

APT Case Study: Real-World Incident (02)



APT Case Study: Real-World Incident (02)



APT Case Study: Real-World Incident (02)

Control the organization's employee computers through Trojan horses

Use the VPN network of the employee's computer to access the Vault server

Get the private key on the Vault server and steal cryptocurrency assets

APT Case Study: Real-World Incident (02)

Incident Overview

After the Bybit breach, SlowMist publicly disclosed the attack intelligence (IOCs/TTPs) for the first time, enabling ecosystem projects to rapidly assess risks and enhance defenses.

Attack Pathway:

Disguised Open-Source Projects: Uploaded fake GitHub repositories (e.g., xxxstockinvestsimulator-main.zip) mimicking legitimate financial analysis tools.

Social Engineering: Deceiving the target to run a financial analysis tool.

Malicious Code Injection: Inserted RCE logic via PyYAML's yaml.load in files like data_fetcher.py.

C2 Communication: Used malicious domains (e.g., getstockprice.info, etc) and IPs (e.g., 193.233.171.58, etc) to control devices and exfiltrate data.

APT Case Study: Real-World Incident (02)

Timeline

Timestamp (UTC)	Event
2025-02-02 01:50:18	Attacker registered getstockprice[.]com via Namecheap
2025-02-04 08:55:45	Developer1 compromised
2025-02-05 08:36:51	Attacker first accessed Safe{Wallet} AWS environment
2025-02-05 14:06:25	Attacker unsuccessfully attempted to register their own MFA device
2025-02-05 to 2025-02-17	Attacker reconnaissance in AWS environment
2025-02-17 03:22:44	Attacker command and control activity in AWS environment
2025-02-19 15:29:25	Wayback Machine snapshot with malicious JS code inserted to Safe{Wallet} website
2025-02-21 14:13:35	Bybit exploit transaction
2025-02-21 14:15:13	Wayback Machine snapshot without malicious JS code in Safe{Wallet} website
2025-02-21 14:16:11	Bybit heist transaction

Key Findings To Date

- Developer1's macOS workstation was compromised on February 4, 2025 when a Docker project named `MC-Based-Stock-Invest-Simulator-main` communicated with `getstockprice[.]com` which resolved to IP address `70.34.245[.]118`. The Docker project was no longer available on the system at the time of analysis but the files resided in the `~/Downloads/` directory, indicating possible social engineering.
    - Note: Similar stock-themed Docker projects have been utilized by UNC4899 in previous heist investigations. For example, in September 2024, UNC4899 socially engineered a crypto exchange developer via Telegram into helping troubleshoot a Docker project which dropped a second stage macOS malware known as PLOTTWIST that enabled persistent access to the compromised developer workstation.
- Whois reported `getstockprice[.]com` was registered via Namecheap on February 2, 2025. SlowMist's reporting on February 23, 2025 identified a DPRK-attributed indicator of compromise (IOC), `getstockprice[.]info`, a nearly identical domain name registered on January 7, 2025 via Namecheap.
- The Docker project directory structure shared in SlowMist's report is consistent with malicious file names identified on Developer1's workstation.
- The attacker use of Developer1's AWS account originated from ExpressVPN IP addresses with User-Agent strings containing `distrib#kali.2024`. Mandiant assesses that this User-Agent string indicates use of Kali Linux which is designed for offensive security practitioners. Mandiant has previously observed UNC4899 using ExpressVPN infrastructure and Kali when conducting their operations.
- Safe{Wallet}'s AWS configuration required MFA re-authentication for Security Token Service (STS) sessions every 12 hours. Mandiant observed failed attempts by the attacker to register their own MFA device. To bypass this security control, the attacker hijacked active AWS user session tokens, likely via malware deployed on Developer1's workstation, and aligned their hours to Developer1's schedule in order to conduct their operations while the AWS sessions were active.
- Mandiant identified three (3) additional domains linked to UNC4899 used in the attack on Safe{Wallet} and were recently registered via Namecheap. The domains were identified in logs recovered from Developer1's workstation and in AWS network logs.

APT Case Study: Real-World Incident (02)

How much does it cost?

¥ 2,000

Current State of Corporate Defense Strategies

1.Secure Network Proxy Configuration

Implement security policies on network proxies to enable security decisions and service management based on a zero-trust model.

Solution: Fortinet , Akamai , Cloudflare etc.

2.DNS Traffic Security Protection

Enforce security controls at the DNS layer to detect and block requests resolving known malicious domains, preventing DNS spoofing or data leaks.

Solution: Heimdal, Palo Alto, Cisco Umbrella etc.

3.Network Traffic/Host Monitoring and Threat Detection

Analyze network traffic data in real time to detect anomalies and identify potential attacks (e.g., IDS/IPS). Deploy HIDS on servers to detect exploitation attempts early.

Solution: SolarWinds, Alibaba Cloud Security Center, GlassWire, Little Snitch etc.

4.Network Segmentation

Divide the network into smaller, isolated zones to limit threat propagation and enhance security controls.

Solution: Akamai Guardicore, Cisco Identity Services Engine etc

Current State of Corporate Defense Strategies

5.System Hardening Measures

Hardening considerations involve implementing security measures to reduce vulnerabilities and strengthen system defenses against potential attacks.

Solution: Tenable.io, public.cyber.mil etc

6.Endpoint Visibility

Provide real-time monitoring of endpoint activities, detect potential threats, enable rapid response (e.g., EDR), and enforce application whitelisting to identify and alert on abnormal programs.

Solution: CrowdStrike Falcon, Microsoft Defender for Endpoint etc.

7.Centralized Log Management and Analysis

Consolidate log data from different systems into a unified platform for easier tracking, analysis, and response to security incidents.

Solution: Splunk Enterprise Security, Graylog, ELK etc.

8.Enhancing Security Awareness

Improve security awareness among team members, enabling them to recognize most social engineering attacks and proactively report anomalies for quicker investigation.

Solution: Blockchain Dark Forest Selfguard Handbook, Web3 Phishing Techniques Analysis etc.

User Case Study:
Phishing Attacks Cause $494 Million in Losses (03)

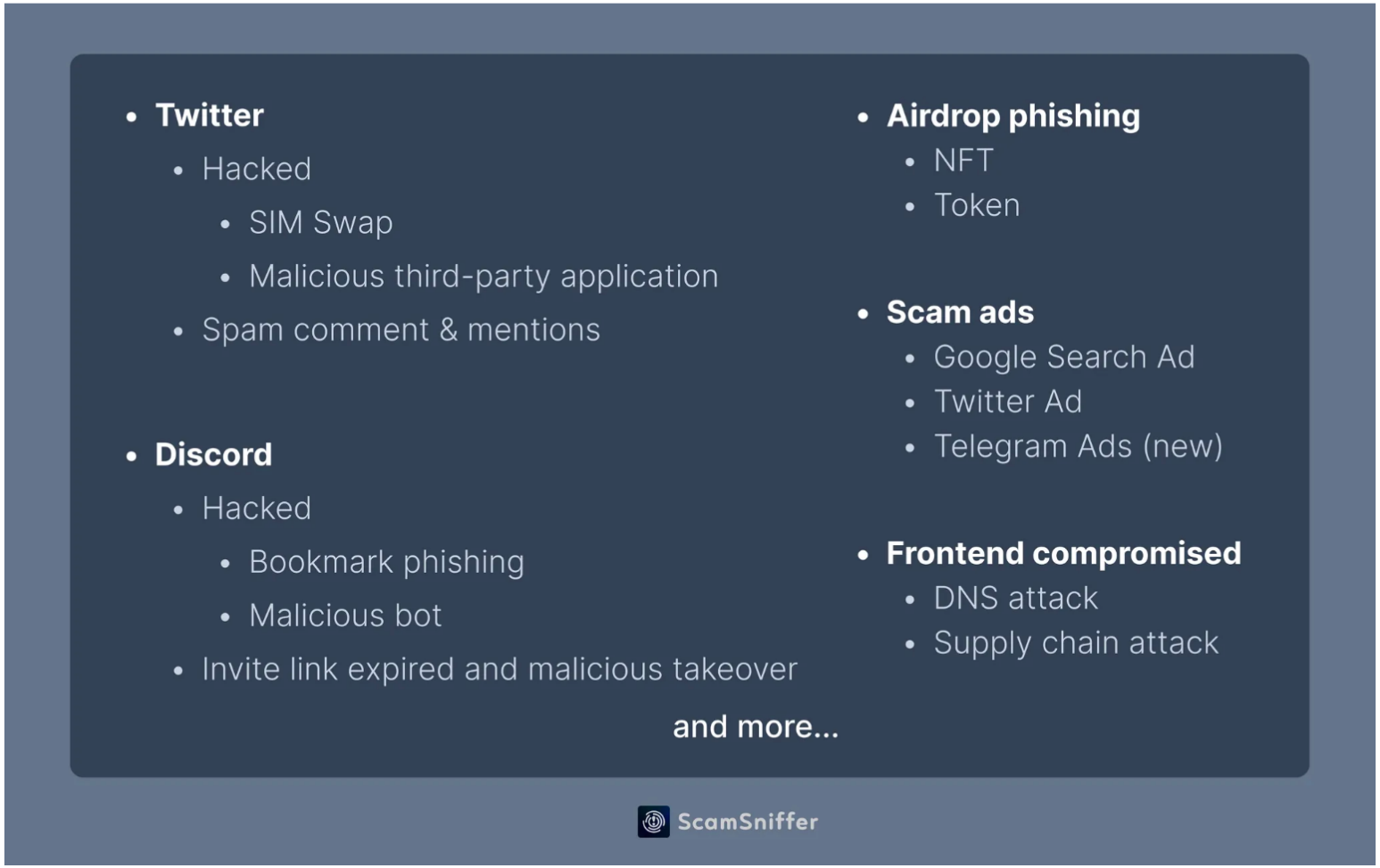
User Case Study:
Phishing Attacks Cause $494 Million in Losses (03)

Major Case Analysis

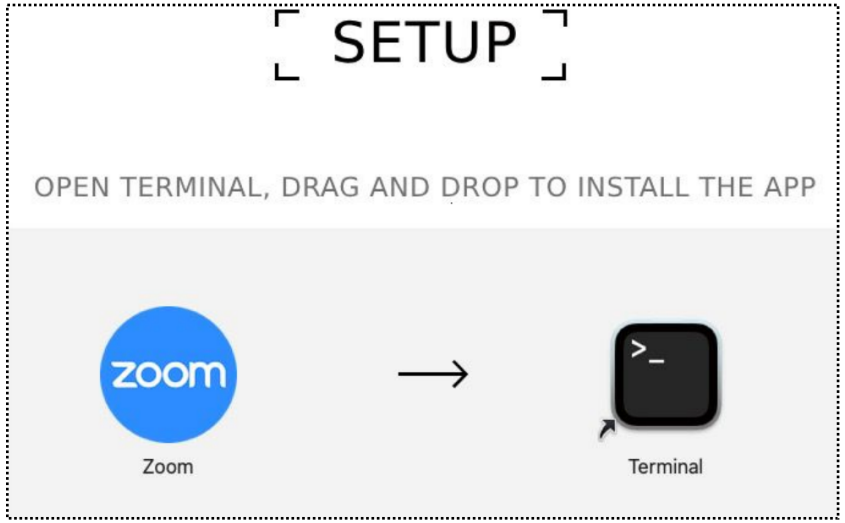
30 cases exceeding $1 million occurred throughout the year, with total losses of $171 million.

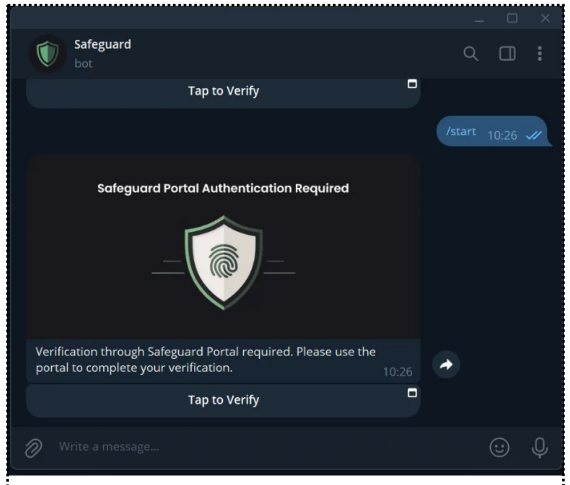
User Case Study: Phishing Attacks Cause $494 Million in Losses (03)

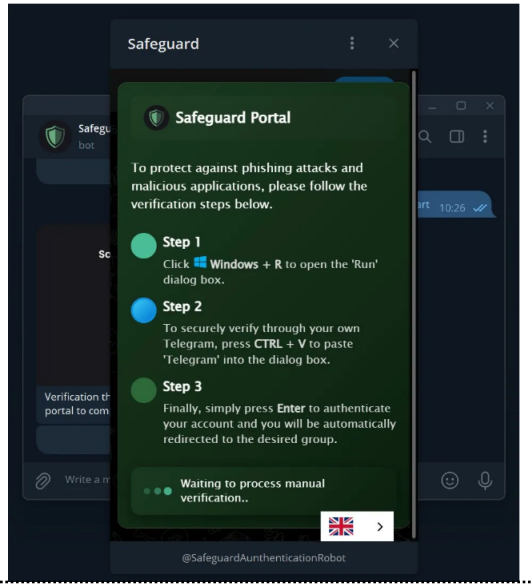
Common Traffic Sources for Phishing Websites



User Case Study:
Phishing Attacks Cause $494 Million in Losses (03)







User Case Study:
Phishing Attacks Cause $494 Million in Losses (03)

SLOWMIST

1 Real-World Web2 Attack Cases in the Web3 Industry

2 The Current State of Offense and Defense from a Red Teamer's Perspective

3 Full-Lifecycle Protection Solutions for Web3

Evolving Red Team Tactics in Response to Enhanced Defenses

Increased Difficulty

Advanced Defenses: AI detection, robust firewalls.

Stricter Policies: Tight access controls, comprehensive monitoring.

Impact on Red Teams

Challenges: Traditional attacks less effective.

Examples: Legacy methods failing, need for stealth.

New Techniques

Innovations: Social engineering, advanced persistence.

Adaptation: Multi-layered strategies, new tech vulnerabilities.

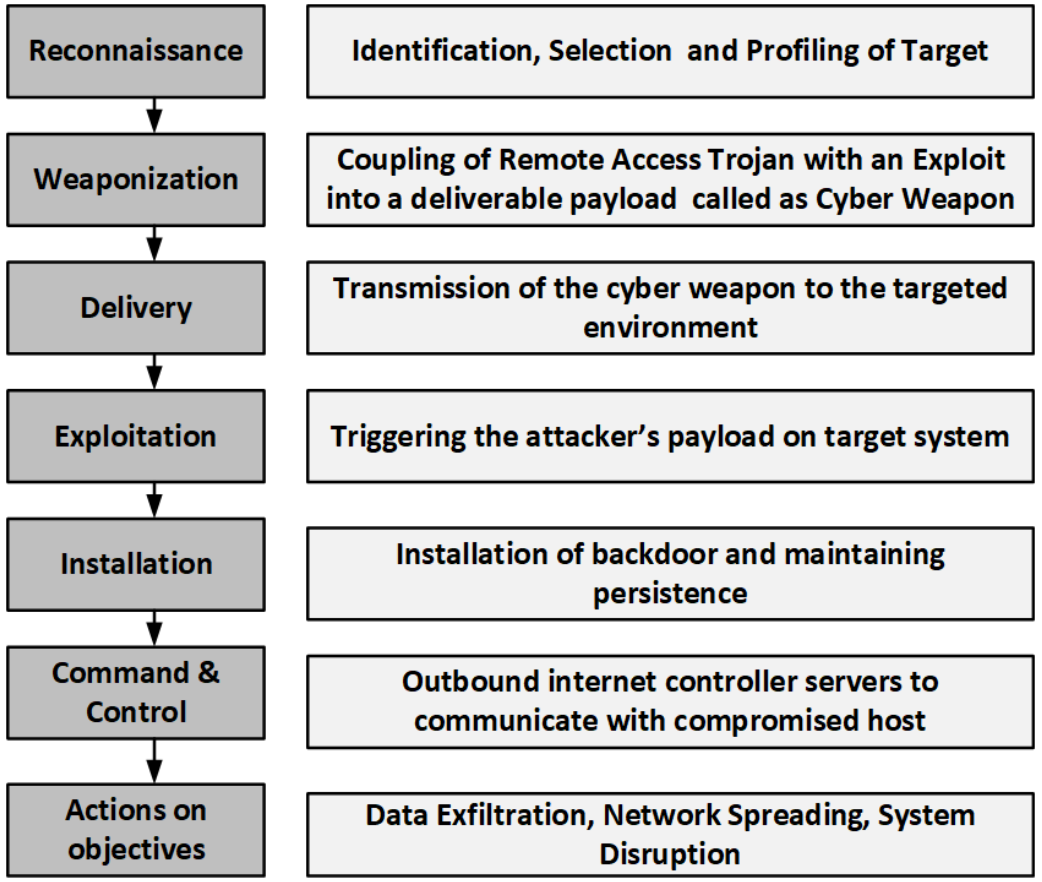
The red teamer must adapt and explore new attack techniques to keep the drill effective.

Cyber Kill Chain => Unified Kill Chain

- The **Cyber Kill Chain**, developed by Lockheed Martin, outlines a linear sequence of attack stages from reconnaissance to achieving objectives, helping organizations understand and defend against specific attack phases. In contrast.

- The **Unified Kill Chain** offers a more comprehensive and flexible framework, integrating additional phases like preparation and post-exploitation, to address a wider range of attack scenarios and defensive strategies.

- **The Unified Kill Chain offers enhanced flexibility for modeling attacks from diverse threat perspectives.**



Red Team vs. Blue Team: Roles and Common Goal

Evolving Defenses and Innovative Breaches: SlowMist's Approach

Blue Team Perspective

- Defense: Comprehensive coverage from reconnaissance to objective.
- Control: People, Process, and Technology.
- Detection: Identify effective TTPs (Tactics, Techniques, and Procedures) for attacks.

Red Team Perspective

"Trust but Verify" – Validate and challenge vendor claims about their security products.

General Bypass Techniques:

- Exploiting software vulnerabilities.
- Using social engineering techniques.
- Implementing stealth techniques to avoid detection.

Open Source Bypass Techniques:

Bypass-AV GitHub Repository - Includes various methods for bypassing antivirus software.
https://github.com/matro7sh/BypassAV/blob/main/img/Bypass-AV.png

Evolving Defenses and Innovative Breaches: SlowMist's Approach

Red Team Exercise

- Simulates realistic attacks and tests defenses.
- Adapt and explore new attack techniques to keep the drill effective.

Blue Team Response

- Analyzes and responds to the simulated attack.

Feedback and Learning

- Gather insights and identify areas for improvement.

Enhanced Defenses

- Implement improved strategies and processes.

Continuous Evolution

- Red Team exercises drive ongoing improvement in security defenses, making the Blue Team more effective with each exercise.

The more you train, the more you improve

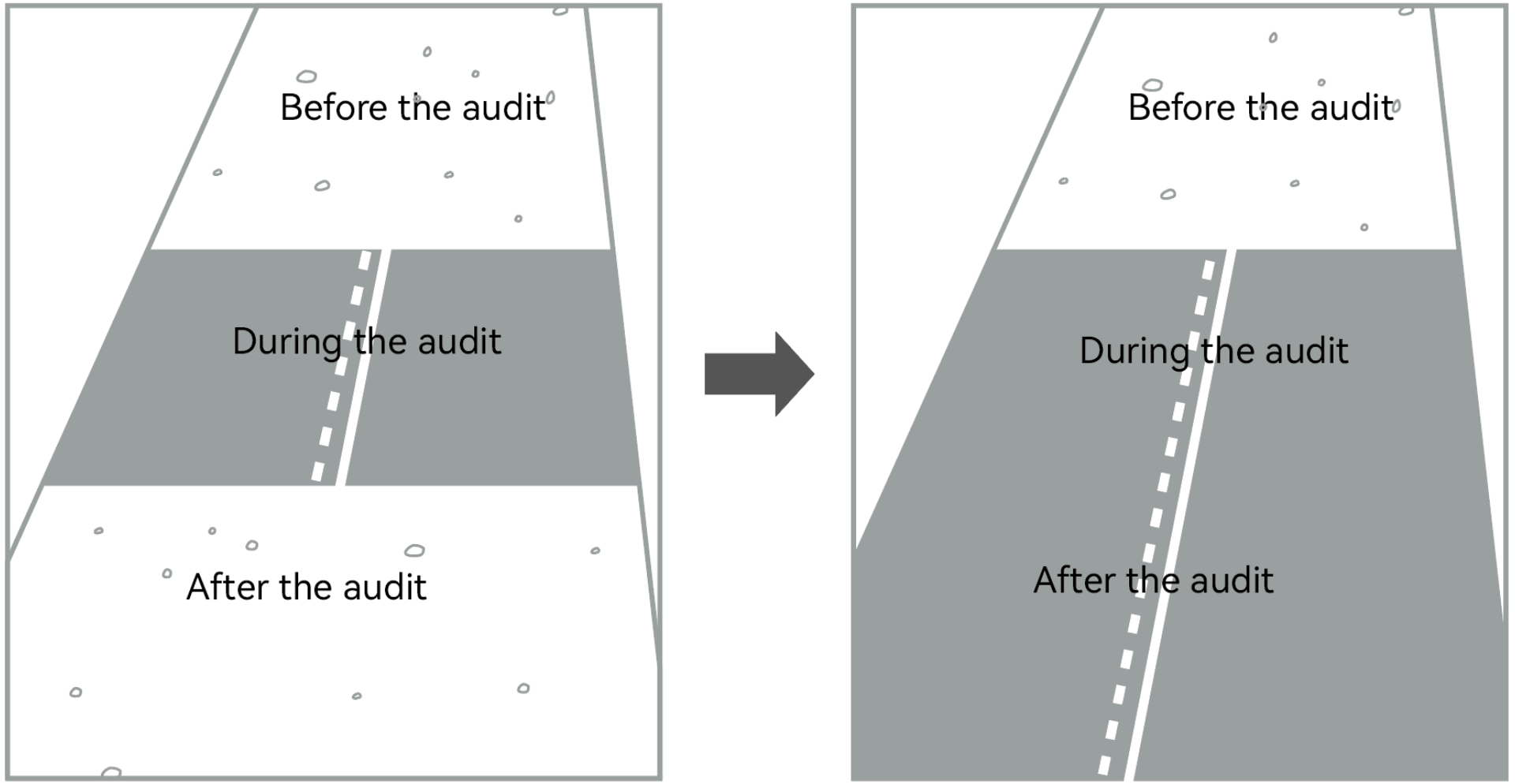
SLOWMIST

1 Real-World Web2 Attack Cases in the Web3 Industry

2 The Current State of Offense and Defense from a Red Teamer's Perspective

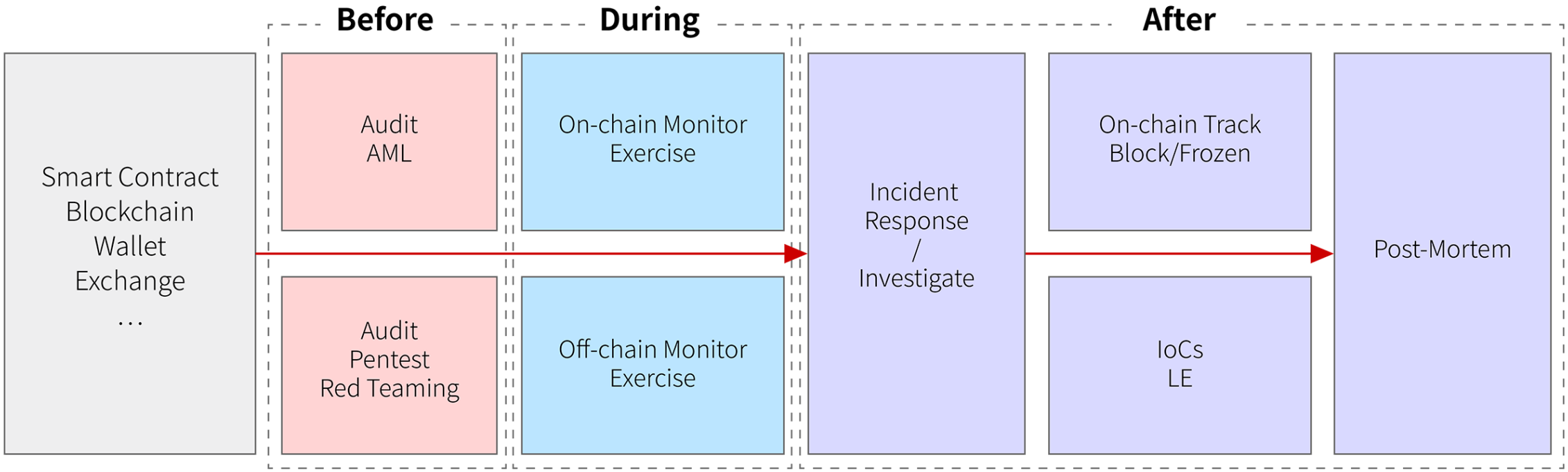
3 Full-Lifecycle Protection Solutions for Web3

How SlowMist Delivers Full-Lifecycle Protection



How SlowMist Delivers Full-Lifecycle Protection

Web3 security requires a full process solution: before, during, and after the event



Security Consulting: Security System(People+Assets+Permissions), Defense Deployment, Zero Trust, BTI

Zero Trust: Disaster Recovery and Exercise, DevSecOps **BTI**: InMist Cooperation Network, Emergency Response, Responsible Disclosure

MistEye Security Monitor

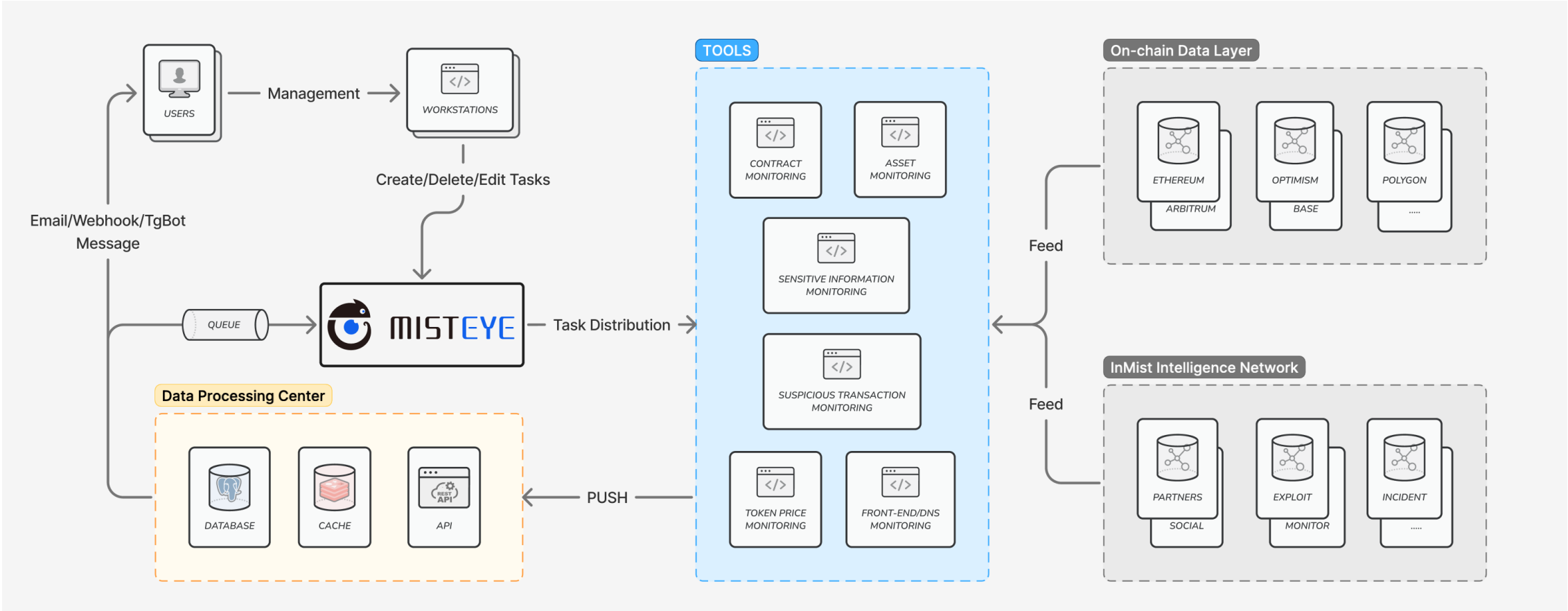
https://misteye.io

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.

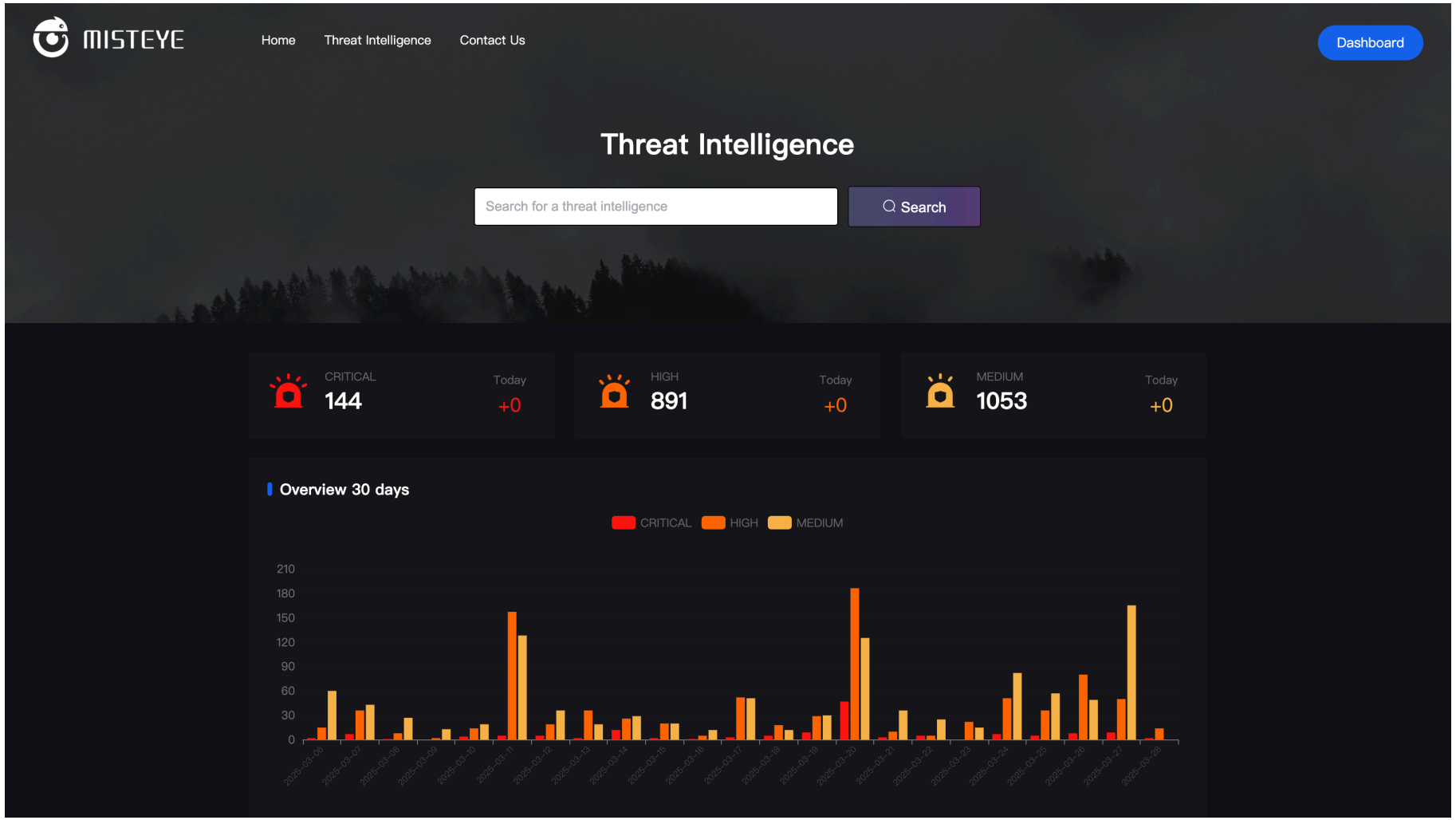
MistEye is equipped to support the following types of security monitoring:

- 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: Newly released vulnerabilities or PoC collection and notification.
- Intelligence: Capture and provide intelligence on APT attacks targeting the cryptocurrency industry.

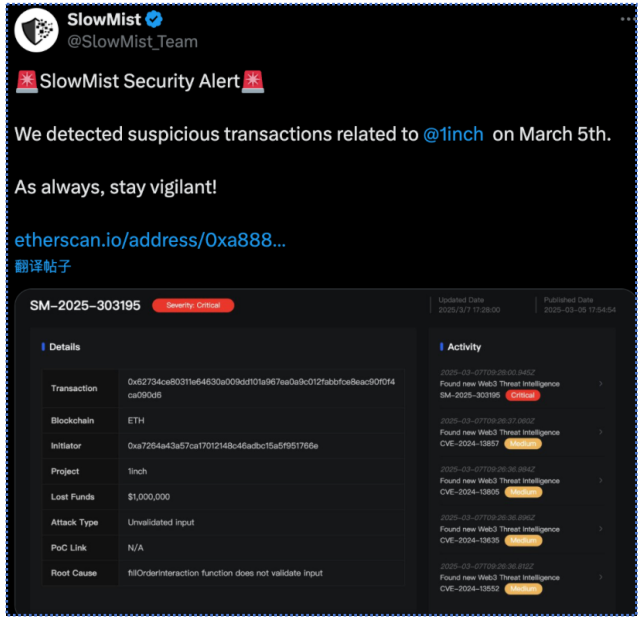
MistEye Security Monitor

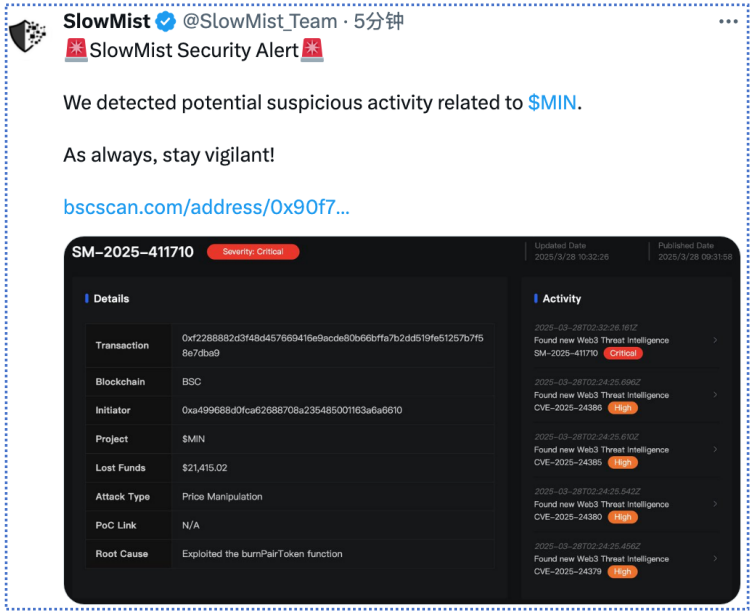


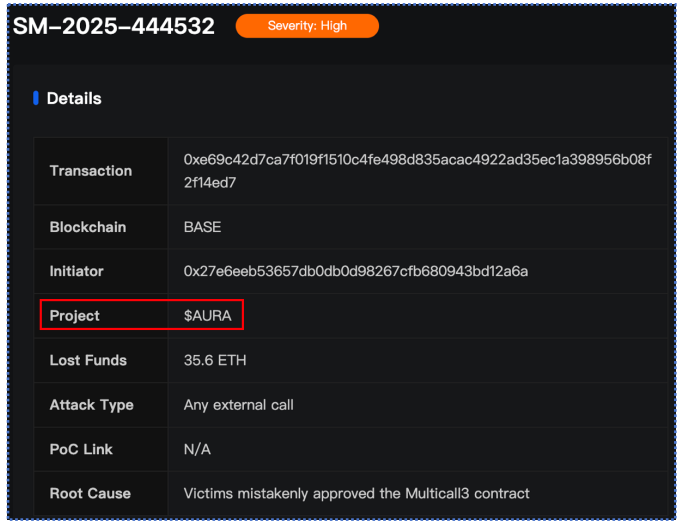
MistEye Security Monitor

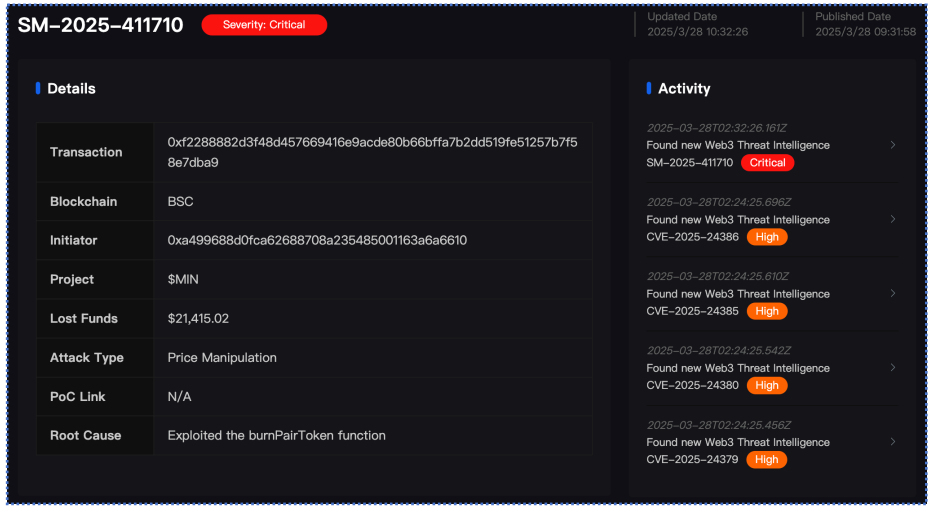


MistEye Security Monitor









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

Blockchain AML Solution

MISTTRACK BY SLOWMIST https://misttrack.io

1K +	500K +	300M +	90M +	17
Address Entities	Threat Intelligence Addresses	Addresses Labeled	Risky Addresses Identified	Blockchains

- Crypto Wallet Screening
- Crypto Transaction Monitoring
- Crypto Investigations
- Crypto KYA/KYT API

Customer Sample

MEXC Global, Bingx, XREX, CoinW, SAFEHERON, imToken, Flashwire, Doo Payment, dtcpay, LEGEND TRADING, Celer, puffer, zkMe, Dupay, Keyblock

Our Solution: MistTrack Tracking Service

Expert services designed to investigate incidents and recover stolen funds.

90+

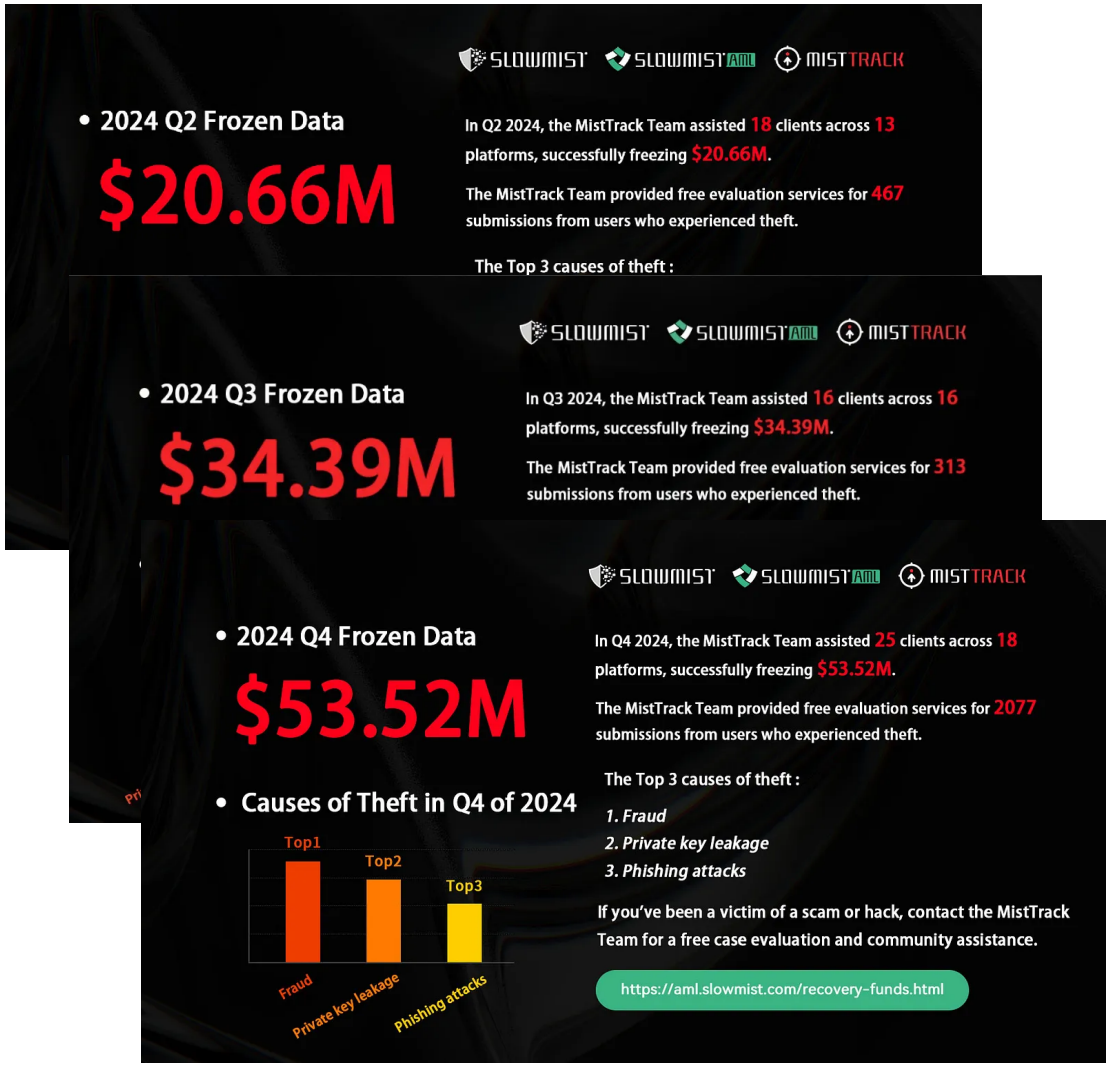
Customers Served

$1,000,000,000+

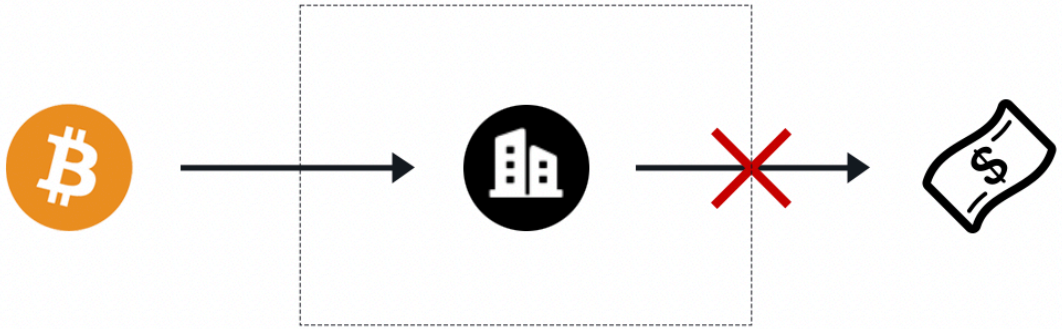
Cumulative Recovered Assets

$120,000,000+

Frozen Assets in 2024



Our Solution: MistTrack Tracking Service



+ More than 100 partners

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

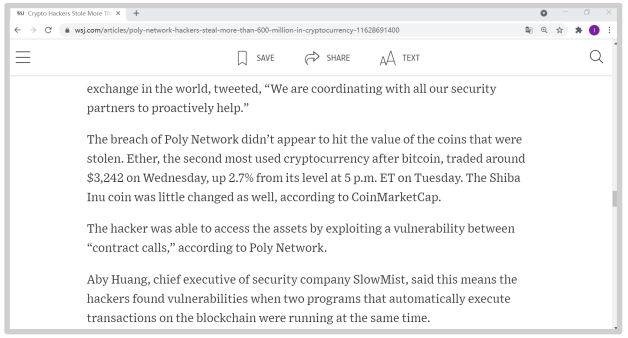
THE WALL STREET JOURNAL.

REUTERS®

THE BLOCK

Forbes

Bloomberg

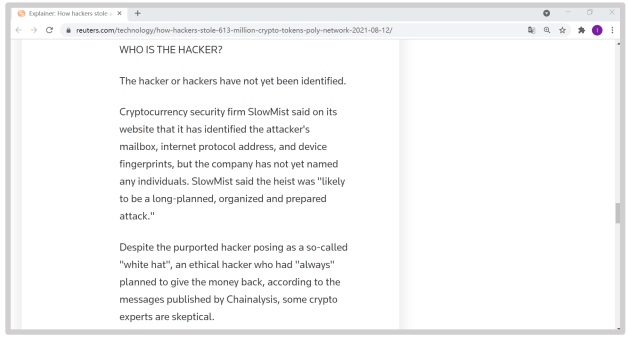


exchange in the world, tweeted, "We are coordinating with all our security partners to proactively help."

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.

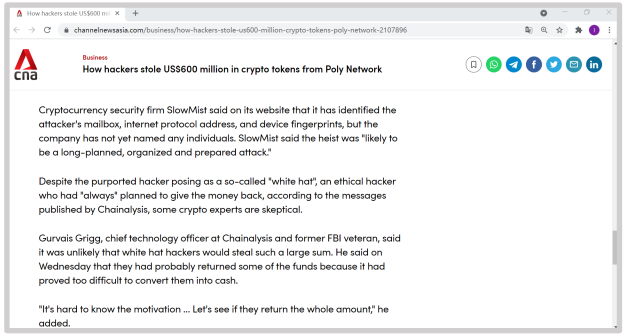


WHO IS THE HACKER?

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.



Business

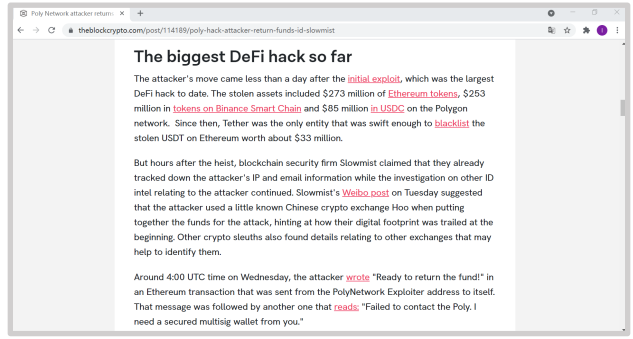
How hackers stole US$600 million in crypto tokens from Poly Network

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.

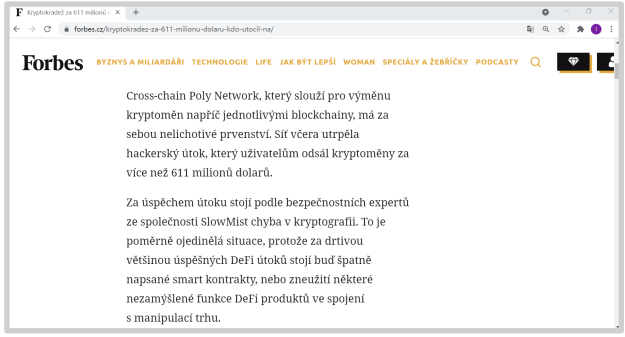


The biggest DeFi hack so far

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.

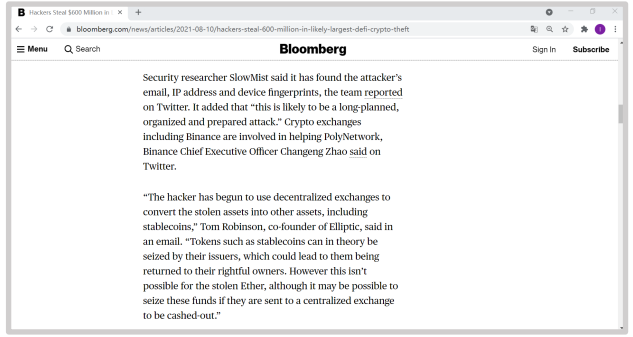
Around 4:00 UTC time on Wednesday, the attacker wrote "Ready to return the fund!" in an Ethereum transaction that was sent from the PolyNetwork Exploiter address to itself. That message was followed by another one that reads: "Failed to contact the Poly. I need a secured multisig wallet from you."



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."

Thank You

Official Website
https://slowmist.com

Email
team@slowmist.com

X (Twitter)
@SlowMist_Team

GitHub
https://github.com/slowmist

Medium
https://slowmist.medium.com