SLOWMIST 2024 Mid-year

Blockchain Security and AML Report

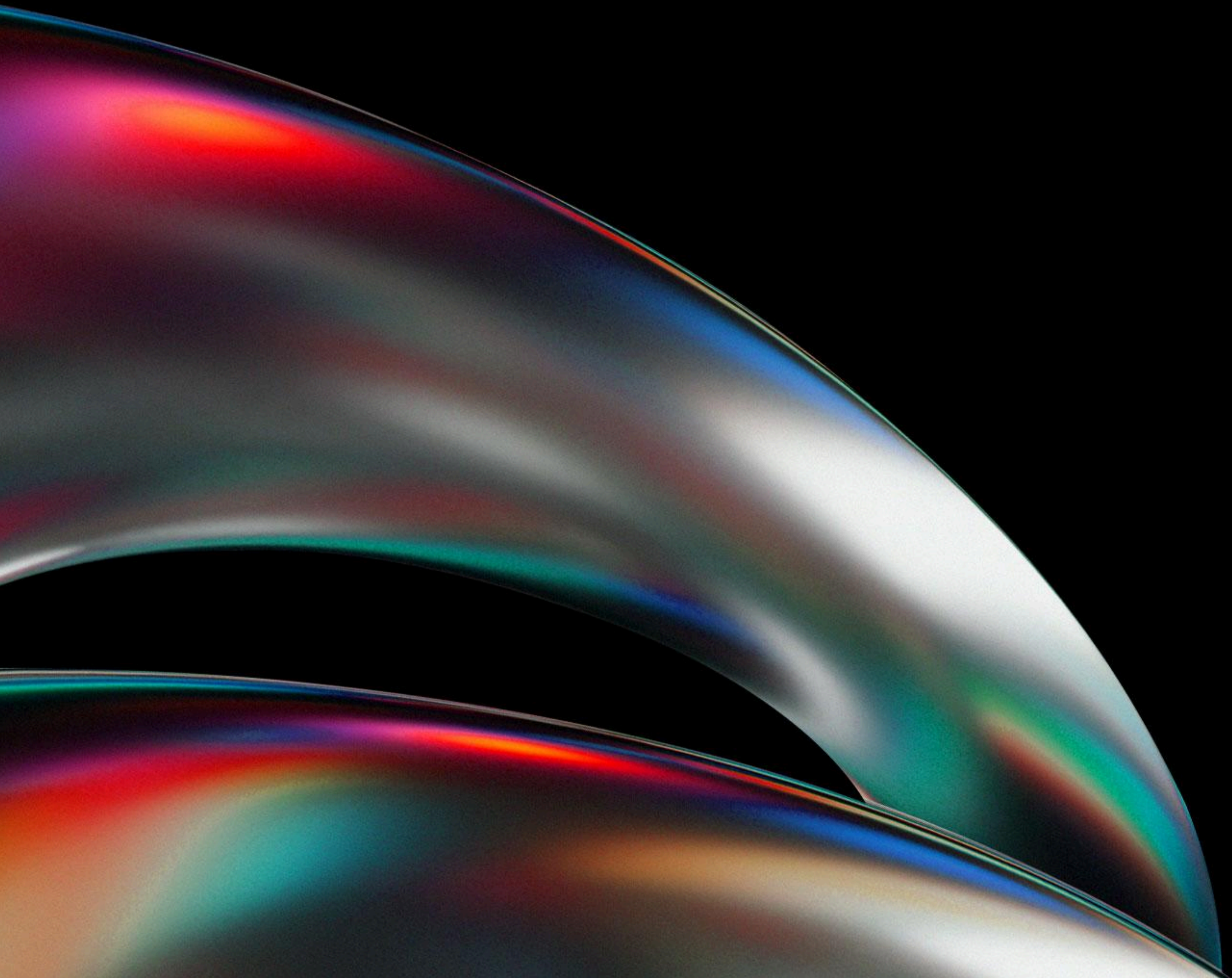


Table of Contents

I. Introduction

The cryptocurrency market has seen significant developments, particularly with the U.S. Securities and Exchange Commission (SEC) surprising Wall Street by making a rule change to allow the creation of spot Ethereum (ETH) exchange-traded funds. On the other hand, regulators continue to target the cryptocurrency industry by taking on crypto exchanges and their high-profile executives, including close allies of former FTX CEO Sam Bankman-Fried.

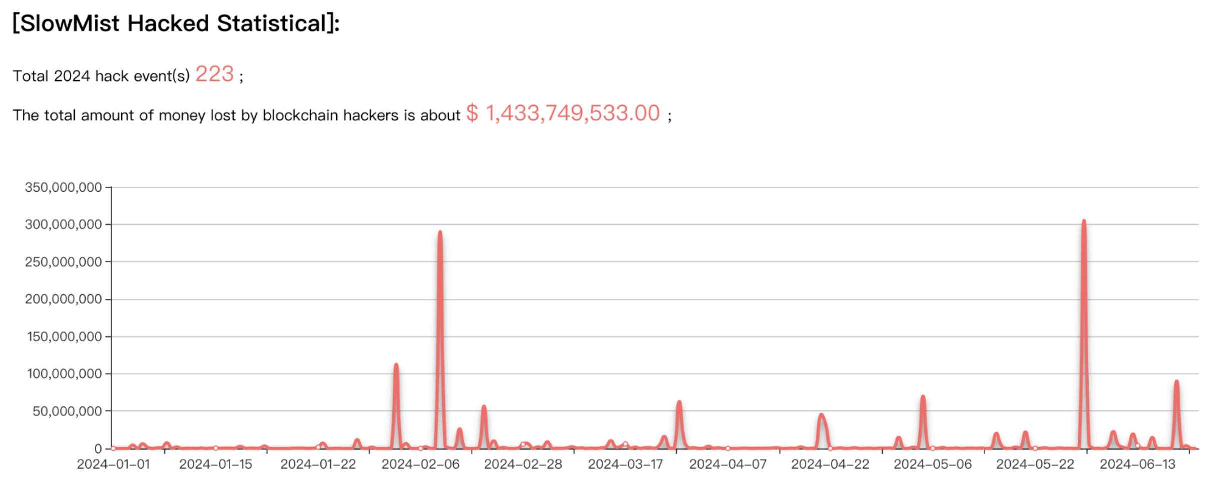
In terms of regulatory policies, as regulatory agencies and the public increasingly understand cryptocurrencies and blockchain technology, countries' policies towards the cryptocurrency field are diverging significantly. Governments' attitudes towards cryptocurrency regulation generally fall into three categories: embracing support, ambiguous uncertainty, and strict prohibition. Despite varying attitudes towards cryptocurrencies among governments, the policies in the first half of 2024 undoubtedly mark the beginning of a new era of cryptocurrency regulation, with the cryptocurrency market moving towards compliance. Simultaneously, many emerging trends and themes are emerging, with increasing numbers of cryptocurrency users and Web3 developers, and AI gradually taking shape. According to CoinMarketCap data, as of June 30, the global cryptocurrency market capitalization exceeded $2.34 trillion, indicating robust overall growth in the global blockchain market.

Against this backdrop, this report focuses on two major aspects of blockchain ecosystem security and anti-money laundering (AML) security: the first part outlines the security situation of blockchain in the first half of 2024 and common phishing/theft techniques during this period; the second part reviews AML regulatory dynamics, analyzes the activities of hacker groups and laundering tools, and provides statistics on frozen and returned funds from security incidents in the first half of the year. Through this analysis, the report aims to provide a comprehensive understanding of the current and future security risks in the blockchain ecosystem.

II. Blockchain Security Trends

2.1 Overview of Blockchain Security Incidents

According to incomplete statistics from the SlowMist Hacked, a total of 223 security incidents occurred in the first half of 2024, resulting in losses as high as $1.43 billion. Compared to the first half of 2023 (185 incidents with losses of approximately $920 million), this represents an over 50% increase in losses. (Note: This report does not include personal losses in statistics)



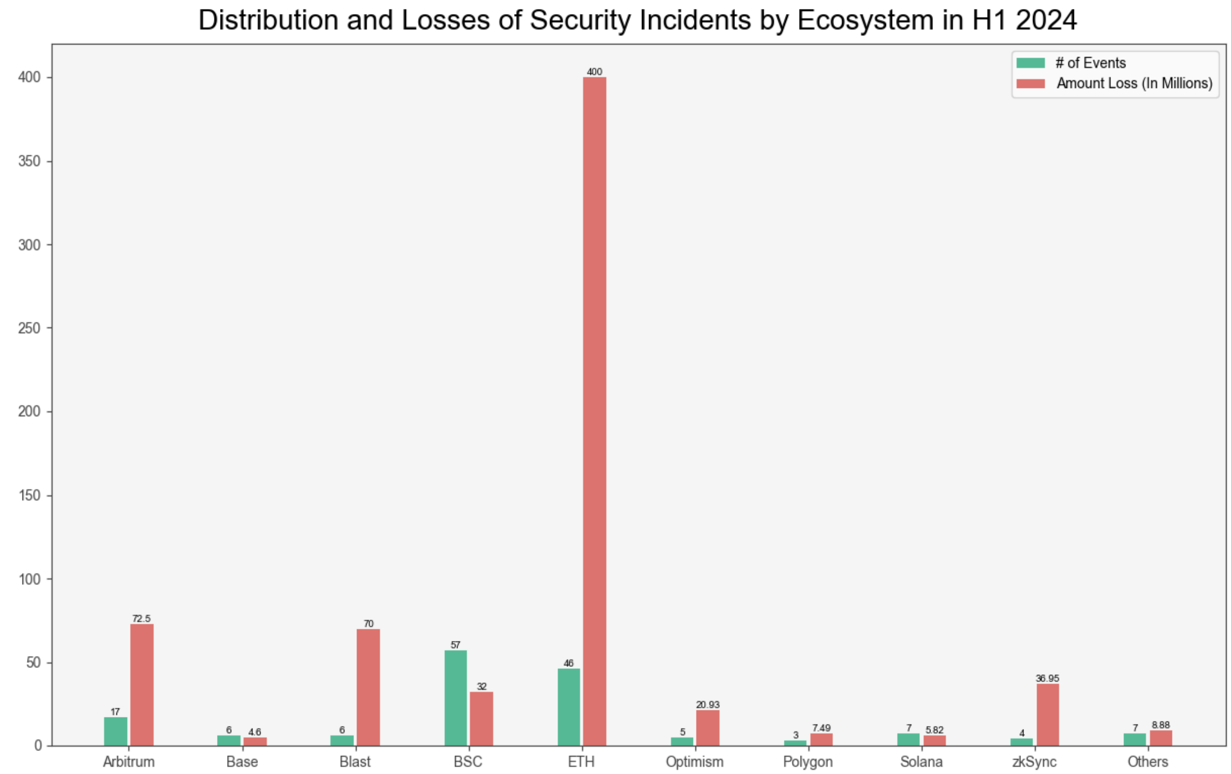
[SlowMist Hacked Statistical]:

Total 2024 hack event(s) 223 ;

The total amount of money lost by blockchain hackers is about $ 1,433,749,533.00 ;

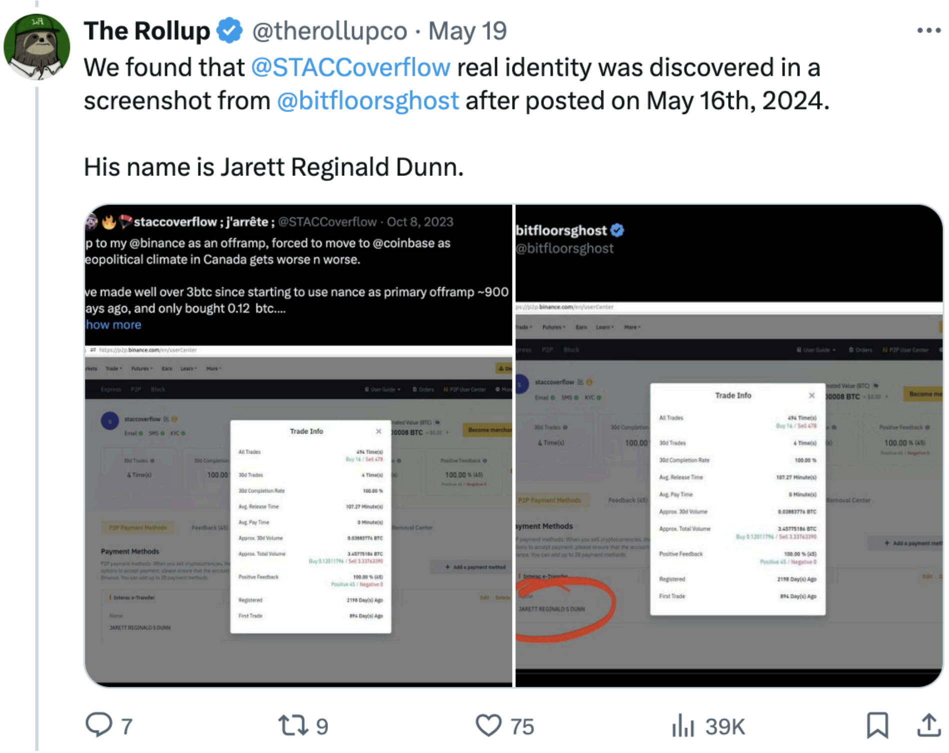
(https://hacked.slowmist.io/)

From an ecosystem perspective, Ethereum suffered the highest losses, amounting to $400 million. Followed by, Arbitrum incurred losses of $72.46 million, and Blast suffered losses of $70 million. Additionally, Binance Smart Chain (BSC) experienced the highest number of security incidents, totaling 57, with losses of approximately $32.12 million.



(Distribution and Losses of Security Incidents by Ecosystem in H1 2024)

It is noteworthy that with Solana's rapid rise in 2024, security incidents within its ecosystem have significantly increased. For instance, on May 16th, the token launcher pump.fun, based on Solana, was subjected to a flash loan attack, where the attacker randomly airdropped assets worth $80 million to holders like Slerf, Stacc, Saga, among others. pump.fun stated that the attack occurred due to a former employee exploiting privileged access to illegally obtain withdrawal permissions, leveraging a flash loan protocol. Out of the $45 million liquidity in its bonding curve contract, approximately $1.9 million was affected. On May 19th, Twitter user The Rollup reported that @STACCoverflow, the attacker of pump.fun, was arrested and detained by law enforcement in London, subsequently released on bail. The real name of the individual is believed to be Jarett Reginald Dunn.



The Rollup @therollupco · May 19

We found that @STACCoverflow real identity was discovered in a screenshot from @bitfloorsghost after posted on May 16th, 2024.

His name is Jarett Reginald Dunn.

staccoverflow ; j'arrête ; @STACCoverflow · Oct 8, 2023

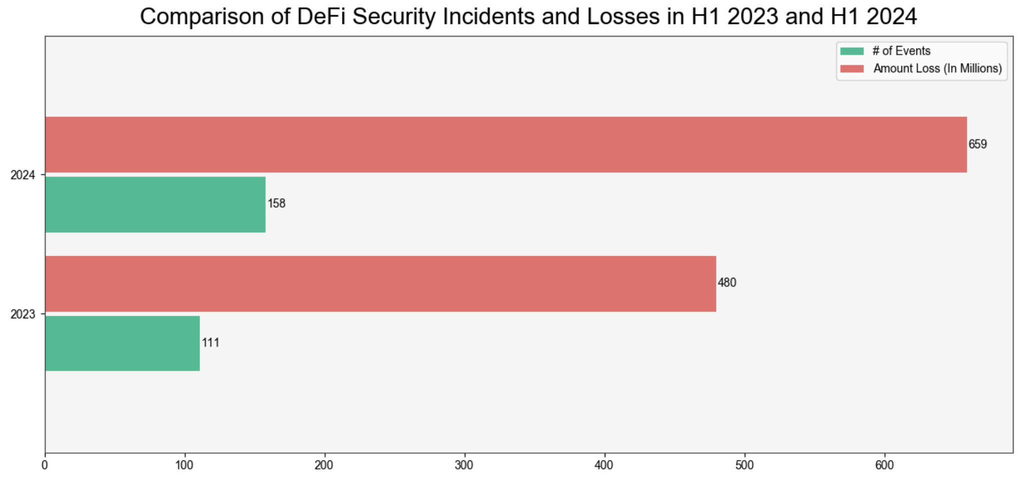
p to my @binance as an offramp, forced to move to @coinbase as eopolitical climate in Canada gets worse n worse.

ve made well over 3btc since starting to use nance as primary offramp ~900 ays ago, and only bought 0.12 btc....

how more

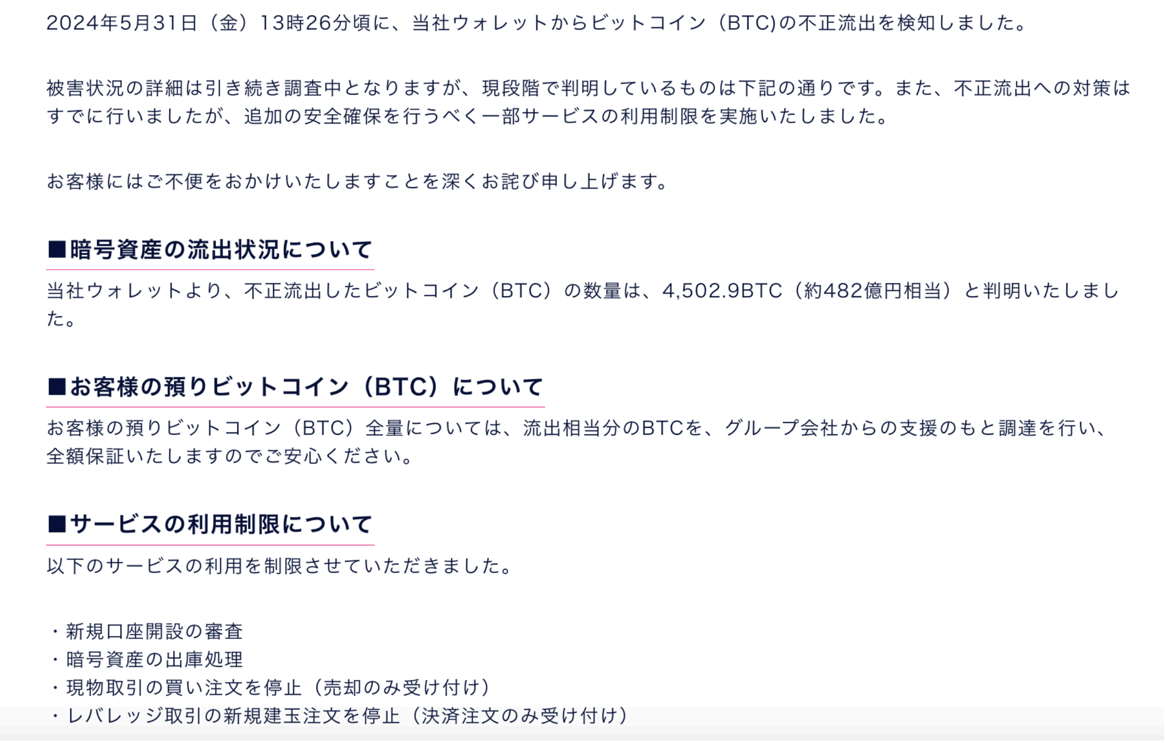
bitfloorsghost @bitfloorsghost

From the project track perspective, DeFi is the most frequently attacked area. In the first half of 2024, there were 158 DeFi security incidents, accounting for 70.85% of the total Incidents, with losses amounting to $659 Million. Compared to the First Half of 2023 (111 incidents with losses of approximately $480 Million), this represents a 37.29% year-on-year increase in losses.



(Comparison of DeFi Security Incidents and Losses in H1 2023 and H1 2024)

Next, security incidents on trading platforms resulted in losses as high as $524 Million, with the DMM Bitcoin incident alone accounting for $305 Million, making it the largest security incident of the first half of 2024. On May 31st, the Japanese cryptocurrency exchange DMM Bitcoin reported that 4,502.9 BTC was illegally transferred from its official wallet, resulting in a loss valued at approximately 48.2 billion yen ($305 million). A representative from Japan's Financial Services Agency (FSA) stated that a report request had been issued to DMM Bitcoin under the Payment Services Act, demanding a report on the cause of the theft and a customer compensation plan. DMM Bitcoin indicated that they had raised a total of 55 billion yen (approximately $354 million) for user compensation, and an equivalent amount of Bitcoin to cover the stolen quantity was purchased on June 14th. The investigation into the cause of this theft is ongoing. It is noted that the loss from the DMM Bitcoin security incident ranks seventh in cryptocurrency hacking history since December 2022 and is the largest attack since then. Previously, Japan experienced two major cryptocurrency exchange hacks: the Mt.Gox incident in 2014 ($450 million) and the Coincheck incident in 2018 ($534 million). The DMM Bitcoin attack now ranks as Japan's third-largest such case.



2024年5月31日（金）13時26分頃に、当社ウォレットからビットコイン（BTC)の不正流出を検知しました。

被害状況の詳細は引き続き調査中となりますが、現段階で判明しているものは下記の通りです。また、不正流出への対策はすでに行いましたが、追加の安全確保を行うべく一部サービスの利用制限を実施いたしました。

お客様にはご不便をおかけいたしますことを深くお詫び申し上げます。

■暗号資産の流出状況について

当社ウォレットより、不正流出したビットコイン（BTC）の数量は、4,502.9BTC（約482億円相当）と判明いたしました。

■お客様の預りビットコイン（BTC）について

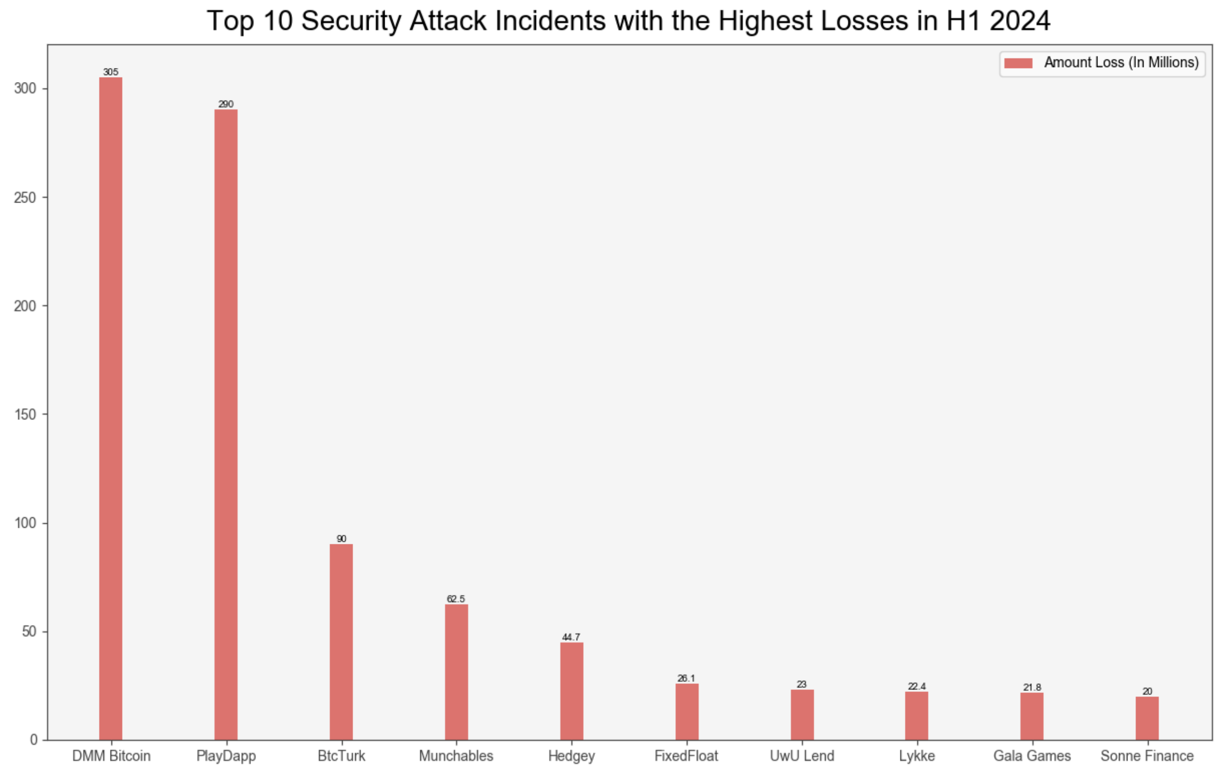
お客様の預りビットコイン（BTC）全量については、流出相当分のBTCを、グループ会社からの支援のもと調達を行い、全額保証いたしますのでご安心ください。

■サービスの利用制限について

以下のサービスの利用を制限させていただきました。

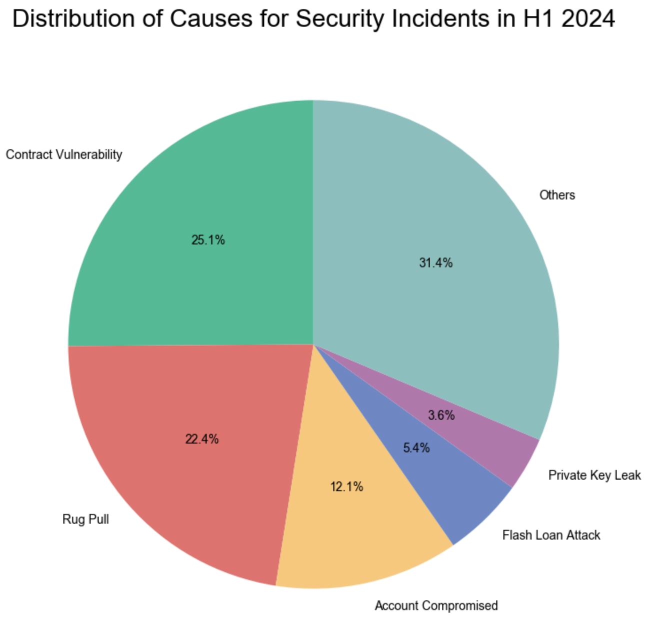
・新規口座開設の審査
・暗号資産の出庫処理
・現物取引の買い注文を停止（売却のみ受け付け）
・レバレッジ取引の新規建玉注文を停止（決済注文のみ受け付け）

In terms of losses, two incidents had losses of over $100 million. The following are the top 10 security attack incidents with the highest losses in the first half of 2024:



(Top 10 Security Attack Incidents with the Highest Losses in H1 2024)

Regarding the causes of incidents, Contract Vulnerabilities accounted for most of the incidents, totaling 56, with losses of approximately $104 Million. The second-most incidents were due to exit scams, totaling 50. The second-largest loss incident in the first half of 2024 was the PlayDapp incident, which resulted from a leaked private key. On February 10th, the Ethereum-based gaming platform PlayDapp reported an attack due to a leaked private key, where the unauthorized minting of 200 million PLA tokens (valued at $36.5 million) occurred. Shortly after the incident, PlayDapp attempted negotiation through on-chain transactions with the attacker, demanding the return of stolen funds and offering a $1 million white hat reward. Negotiations failed, and on February 12th, the hacker minted an additional 1.59 billion PLA tokens ($253.9 million) and dispersed the funds across multiple blockchain addresses and trading platforms.



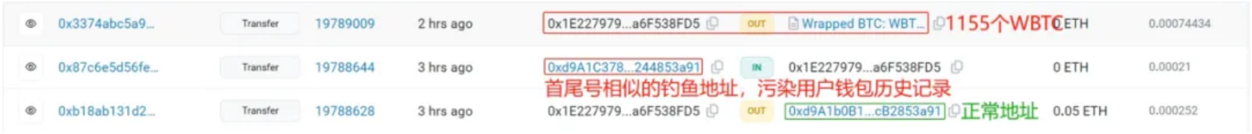
(Distribution of Causes for Security Incidents in H1 2024)

2.2 Phishing/Theft Techniques

This section highlights some phishing and theft techniques disclosed by SlowMist in the first half of 2024.

2.2.1 Identical Prefix and Suffix Address Phishing

On May 3, 2024, the Web3 anti-scam platform Scam Sniffer reported that a high-net-worth wallet, or "whale," lost 1155 WBTC (approximately $70 million) in an address poisoning attack. The victim offered the attacker a 10% white hat bounty, worth $7 million, in an effort to recover the remaining funds, highlighting the potential complications of holding such a large stolen amount. Initially, the attacker did not respond, but a few days later, they unexpectedly transferred 51 ETH back to the victim and provided a Telegram contact. Eventually, the attacker returned all the stolen assets.



👁	0x3374abc5a9...	Transfer	19789009	2 hrs ago	0x1E227979...a6F538FD5	OUT	Wrapped BTC: WBT...	ETH	0.00074434
👁	0x87c6e5d56fe...	Transfer	19788644	3 hrs ago	0xd9A1C378...244853a91	IN	0x1E227979...a6F538FD5	0 ETH	0.00021
👁	0xb18ab131d2...	Transfer	19788628	3 hrs ago	0x1E227979...a6F538FD5	OUT	0xd9A1b0B1...cB2853a91	0.05 ETH	0.000252

1155个WBTC

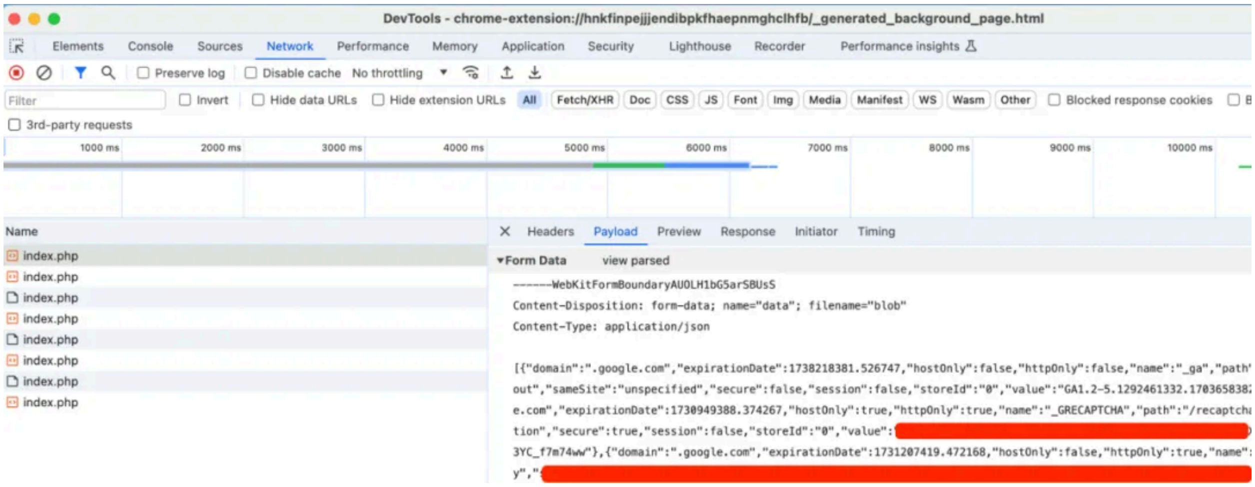
首尾号相似的钓鱼地址，污染用户钱包历史记录

正常地址

The technique of address poisoning has been around for a long time, but the losses in this incident were exceptionally large. Typically, attackers pre-generate a large number of phishing addresses and deploy batch programs distributedly, targeting users with large or frequent transaction volumes. When these users initiate transactions, hackers immediately use generated phishing addresses to continuously airdrop small amounts of funds (e.g., 0.01 USDT, 0.001 USDT, 0 ETH, etc.). Exploiting the similarity in the first and last digits between the attacker's address and the user's address, they conduct phishing attacks to contaminate the user's transaction records. Users often copy recent transaction information from wallet histories and generally only pay attention to the first and last digits, which can lead to asset losses if they are not careful. We strongly advise users to save frequently used addresses in their wallets for future use and enable wallet features that filter small transactions to block such malicious transfers to reduce phishing risks. Overall, since blockchain transactions are immutable and irreversible, users must carefully verify addresses before any operation. New transaction records should be treated with caution, and users should remain vigilant against risks.

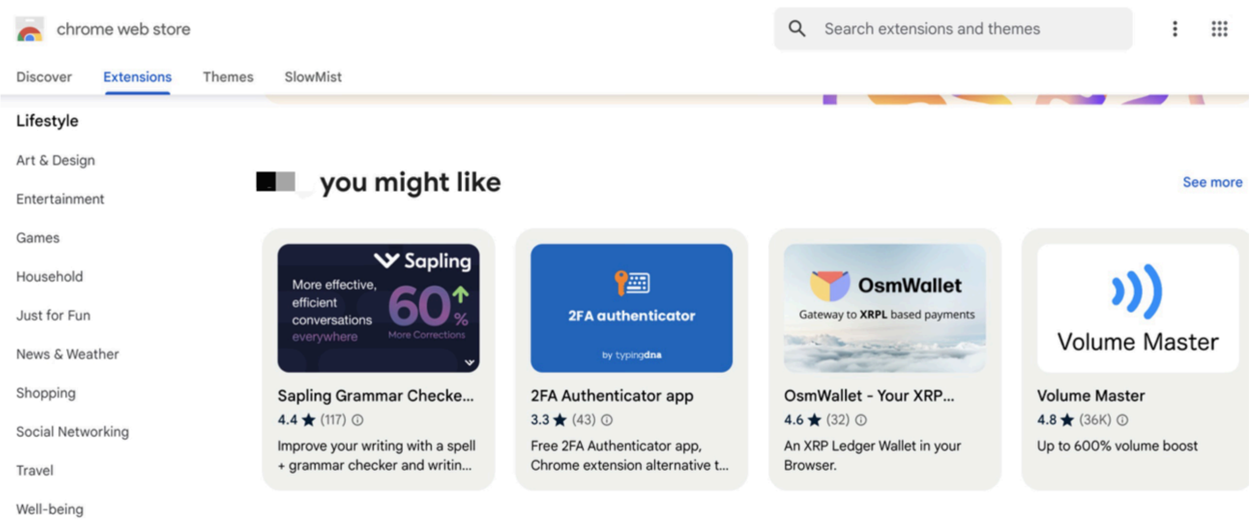
2.2.2 Malicious Browser Extensions

On March 1, 2024, a Twitter user reported anomalies in their account, resulting in a $1 million loss, although it did not attract public attention. In May, there were suspicions among netizens that the victim may have installed a highly rated malicious browser extension (this information has not been directly verified with the victim). The extension could steal all cookies from websites visited by users, and it was promoted by paying influential individuals. Since Google has already removed this malicious extension, investigations rely on historical data from snapshot information. During testing, suspicious malicious code was found embedded in the extension. In testing, cookies were sent to external servers, enabling attackers to obtain user authentication credentials and other information, conduct sim swap attacks on some trading websites, and steal users' cryptocurrency assets.



```
------WebKitFormBoundaryAUOLH1bG5arSBUsS
Content-Disposition: form-data; name="data"; filename="blob"
Content-Type: application/json

[{"domain":".google.com","expirationDate":1738218381.526747,"hostOnly":false,"httpOnly":false,"name":"_ga","path'
out","sameSite":"unspecified","secure":false,"session":false,"storeId":"0","value":"GA1.2-5.1292461332.170365838
e.com","expirationDate":1730949388.374267,"hostOnly":true,"httpOnly":true,"name":"_GRECAPTCHA","path":"/recaptcha
tion","secure":true,"session":false,"storeId":"0","value":[redacted]
3YC_f7m74ww"},{"domain":".google.com","expirationDate":1731207419.472168,"hostOnly":false,"httpOnly":true,"name":
y","[redacted]
```

Chrome Extensions (Chrome Extension) are plugins designed for Google Chrome to enhance browser functionality and optimize user experience. They are typically built using HTML, CSS, JavaScript, and other web technologies, often including essential components like the manifest.json configuration file, background scripts, content scripts, and user interface elements. Chrome extensions cover various browsing scenarios, including ad-blocking with uBlock Origin, privacy and security tools like LastPass, productivity tools such as Todoist, developer tools like React Developer Tools, and cryptocurrency tools like MetaMask, providing numerous conveniences for both work and personal life.



However, Chrome extensions once granted the necessary permissions for specific functionalities, can access sensitive user data such as cookies and authentication information. This becomes particularly apparent when dealing with malicious Chrome extensions, which can exploit these permissions to directly access and manipulate a user's browser environment and data. For instance, by leveraging broad permissions, malicious extensions can manipulate network requests, read and write page content, access browser storage, manipulate clipboard data, and even impersonate legitimate websites, thereby stealing user credentials and authentication information. If a malicious extension hijacks cookies, it could gain access to accounts, alter account settings, extract funds, or even engage in social engineering attacks impersonating the user. Faced with such risks, users may contemplate extreme measures like disconnecting from the internet or switching devices. However, there are more sensible strategies to mitigate these risks:

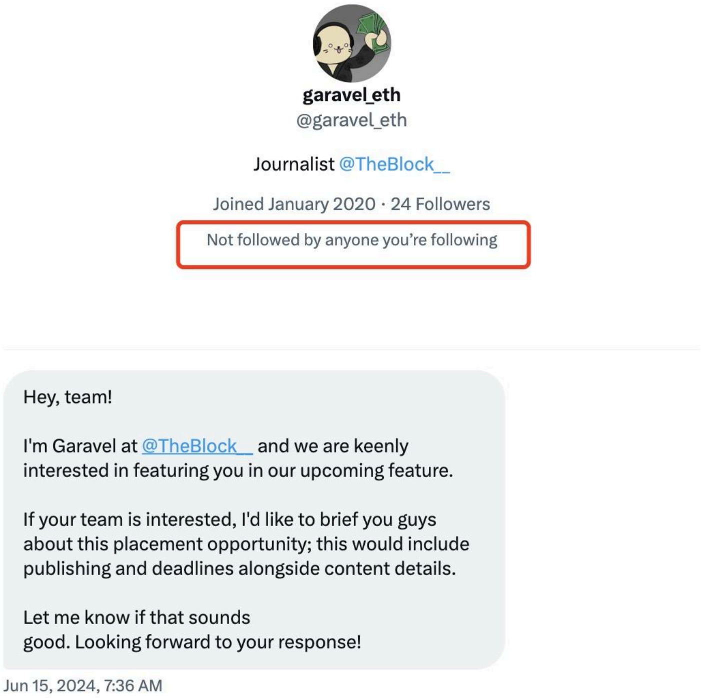
For individual users, it is advisable to install extensions only from trusted sources, use different browsers to isolate plugins and transaction funds, install antivirus software (e.g., Kaspersky, Bitdefender, AVG), regularly check devices for security, exercise caution when granting Chrome extension permissions to protect personal information and financial security. For trading platforms, enabling global two-factor authentication (2FA) and utilizing multiple verification methods such as SMS, email, Google Authenticator, and hardware tokens are recommended. It's crucial to promptly notify users of important account activities such as logins, password changes, and fund withdrawals and provide options for quickly freezing accounts in emergencies.

Additionally, employing machine learning and big data analytics to monitor user behavior, identify unusual transaction patterns, and detect suspicious activities such as frequent changes in account information or multiple failed login attempts can provide early warnings and restrictions. Educating users through various channels about security practices, emphasizing the risks associated with browser extensions, and promoting official browser plugins or extensions to enhance account security are also effective measures.

2.2.3 Malicious Trojan Programs

Malicious trojan programs are a frequent threat in the cryptocurrency realm. Attackers often disguise trojans as other types of programs or files to deceive users into downloading and installing them. Once installed on a user's computer or mobile device, these trojans operate in the background, carrying out various malicious activities.

For example, many scammers use bait such as "looking for freelance translators," "interviews with prominent media journalists," or posing as investors seeking collaboration to gain user trust. They encourage users to download what appears to be conferencing software for real-time translation. However, this "conference software" is actually a trojan program. Checking the domain information via Whois often reveals that the "official website" of such software was recently registered, and further investigation may uncover past malicious records associated with the domain's IP address. Once downloaded, this "conference software" scans files on the user's computer, filtering out files containing keywords like Wallet or Key, and uploads them to a server controlled by the attacker, aiming to steal cryptocurrency. Typically, these trojan files evade antivirus software, with online antivirus capable of analyzing files up to 50 MB in size, and PC-based antivirus up to 500 MB. Some trojan files are exceptionally large to avoid detection, and these trojans are often sold to criminals for around $100 per month, providing scammers with easy access.



garavel_eth
@garavel_eth

Journalist @TheBlock__

Joined January 2020 · 24 Followers

Not followed by anyone you're following

Hey, team!

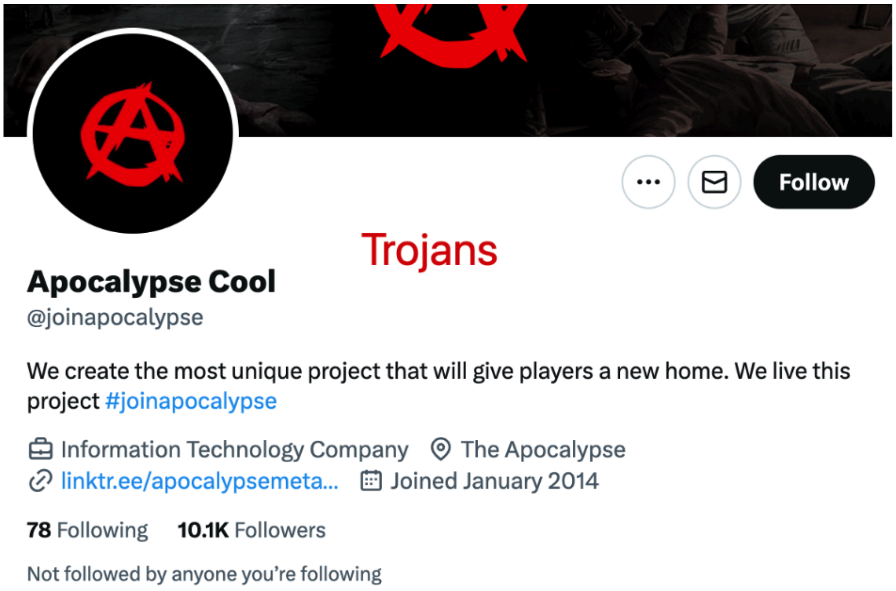
I'm Garavel at @TheBlock__ and we are keenly interested in featuring you in our upcoming feature.

If your team is interested, I'd like to brief you guys about this placement opportunity; this would include publishing and deadlines alongside content details.

Let me know if that sounds good. Looking forward to your response!

Jun 15, 2024, 7:36 AM

According to victims' reports, some scammers employ more sophisticated methods to lure users into downloading their phishing software, such as labeling it as "game testing." They set up realistic-looking websites and provide complete whitepapers to persuade users to download the "game" for an authentic experience of their "company's products." However, these "games" are also malicious programs. Accidentally downloading a trojan disguised as a blockchain game allows the trojan to stealthily steal everything on the user's computer, including wallet passwords, local files, and potentially sensitive personal information stored in browsers.



Trojans

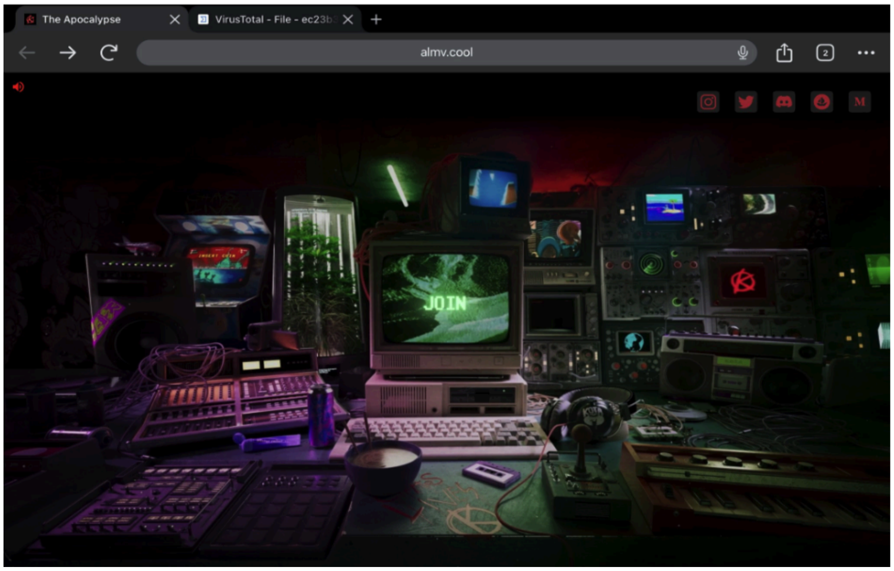
Apocalypse Cool
@joinapocalypse

We create the most unique project that will give players a new home. We live this project #joinapocalypse

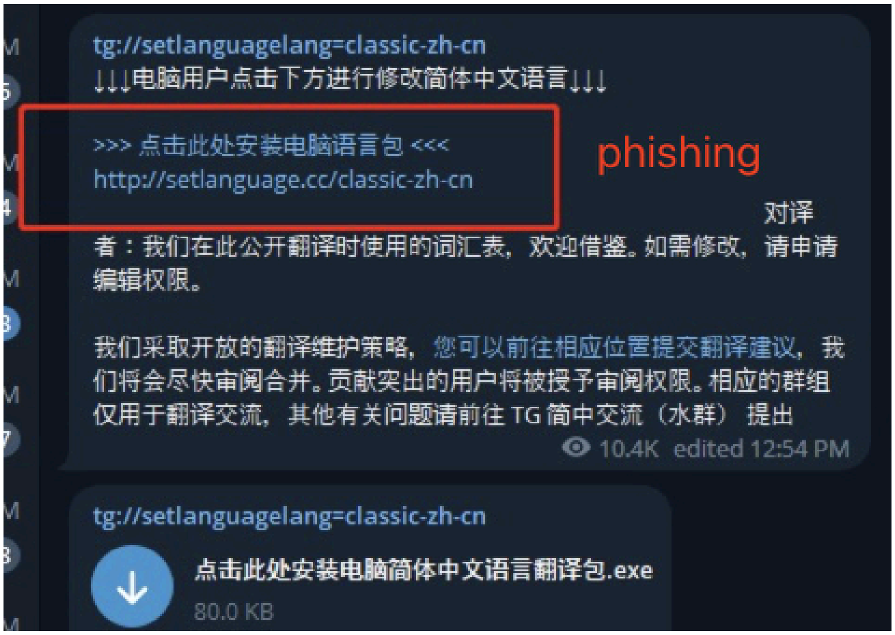
Information Technology Company · The Apocalypse
linktr.ee/apocalypsemeta... · Joined January 2014

78 Following · 10.1K Followers

Not followed by anyone you're following



Furthermore, the use of communication platforms like Telegram to spread trojans is becoming increasingly common. Many third-party localized apps harbor threats of phishing and background trojans. Casual usage can lead to virus or trojan attacks on computers. For instance, when victims receive wallet addresses from others for transaction purposes, infected devices alter the clipboard address during copy-paste operations to that of the attacker, causing funds to be transferred to the attacker's address and resulting in financial loss. Additionally, some trojan programs record user keystrokes to obtain passwords and private key information.



tg://setlanguagelang=classic-zh-cn
↓↓↓电脑用户点击下方进行修改简体中文语言↓↓↓

>>> 点击此处安装电脑语言包 <<<
http://setlanguage.cc/classic-zh-cn

phishing

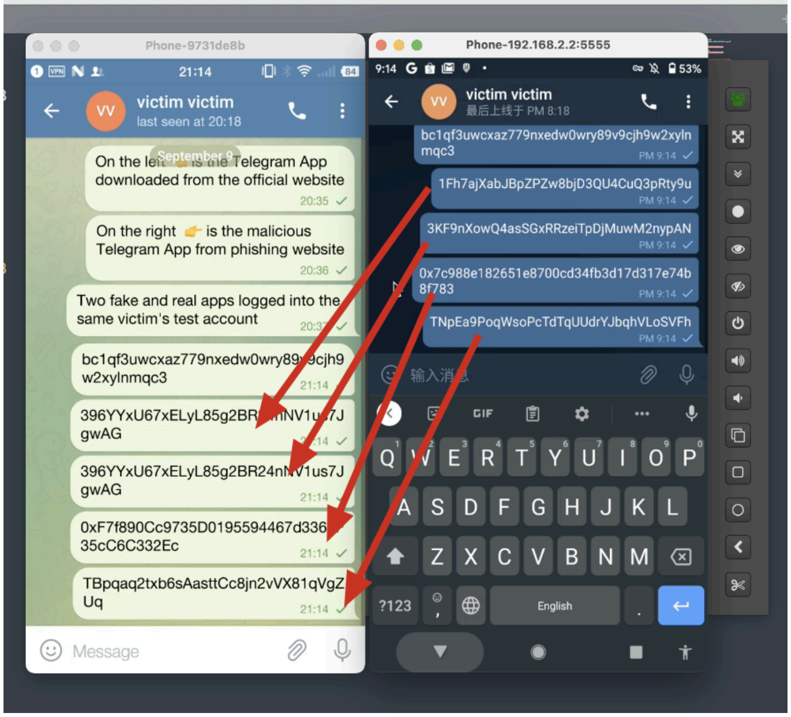
对译者：我们在此公开翻译时使用的词汇表，欢迎借鉴。如需修改，请申请编辑权限。

我们采取开放的翻译维护策略，您可以前往相应位置提交翻译建议，我们将会尽快审阅合并。贡献突出的用户将被授予审阅权限。相应的群组仅用于翻译交流，其他有关问题请前往 TG 简中交流（水群） 提出

10.4K edited 12:54 PM

tg://setlanguagelang=classic-zh-cn

点击此处安装电脑简体中文语言翻译包.exe
80.0 KB



Phone-9731de8b

victim victim
last seen at 20:18

September 9

On the left 👈 is the Telegram App downloaded from the official website 20:35 ✓

On the right 👉 is the malicious Telegram App from phishing website 20:36 ✓

Two fake and real apps logged into the same victim's test account 20:37 ✓

bc1qf3uwcxaz779nxedw0wry89[illegible]9cjh9w2xylnmqc3 21:14

396YYxU67xELyL85g2BR[illegible]nNV1u[illegible]7JgwAG 21:14 ✓

396YYxU67xELyL85g2BR24nN[illegible]V1us7JgwAG 21:14 ✓

0xF7f890Cc9735D0195594467d336[illegible]35cC6C332Ec 21:14 ✓

TBpqaq2txb6sAasttCc8jn2vVX81qVgZUq 21:14 ✓

Phone-192.168.2.2:5555

victim victim
最后上线于 PM 8:18

bc1qf3uwcxaz779nxedw0wry89v9cjh9w2xylnmqc3 PM 9:14 ✓

1Fh7ajXabJBpZPZw8bjD3QU4CuQ3pRty9u PM 9:14 ✓

3KF9nXowQ4asSGxRRzeiTpDjMuwM2nypAN PM 9:14 ✓

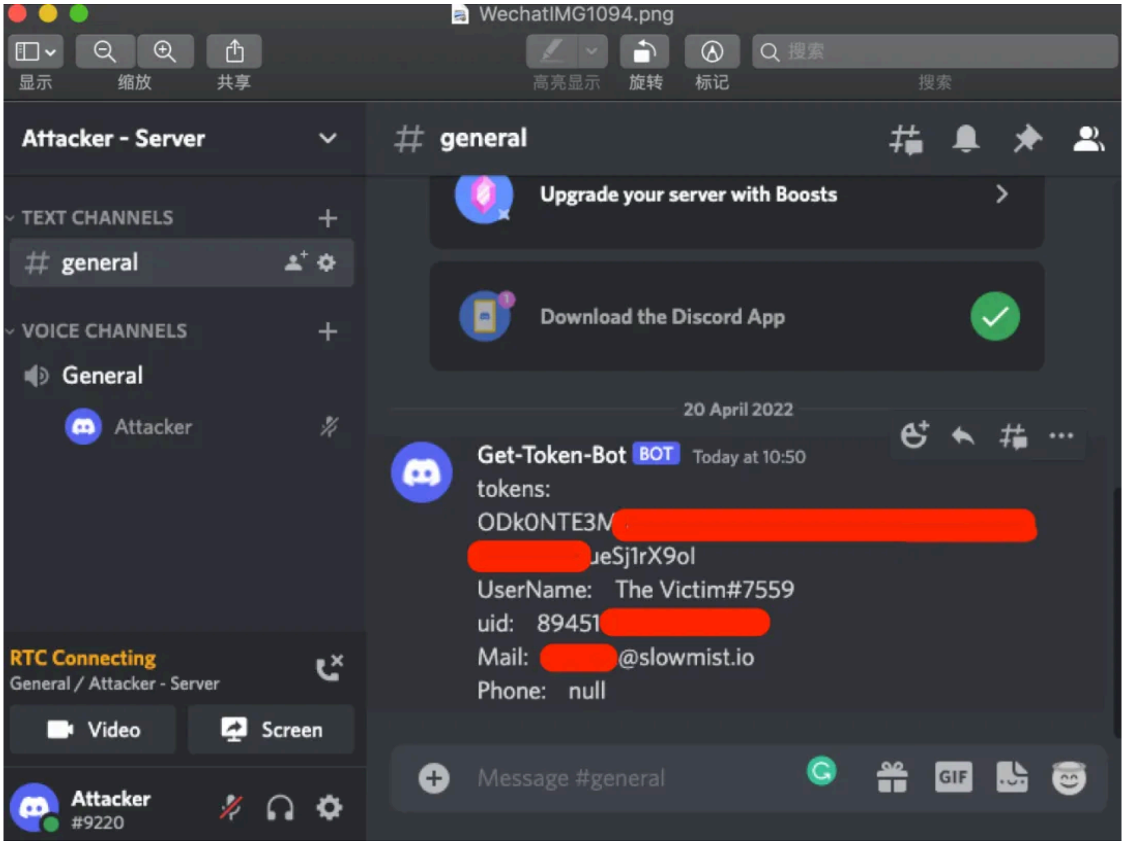
0x7c988e182651e8700cd34fb3d17d317e74b8f783 PM 9:14 ✓

TNpEa9PoqWsoPcTdTqUUdrYJbqhVLoSVFh PM 9:14 ✓

In case of a trojan attack, immediate actions include disconnecting from the internet to halt trojan activities, promptly transferring funds, updating permissions for all online accounts and applications, and downloading reputable antivirus software for scanning and removing any malicious programs lingering on your device. If necessary, consider resetting your system. To preempt trojan risks, proactive defensive measures include prioritizing security updates to keep your operating system and security software current, refraining from downloading files or programs of unknown origin, and avoiding clicking on suspicious emails or links. For managing substantial assets, consider using a hardware wallet as a more secure option. Regularly backing up and updating cryptocurrency wallets is also essential.

2.2.4 Malicious Bookmark Phishing

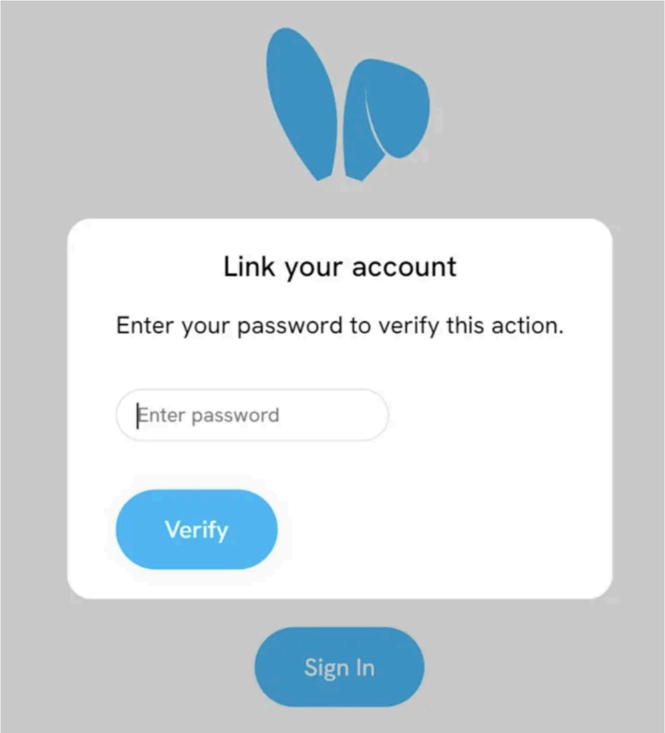
Modern browsers come equipped with built-in bookmark management, providing convenience. However, this convenience can also be exploited by hackers who carefully construct malicious phishing pages and add them to bookmarks. These pages often contain malicious JavaScript code. When you click on such a bookmark, it executes within the current browser tab's domain. For instance, when a Discord user clicks, malicious JavaScript code executes within the Discord domain, stealing Discord Tokens. If attackers obtain the project's Discord Token, they can automate takeover of the project's Discord account permissions, posting phishing links and causing user fund losses. Theoretically, browsers have protective measures like Same-Origin Policy, which should prevent responses on Discord pages unless actions originate from Discord. However, malicious bookmarks can bypass these restrictions, sending user Tokens and personal information to hacker channels, effectively disabling permissions.



20 April 2022

Get-Token-Bot BOT Today at 10:50
tokens:
ODkONTE3M[redacted]
[redacted]ueSj1rX9ol
UserName: The Victim#7559
uid: 89451[redacted]
Mail: [redacted]@slowmist.io
Phone: null

As an example, a victim on the decentralized social platform Friend.tech encountered a hacker posing as a well-known media journalist with tens of thousands of Twitter followers. The hacker contacted the victim (a KOL) under the guise of an interview and sent a phishing webpage disguised as a verification form after the interview. The victim filled out the form and clicked "Verify," only to encounter an error prompt on the page. The attacker then guided the victim to add the "Verify" link to bookmarks in Google Chrome, instructing them to open Friend.tech and click the bookmark. Following these steps, a dialog box requesting the victim's password appeared on the page. Ultimately, the victim's Friend.tech account and associated funds were stolen, resulting in a total loss of approximately 14.2 ETH.



Link your account

Enter your password to verify this action.

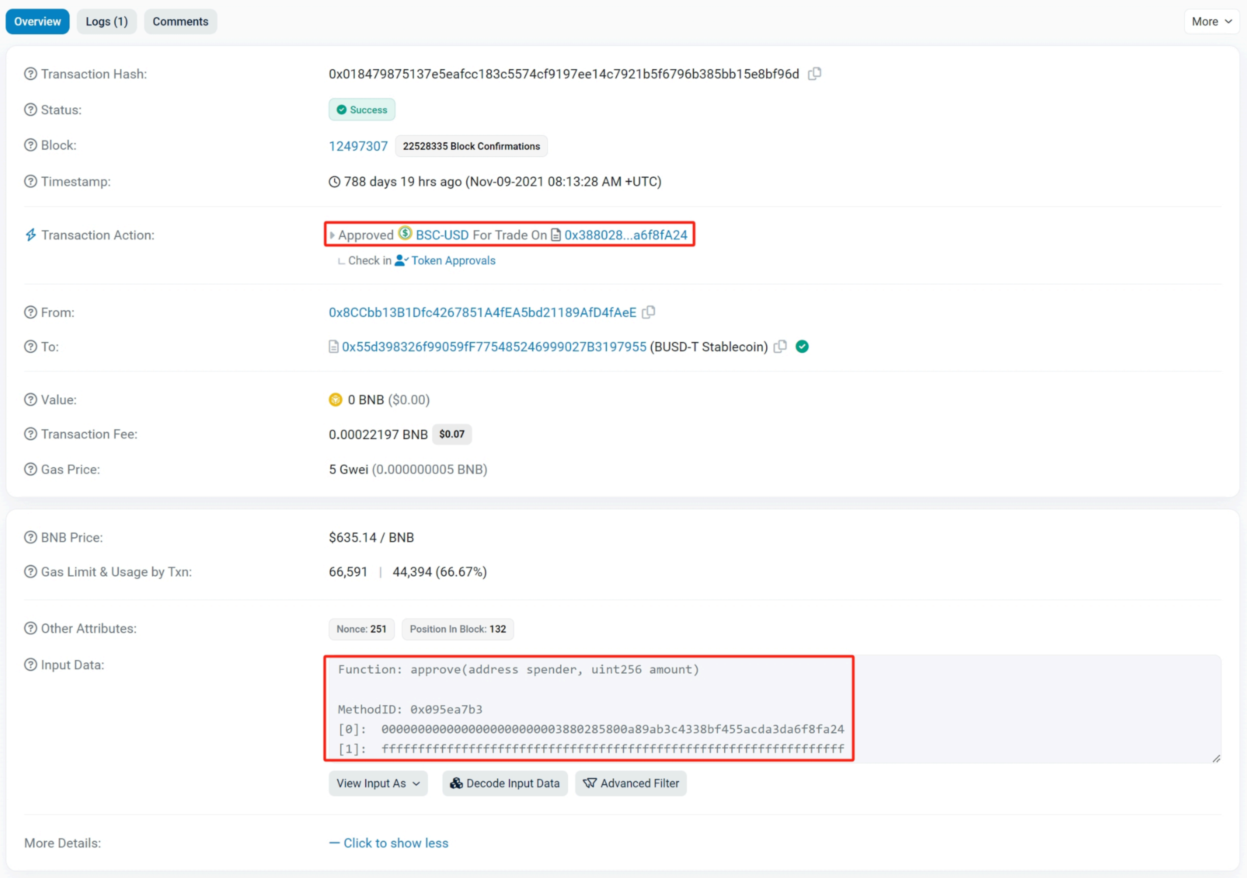
The victim promptly reported the theft and sought assistance. Upon tracking, we discovered the funds were transferred to a platform and immediately contacted the platform to initiate temporary freeze controls, requiring law enforcement intervention within 72 hours to continue freezing illicit funds. With collaborative efforts, the victim filed a report and engaged with law enforcement and prosecutors to secure an asset freeze order from the court. After three and a half months, the victim successfully reclaimed the stolen funds. This case holds significant importance, marking a milestone in Taiwan's judicial history as possibly the first case where illegal fund flows and cryptocurrency asset ownership were traced solely through blockchain analysis, aiding law enforcement in freezing and recovering funds for the victim.

As users, the key takeaway is that despite the appearance of many seemingly friendly and flexible extensions on the web, bookmarks do not block network requests. At the moment of manual triggering execution, it is essential to remain vigilant, as any added operation or code may potentially be malicious. Always maintain a skeptical approach toward everything.

2.2.5 Signature Authorization Phishing

Signature authorization is a vulnerable area for fund security, with "signature phishing" now a major threat to user asset safety. This section primarily discusses the three most common types of signature phishing methods:

Approve: Commonly found in ERC-20 token standards, Approve authorizes third parties (such as smart contracts) to spend a specified amount of tokens on behalf of the token holder. Users need to pre-authorize a certain amount of tokens for a smart contract, after which the contract can call the transferFrom function to transfer these tokens at any time. If a user inadvertently authorizes a malicious contract, these authorized tokens can be immediately transferred. It's important to note that traces of Approve authorizations can be seen in the victim's wallet address.



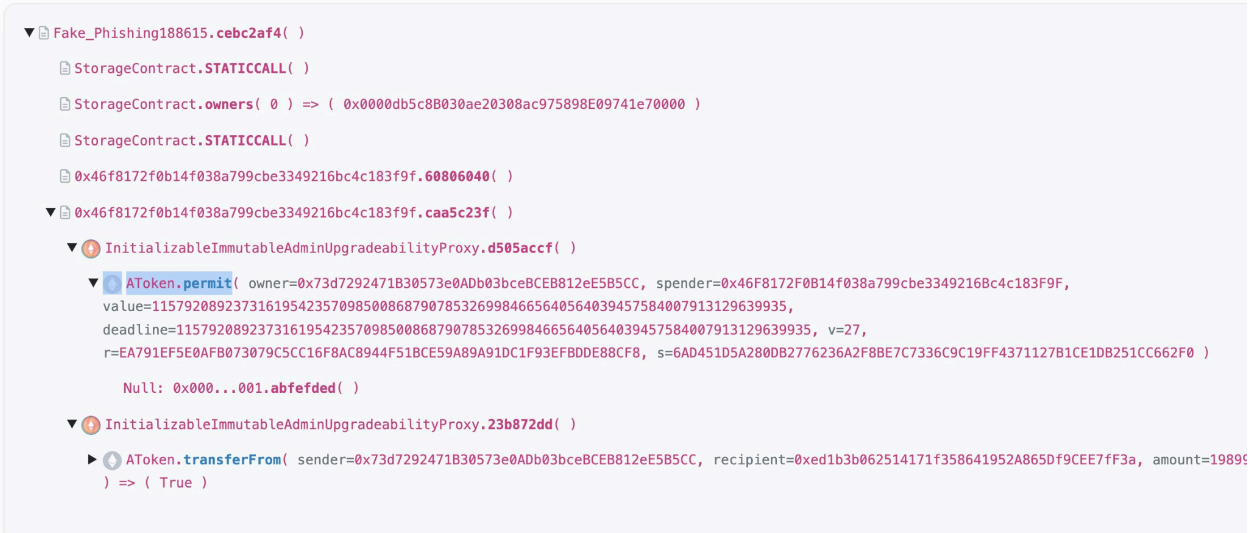
Transaction Hash:	0x018479875137e5eafcc183c5574cf9197ee14c7921b5f6796b385bb15e8bf96d
Status:	Success
Block:	12497307 22528335 Block Confirmations
Timestamp:	788 days 19 hrs ago (Nov-09-2021 08:13:28 AM +UTC)
Transaction Action:	Approved BSC-USD For Trade On 0x388028...a6f8fA24 Check in Token Approvals
From:	0x8CCbb13B1Dfc4267851A4fEA5bd21189AfD4fAeE
To:	0x55d398326f99059fF775485246999027B3197955 (BUSD-T Stablecoin)
Value:	0 BNB ($0.00)
Transaction Fee:	0.00022197 BNB $0.07
Gas Price:	5 Gwei (0.000000005 BNB)
BNB Price:	$635.14 / BNB
Gas Limit & Usage by Txn:	66,591 | 44,394 (66.67%)
Other Attributes:	Nonce: 251 Position In Block: 132

Input Data:

```
Function: approve(address spender, uint256 amount)

MethodID: 0x095ea7b3
[0]:  0000000000000000000000003880285800a89ab3c4338bf455acda3da6f8fa24
[1]:  ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
```

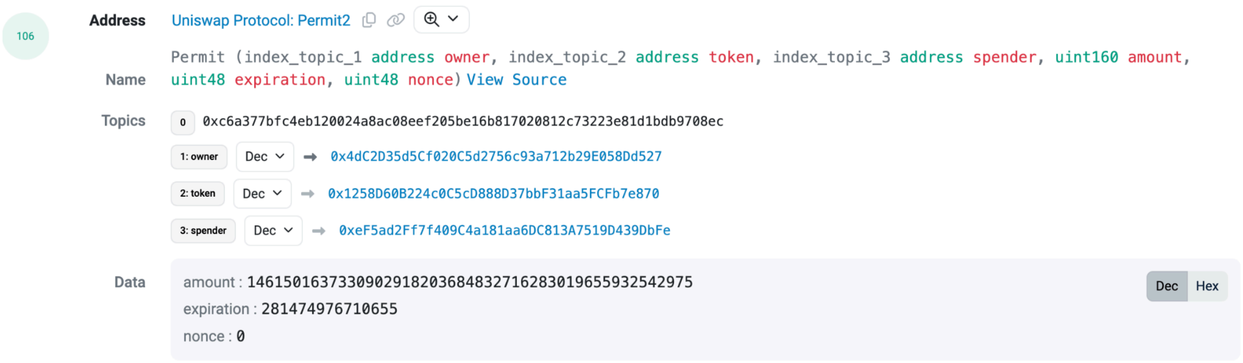
More Details: — Click to show less

Permit: Introduced as an extension authorization method based on the ERC-20 standard, Permit authorizes third parties to spend tokens using message signatures rather than directly invoking smart contracts. Simply put, users can approve others to transfer their tokens via a signature. Hackers can exploit this method for attacks, such as replacing the wallet login button on a phishing website with Permit, making it easy to obtain the user's signature.



```
▼ Fake_Phishing188615.cebc2af4( )
    StorageContract.STATICCALL( )
    StorageContract.owners( 0 ) => ( 0x0000db5c8B030ae20308ac975898E09741e70000 )
    StorageContract.STATICCALL( )
    0x46f8172f0b14f038a799cbe3349216bc4c183f9f.60806040( )
  ▼ 0x46f8172f0b14f038a799cbe3349216bc4c183f9f.caa5c23f( )
    ▼ InitializableImmutableAdminUpgradeabilityProxy.d505accf( )
      ▼ AToken.permit( owner=0x73d7292471B30573e0ADb03bceBCEB812eE5B5CC, spender=0x46F8172F0B14f038a799cbe3349216Bc4c183F9F,
        value=115792089237316195423570985008687907853269984665640564039457584007913129639935,
        deadline=115792089237316195423570985008687907853269984665640564039457584007913129639935, v=27,
        r=EA791EF5E0AFB073079C5CC16F8AC8944F51BCE59A89A91DC1F93EFBDDE88CF8, s=6AD451D5A280DB2776236A2F8BE7C7336C9C19FF4371127B1CE1DB251CC662F0 )
          Null: 0x000...001.abfefded( )
    ▼ InitializableImmutableAdminUpgradeabilityProxy.23b872dd( )
      ▶ AToken.transferFrom( sender=0x73d7292471B30573e0ADb03bceBCEB812eE5B5CC, recipient=0xed1b3b062514171f358641952A865Df9CEE7fF3a, amount=1989
        ) => ( True )
```

Permit2: Not a standard ERC-20 feature, Permit2 was introduced by Uniswap for user convenience. This feature allows Uniswap users to pay gas fees only once during use. However, if you've used Uniswap and granted unlimited allowance to a contract, you may become a target for Permit2 phishing attacks.



```
Address  Uniswap Protocol: Permit2
Name     Permit (index_topic_1 address owner, index_topic_2 address token, index_topic_3 address spender, uint160 amount,
         uint48 expiration, uint48 nonce) View Source
Topics   0  0xc6a377bfc4eb120024a8ac08eef205be16b817020812c73223e81d1bdb9708ec
         1: owner    Dec → 0x4dC2D35d5Cf020C5d2756c93a712b29E058Dd527
         2: token    Dec → 0x1258D60B224c0C5cD888D37bbF31aa5FCFb7e870
         3: spender  Dec → 0xeF5ad2Ff7f409C4a181aa6DC813A7519D439DbFe
Data     amount : 1461501637330902918203684832716283019655932542975
         expiration : 281474976710655
         nonce : 0
```

Permit and Permit2 involve offline signature methods where the victim's wallet address does not pay gas fees, and the phishing wallet address provides on-chain authorization operations. Therefore, traces of these signature authorizations can only be seen in the phisher's wallet address.

Given the severity and complexity of signature phishing attacks, we recommend users remain vigilant during the signature process to ensure the security of each signing operation. Additionally, regularly check your wallet address for authorization traces and use tools like Revoke.cash and ScamSniffer periodically to detect any abnormal authorizations promptly and cancel them to prevent fund losses.

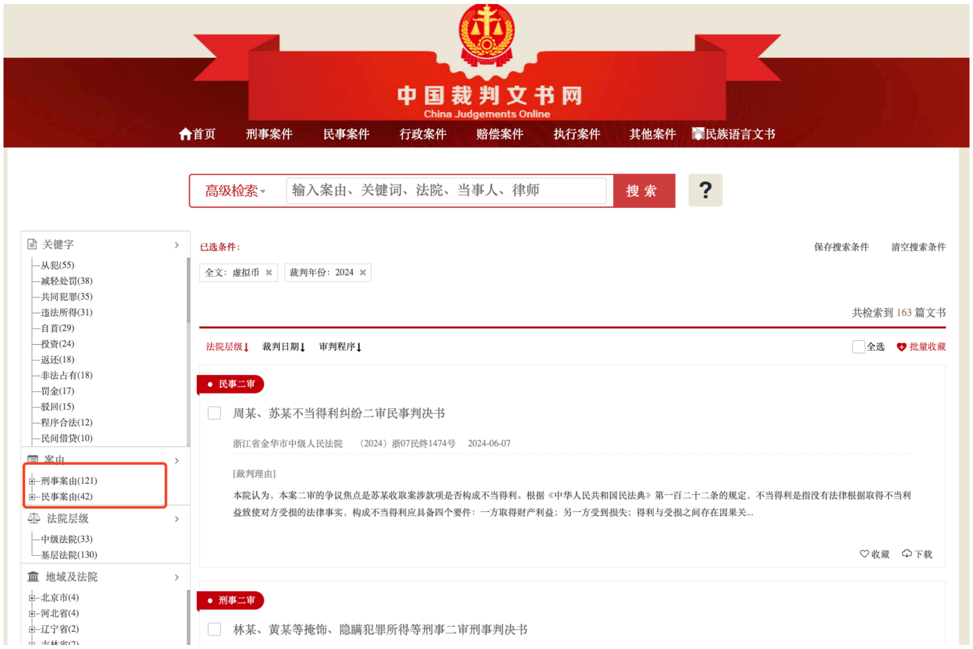
III. Anti-Money Laundering Landscape

3.1 Anti-Money Laundering and Regulatory Trends

This section highlights significant developments in Anti-Money Laundering (AML) and regulatory dynamics within the cryptocurrency sector.

3.1.1 Enforcement in China

In the first half of 2024, mainland Chinese courts issued a total of 163 judgments related to virtual currencies, comprising 121 criminal judgments and 42 civil judgments.



关键字
- 从犯(55)
- 减轻处罚(38)
- 共同犯罪(35)
- 违法所得(31)
- 自首(29)
- 投资(24)
- 返还(18)
- 非法占有(18)
- 罚金(17)
- 驳回(15)
- 程序合法(12)
- 民间借贷(10)

案由
- 刑事案由(121)
- 民事案由(42)

法院层级
- 中级法院(33)
- 基层法院(130)

地域及法院
- 北京市(4)
- 河北省(4)
- 辽宁省(2)

已选条件：

全文：虚拟币 ✖ 裁判年份：2024 ✖

共检索到 163 篇文书

● 民事二审

□ 周某、苏某不当得利纠纷二审民事判决书

浙江省金华市中级人民法院 （2024）浙07民终1474号 2024-06-07

[裁判理由]

本院认为，本案二审的争议焦点是苏某收取案涉款项是否构成不当得利。根据《中华人民共和国民法典》第一百二十二条的规定，不当得利是指没有法律根据取得不当利益致使对方受损的法律事实，构成不当得利应具备四个要件：一方取得财产利益；另一方受到损失；得利与受损之间存在因果关..．

● 刑事二审

□ 林某、黄某等掩饰、隐瞒犯罪所得等刑事二审刑事判决书

3.1.2 Hong Kong in China

As an important hub for global financial and technological innovation, Hong Kong's policy trends in the field of virtual assets have a far-reaching impact on the entire industry. In 2024, Hong Kong's virtual asset regulation ushered in a new stage of full compliance.

On February 8, the Hong Kong government launched a public consultation on legislative proposals to establish a licensing system for virtual asset over-the-counter (OTC) service providers. For example, according to the legislative proposal, all virtual asset OTC services, whether through offline physical stores (including ATMs) or online website services, must obtain relevant licenses issued by Hong Kong Customs.

On March 12, the Hong Kong Monetary Authority launched a regulatory sandbox for the development and issuance of stablecoins, following a discussion document that began in 2022. The sandbox aims to encourage the safe development of stablecoins in a controlled environment, and regulatory decisions can be iterated as needed.

On April 15, the Hong Kong subsidiaries of China Public Fund, Bosera International, China Asset Management (Hong Kong), and Harvest International obtained in-principle approval from the Hong Kong Securities Regulatory Commission for the issuance of virtual asset spot ETF products.

On April 30, six of the first batch of virtual asset spot ETFs issued in Hong Kong officially rang the bell and were listed on the Hong Kong Stock Exchange and opened for trading, becoming the first batch of virtual asset spot ETFs in Asia.

3.1.3 Singapore

On January 18, a spokesperson for the Monetary Authority of Singapore said that collective investment schemes (CIS) available to retail investors in Singapore are regulated by the Securities and Futures Act and cover ETFs. The types of assets they can invest in are limited. Currently, Bitcoin and other digital payment tokens (cryptocurrencies) (DPTs) are not eligible assets for retail CISs.

On April 2, the Monetary Authority of Singapore (MAS) amended the Payment Services Act (PS Act) and its subsidiary legislation, expanding the scope of payment services regulated by MAS and imposing user protection and financial stability-related requirements on digital payment token (DPT) service providers. The amendments include: regulating DPT custody services, facilitating transmission and exchange between DPTs, and standardizing cross-border remittance services; empowering MAS to impose requirements on DPT service providers related to anti-money laundering, counter-terrorism financing, user protection and financial stability; and setting up transitional arrangements requiring relevant entities to notify MAS and submit license applications within the prescribed time.

3.1.4 US Regulatory

- **SEC**

1. In the Matter of TradeStation Crypto, Inc.: The SEC charged TradeStation Crypto, Inc., a company based in Plantation, Florida, for failing to register the offer and sale of a crypto lending product. This product allowed U.S. investors to deposit or purchase crypto assets in exchange for

promised interest payments. TradeStation agreed to pay a $1.5 million penalty to settle the charges, reflecting the SEC's commitment to regulating crypto lending products.

2. SEC v. Sewell and Rockwell Capital Management LLC: Brian Sewell and his company, Rockwell Capital Management, settled fraud charges related to a scheme targeting students of Sewell's online crypto trading course, the American Bitcoin Academy. The fraudulent scheme cost 15 students $1.2 million, illustrating the SEC's efforts to protect educational settings from fraudulent investment schemes.

3. SEC v. Lee, et al.: Xue Lee (aka Sam Lee) and Brenda Chunga (aka Bitcoin Beautee) were charged for their involvement in the fraudulent crypto asset pyramid scheme HyperFund, which raised over $1.7 billion from investors worldwide. This case highlights the SEC's actions against large-scale, international frauds that exploit investors' trust and promise unrealistic returns.

4. Bitcoin Spot ETF: On January 10, 2024, the SEC approved the listing and trading of several spot bitcoin exchange-traded product (ETP) shares, following a court ruling that criticized previous disapprovals. Chair Gary Gensler emphasized that this approval is limited to bitcoin ETPs, ensuring they provide full disclosure and are traded on regulated exchanges designed to prevent fraud. The SEC will enforce existing investor protection standards and closely monitor compliance. Gensler also warned about the speculative and risky nature of bitcoin, advising investors to remain cautious.

- **OFAC Sanctions**

1. Treasury Sanctions Russian Entities for Sanctions Evasion
On March 25, 2024, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned thirteen entities and two individuals for aiding the evasion of U.S. sanctions through virtual asset services and technology procurement in Russia. This includes five entities controlled by previously designated persons. These designations follow the G7's February commitment to counter sanctions evasion and target companies supporting Russia's financial infrastructure amid its war against Ukraine. Notably, Moscow-based fintech companies such as B-Crypto, Masterchain, and Laitkhaus, along with others, were designated for their roles in facilitating

transactions for Russian financial institutions. The sanctions block all U.S.-based property of the designated persons and prohibit U.S. transactions with them. Additionally, foreign financial institutions aiding Russia's military-industrial base face potential sanctions. This action aims to curb Russia’s use of alternative payment mechanisms and virtual assets to circumvent sanctions and fund its military activities.

2. U.S. Targets Russia-Based LockBit Ransomware Affiliates
On February 20, 2024, the United States sanctioned affiliates of the Russia-based LockBit ransomware group, adding several individuals to the OFAC's Specially Designated Nationals (SDN) List. Key figures include Ivan Gennadievich Kondratiev, known by various aliases and linked to multiple digital currency addresses, and Artur Ravilevich Sungatov, also associated with several email addresses and digital currency addresses. These sanctions are part of the ongoing efforts to address cyber threats and enforce Ukraine-/Russia-related sanctions regulations.

3. U.S. Sanctions 911 S5 Botnet Cyber Crime Network
On May 28, 2024, the United States sanctioned a cybercrime network associated with the 911 S5 Botnet, adding several individuals and entities to OFAC's Specially Designated Nationals (SDN) List. Key figures include Liu Jingping and Wang Yunhe, both holding multiple digital currency addresses and associated with various locations in Singapore, Thailand, and China. Entities like Lily Suites Company Limited, Spicy Code Company Limited, and Tulip Biz Pattaya Group Company Limited were also designated. These actions are part of broader efforts to combat cybercrime and enforce sanctions regulations.

3.1.5 European Parliament

- **EU**

On April 24, 2024, the European Parliament passed new laws to strengthen the fight against money laundering and terrorist financing. Key measures include: Public access to beneficial ownership registries with data from the past five years. An EU-wide limit of EUR 10,000 on cash payments. Enhanced due diligence for financial entities and football clubs from 2029. A new authority, AMLA, based in Frankfurt, to oversee high-risk entities and ensure compliance. These laws aim to improve transparency, empower Financial Intelligence Units, and enforce stricter supervision on financial transactions.

3.1.6 Middle East

- **Türkiye**

On June 27, 2024, the Turkish Parliament passed a bill imposing strict regulations on crypto assets. Unauthorized crypto service providers will face imprisonment of 3 to 5 years. The Capital Markets Board (SPK) will oversee the authorization and regulation of these providers, ensuring compliance with set criteria. Severe penalties include up to 22 years in prison for embezzlement or misuse of resources. Platforms must adhere to transparent and fair market practices, and maintain secure records of transactions. Approval from the Banking Regulation and Supervision Agency (BDDK) is required for bank-related activities.

In summary, due to the complexity of cryptocurrency itself, regulatory policy has become a complex discussion involving multiple aspects such as financial stability, consumer protection, and anti-money laundering. As the cryptocurrency market continues to develop, a sound regulatory framework and international cooperation are becoming increasingly important in addressing its challenges.

3.2 Anti-Money Laundering in Security Incidents

3.2.1 Frozen Funds

Tether: In the first half of 2024, a total of 374 ETH addresses were blocked, resulting in the freezing of USDT-ERC20 assets on these addresses, rendering them non-transferable.

Circle: In the first half of 2024, a total of 28 ETH addresses were blocked, leading to the freezing of USDC-ERC20 funds on these addresses, making them non-transferable.

With the strong support of InMist Intelligence Network partners, SlowMist assisted customers, partners and public hacking incidents in freezing funds of approximately $24.39 million in the first half of 2024.

3.2.2 Recovered Funds

In the first half of 2024, there were 16 major incidents where victims were able to fully or partially recover their stolen funds. The total amount of stolen funds in these incidents was approximately $113 million, with nearly $98.64 million being returned, accounting for 87.3% of the stolen funds.

3.3 Profile and Activities of Hacker Groups

3.3.1 Lazarus Group

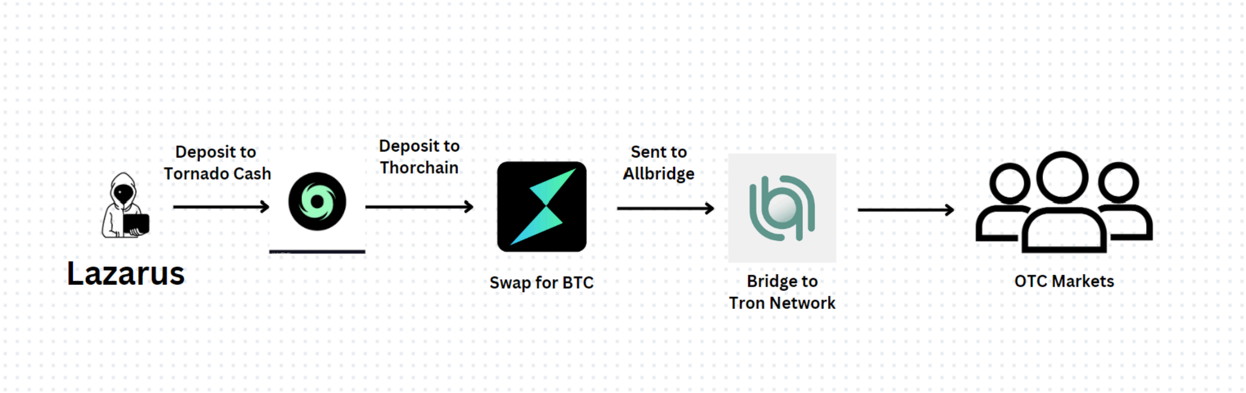
In 2024, the notorious North Korean hacking group Lazarus continued to be a major player in cryptocurrency-related money laundering activities. According to the latest statistics, Lazarus was responsible for the majority of funds being funneled into Tornado Cash, a well-known cryptocurrency mixing service.

- **Modus Operandi**

After depositing substantial amounts into Tornado Cash to obscure the origin of their funds, Lazarus employed a multi-layered mixing strategy to further evade detection. Here is a detailed example of one of their methods, which often involves targeting BTC for its vast liquidity pool, facilitating easier laundering of funds.

1. Initial Mixing in Tornado Cash: Funds were first deposited into Tornado Cash, where they were mixed with other users' funds to break the transaction trail and anonymize the origins.
2. Conversion via Thorchain: The laundered funds were then sent to Thorchain, a decentralized cross-chain liquidity protocol, where they were converted from Ethereum (ETH) to Bitcoin (BTC). This cross-chain activity added another layer of obfuscation.
3. Distribution Across Addresses: The converted Bitcoin was dispersed to various addresses to further complicate the transaction history and spread out the funds.
4. Bridging to TRON: The funds were then bridged to the TRON blockchain, taking advantage of TRON's decentralized finance (DeFi) ecosystem to further mix the assets and exploit the lower regulatory scrutiny.

5. Use of Over-the-Counter (OTC) Methods: Finally, the laundered funds were laundered through over-the-counter (OTC) trading methods, allowing the criminals to convert their digital assets into fiat currencies or other cryptocurrencies, reducing KYC exposure.



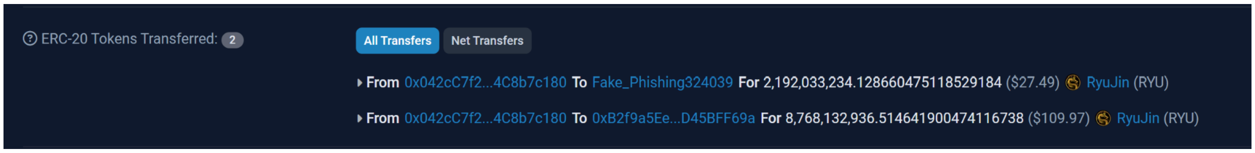
- **New Methods of Laundering**

With the daily development of new protocols, we are witnessing increasingly sophisticated laundering techniques employed by the infamous Lazarus Group. Their sophisticated modus operandi involves multi-layered mixing strategies and leveraging various blockchain technologies, including cross-chain swaps and decentralized exchanges. Further complicating our investigations, Lazarus Group has started leveraging the tBTC protocol to transfer funds to Ethereum, presenting significant challenges for regulators and financial institutions in tracking and intercepting illicit transactions.

3.3.2 Drainers

Drainer Services, or Draining-as-a-Service (DaaS), are illegal operations that provide the tools and infrastructure needed to steal cryptocurrency from victims' wallets through phishing attacks. These services, like Pink Drainer and Inferno Drainer, supply comprehensive phishing kits and operate on a commission basis, taking a cut of the stolen funds. While individual services may shut down due to financial goals or law enforcement pressure, new services constantly emerge, keeping the threat alive for the crypto community.

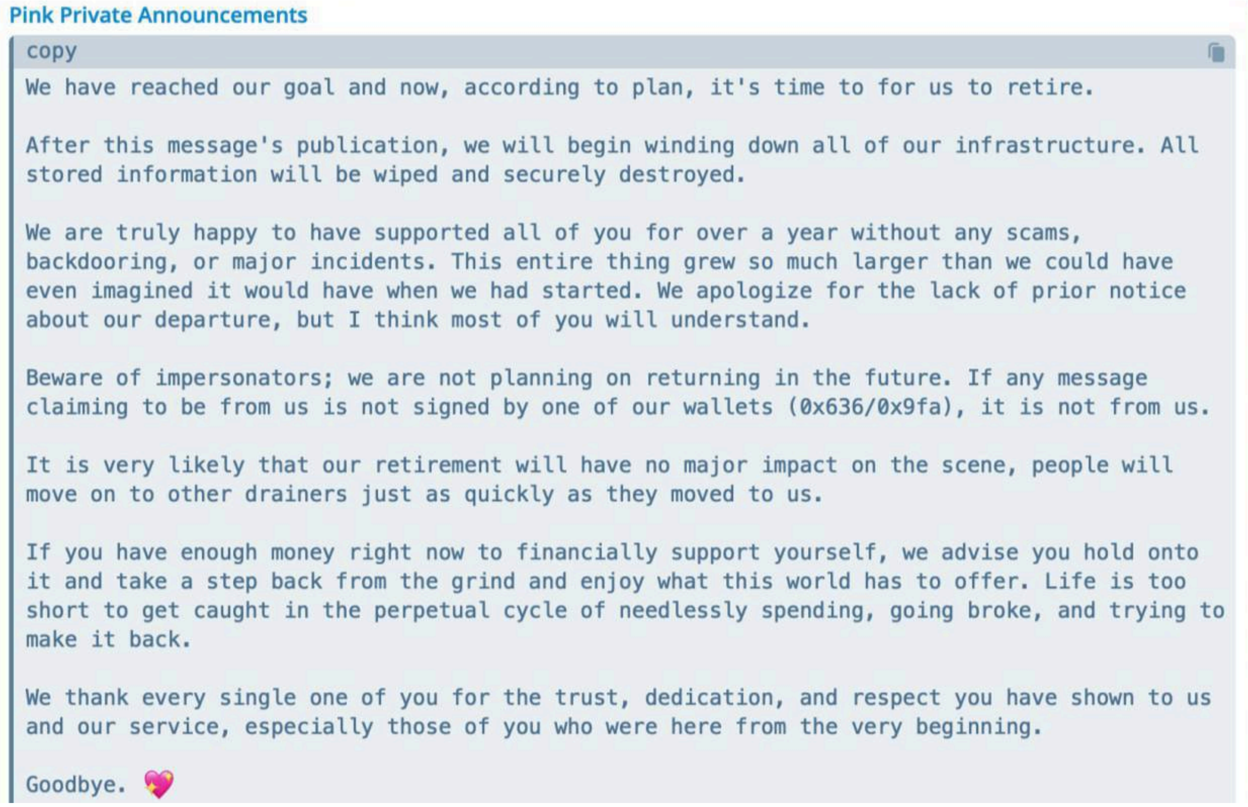
An effective way to determine if you have been a victim of a drainer service is by examining your transfers. Typically, a portion of your funds will be divided between two addresses. The smaller amount is usually paid to the drainer service, while the larger sum is sent to the scammer's address.



ERC-20 Tokens Transferred: 2

- From 0x042cC7f2...4C8b7c180 To Fake_Phishing324039 For 2,192,033,234.128660475118529184 ($27.49) RyuJin (RYU)
- From 0x042cC7f2...4C8b7c180 To 0xB2f9a5Ee...D45BFF69a For 8,768,132,936.514641900474116738 ($109.97) RyuJin (RYU)

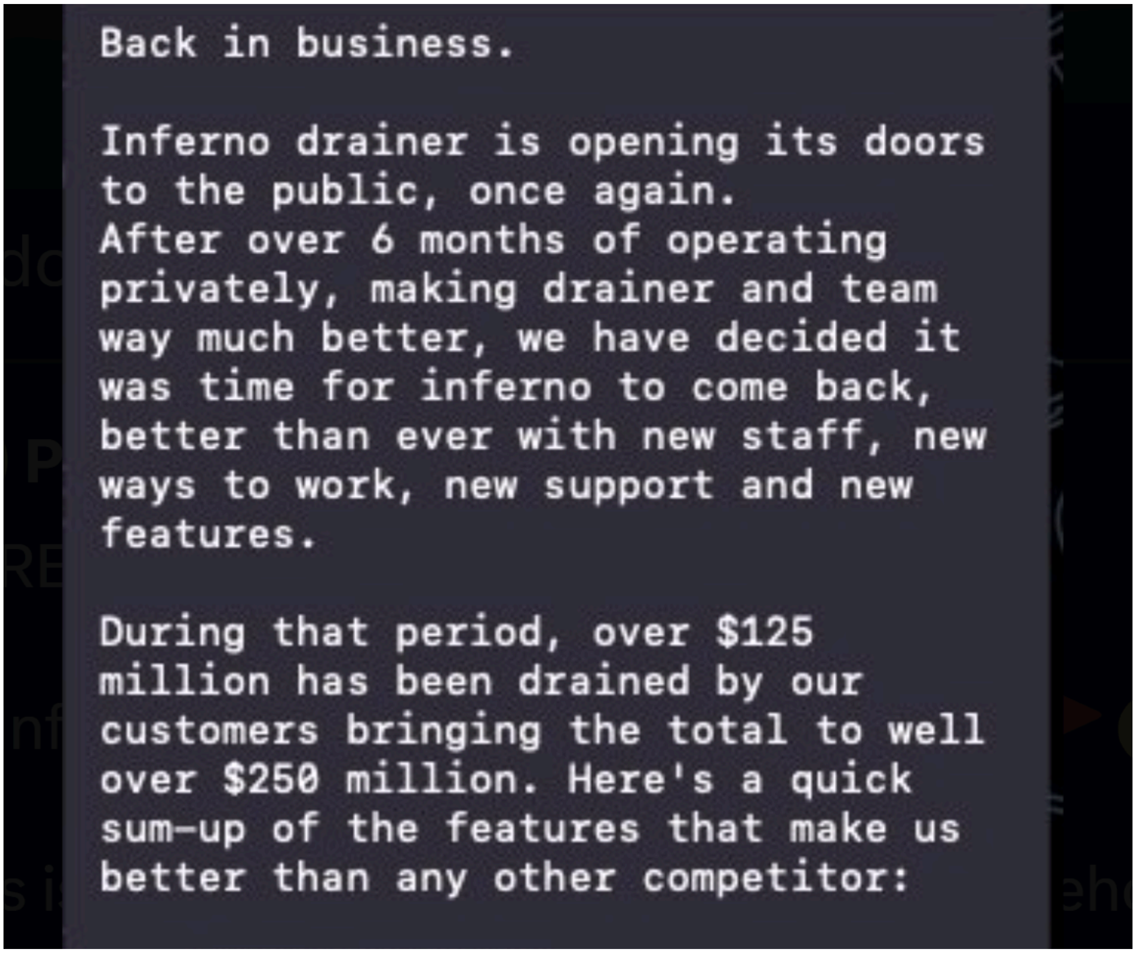
1. Pink Drainer: Pink Drainer was a notorious crypto wallet-draining service that recently announced its retirement after helping to steal over $85 million from more than 21,000 victims. It operated by providing a toolkit that scammers used to drain victims' wallets by tricking them into signing malicious contracts. The service shut down in mid-2024, claiming to have achieved its objectives and promising to securely destroy all stored information to prevent further use.



Pink Private Announcements

```
We have reached our goal and now, according to plan, it's time to for us to retire.

After this message's publication, we will begin winding down all of our infrastructure. All
stored information will be wiped and securely destroyed.

We are truly happy to have supported all of you for over a year without any scams,
backdooring, or major incidents. This entire thing grew so much larger than we could have
even imagined it would have when we had started. We apologize for the lack of prior notice
about our departure, but I think most of you will understand.

Beware of impersonators; we are not planning on returning in the future. If any message
claiming to be from us is not signed by one of our wallets (0x636/0x9fa), it is not from us.

It is very likely that our retirement will have no major impact on the scene, people will
move on to other drainers just as quickly as they moved to us.

If you have enough money right now to financially support yourself, we advise you hold onto
it and take a step back from the grind and enjoy what this world has to offer. Life is too
short to get caught in the perpetual cycle of needlessly spending, going broke, and trying to
make it back.

We thank every single one of you for the trust, dedication, and respect you have shown to us
and our service, especially those of you who were here from the very beginning.

Goodbye. 💖
```

2. Inferno Drainer: This service was another prominent player in the crypto wallet-draining scene, responsible for stealing over $200 million before it ceased operations in late 2023. It operates very similar to Pink Drainer and recently announced it’s coming out of retirement after Pink Drainer announced it was retiring.

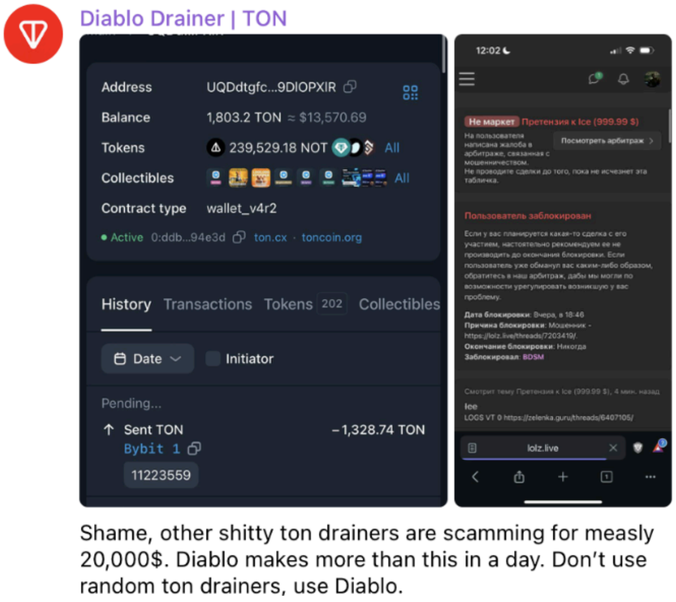


Back in business.

Inferno drainer is opening its doors to the public, once again.
After over 6 months of operating privately, making drainer and team way much better, we have decided it was time for inferno to come back, better than ever with new staff, new ways to work, new support and new features.

During that period, over $125 million has been drained by our customers bringing the total to well over $250 million. Here's a quick sum-up of the features that make us better than any other competitor:

3. Diablo Drainer: While most drainer focus on EVM chains, due to the rise in popularity on the TON blockchain, we’ve recently seens in increase in the Diablo drainer targeting users on the TON network. These services typically use similar phishing tactics and malicious contract signatures to drain crypto wallets, and they often advertise in underground forums or encrypted messaging channels like Telegram.



Diablo Drainer | TON

Address UQDdtgfc...9DIOPXIR
Balance 1,803.2 TON ≈ $13,570.69
Tokens 239,529.18 NOT All
Collectibles All
Contract type wallet_v4r2
● Active 0:ddb...94e3d ton.cx · toncoin.org

Pending...
↑ Sent TON −1,328.74 TON
Bybit 1
11223559

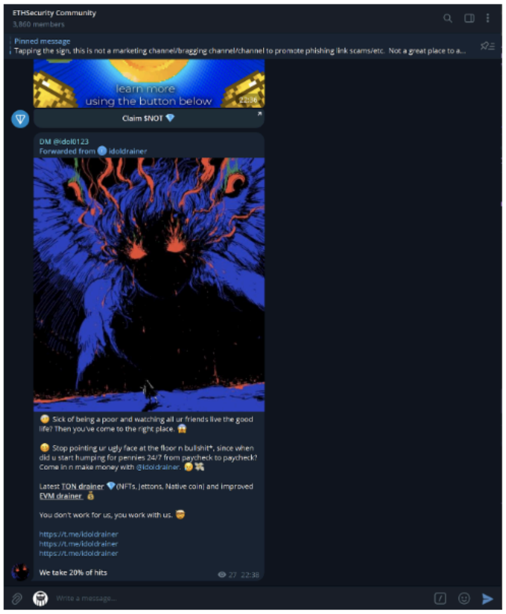
Не маркет Претензия к Ice (999.99 $)
На пользователя написана жалоба в арбитраже, связанная с мошенничеством.
Не проводите сделки до того, пока не исчезнет эта табличка.

Пользователь заблокирован
Если у вас планируется какая-то сделка с его участием, настоятельно рекомендуем ее не производить до окончания блокировки. Если пользователь уже обманул вас каким-либо образом, обратитесь в наш арбитраж, дабы мы могли по возможности урегулировать возникшую у вас проблему.

Дата блокировки: Вчера, в 18:46
Причина блокировки: Мошенник - https://lolz.live/threads/7203419/.
Окончание блокировки: Никогда
Заблокировал: BDSM

Смотрит тему Претензия к Ice (999.99 $), 4 мин. назад
Ice
LOGS VT 0 https://zelenka.guru/threads/6407105/

Shame, other shitty ton drainers are scamming for measly 20,000$. Diablo makes more than this in a day. Don't use random ton drainers, use Diablo.



ETHSecurity Community
3,860 members

Pinned message
Tapping the sign, this is not a marketing channel/bragging channel/channel to promote phishing link scams/etc. Not a great place to a...

DM @idol0123
Forwarded from idoldrainer

Sick of being a poor and watching all ur friends live the good life? Then you've come to the right place.

Stop pointing ur ugly face at the floor n bullshit*, since when did u start humping for pennies 24/7 from paycheck to paycheck? Come in n make money with @idoldrainer.

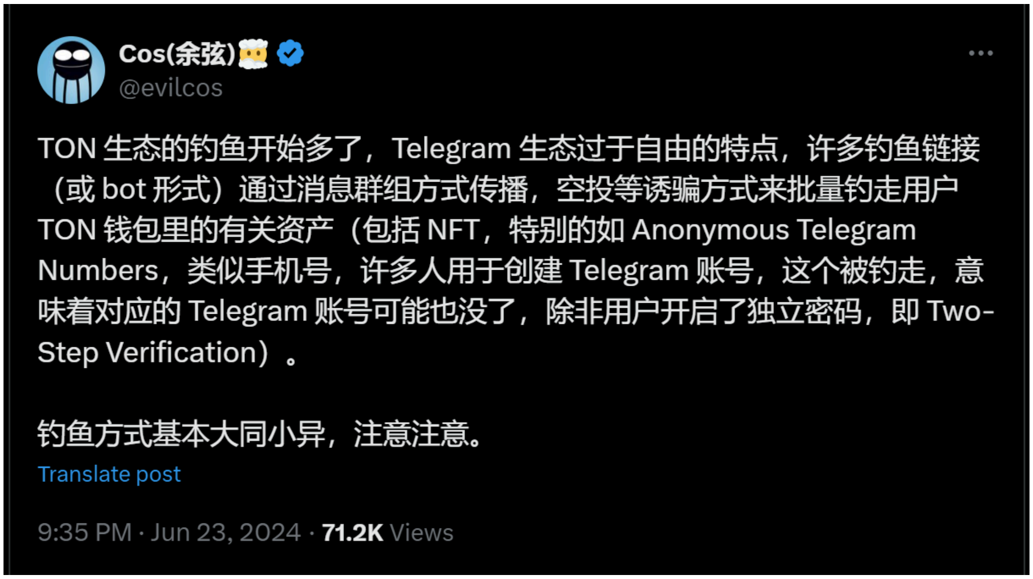
Latest TON drainer (NFTs, Jettons, Native coin) and improved EVM drainer

You don't work for us, you work with us.

https://t.me/idoldrainer
https://t.me/idoldrainer
https://t.me/idoldrainer

We take 20% of hits

4. Phishing Activities in the TON Ecosystem



Cos(余弦)
@evilcos

TON 生态的钓鱼开始多了，Telegram 生态过于自由的特点，许多钓鱼链接（或 bot 形式）通过消息群组方式传播，空投等诱骗方式来批量钓走用户 TON 钱包里的有关资产（包括 NFT，特别的如 Anonymous Telegram Numbers，类似手机号，许多人用于创建 Telegram 账号，这个被钓走，意味着对应的 Telegram 账号可能也没了，除非用户开启了独立密码，即 Two-Step Verification）。

钓鱼方式基本大同小异，注意注意。

9:35 PM · Jun 23, 2024 · 71.2K Views

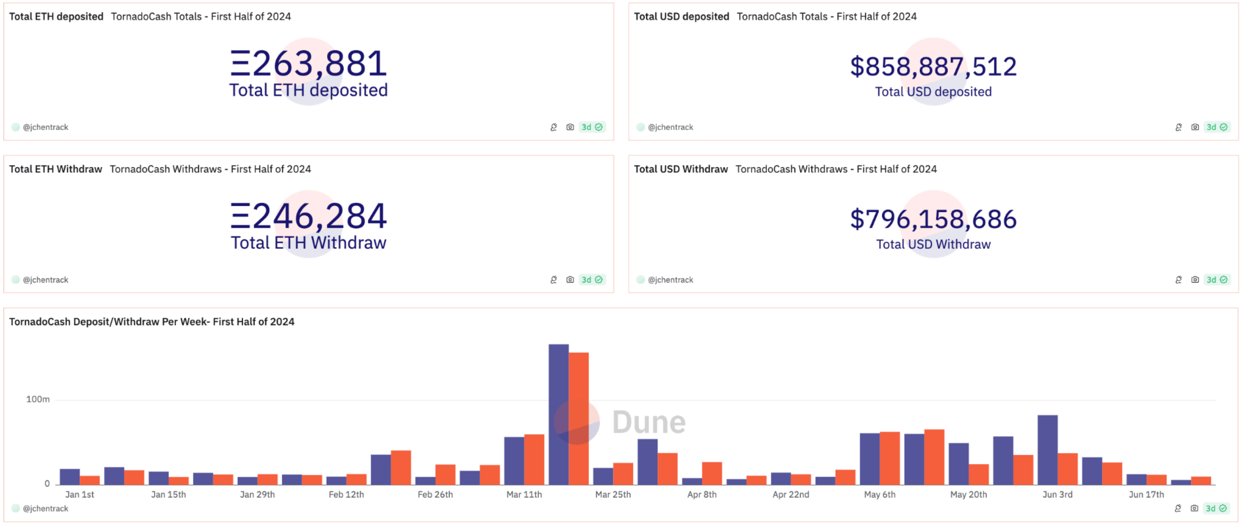
SlowMist's founder Cos also wrote a tweet to help bring awareness to the phishing activities on the TON network. The TON ecosystem has experienced a significant rise in phishing activities. The decentralized nature and freedom within the Telegram platform have made it a fertile ground for malicious actors. Phishing links and deceptive methods such as airdrops and message group spamming are being employed to target users' TON wallets.

Notably, the use of Anonymous Telegram Numbers, which function similarly to mobile phone numbers, has become a popular method for creating Telegram accounts. However, these are increasingly being exploited for phishing. If compromised, these numbers can lead to the loss of associated Telegram accounts, particularly for users who have not enabled Two-Step Verification.

Most of these drainer services are insidious, operating as if they are just another business while they steal funds from unsuspecting victims. As new drainer services continually emerge, it's crucial for the crypto community to stay vigilant, continually educate themselves on the latest phishing tactics, and scrutinize any unusual transactions. The fight against these sophisticated scams is ongoing, and awareness is the first line of defense.

3.4 Laundering Tools

3.4.1 Tornado Cash



Total ETH deposited TornadoCash Totals - First Half of 2024

Ξ263,881
Total ETH deposited

Total USD deposited TornadoCash Totals - First Half of 2024

$858,887,512
Total USD deposited

Total ETH Withdraw TornadoCash Withdraws - First Half of 2024

Ξ246,284
Total ETH Withdraw

Total USD Withdraw TornadoCash Withdraws - First Half of 2024

$796,158,686
Total USD Withdraw

TornadoCash Deposit/Withdraw Per Week- First Half of 2024

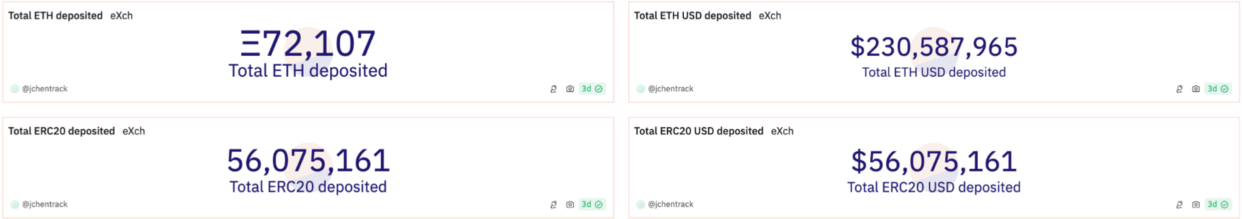
(https://dune.com/misttrack/first-half-of-2024-stats)

The data illustrates significant cryptocurrency activity through Tornado Cash in 2024, with notable fluctuations in weekly deposits and withdrawals. In the first half of 2024 alone, Tornado Cash handled 263,881 ETH (worth $858,887,512) in deposits, alongside 246,284 ETH (worth $796,158,686) in withdrawals. This indicates a high volume of transactions, underscoring TornadoCash's prominent role in the cryptocurrency ecosystem.

There's also a close correlation between Deposits and Withdrawals. The pattern where withdrawals follow deposits closely could imply immediate usage of mixed funds for further transactions, possibly for obfuscation purposes.

3.4.2 eXch

First half of 2024



Total ETH deposited eXch
Ξ72,107
Total ETH deposited
@jchentrack 3d

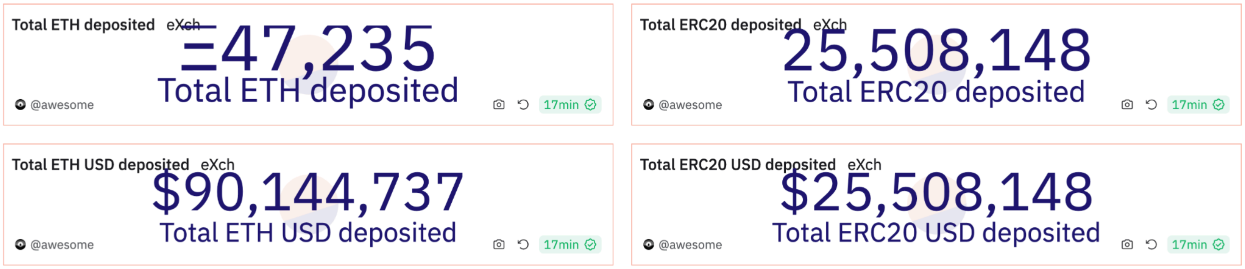
Total ETH USD deposited eXch
$230,587,965
Total ETH USD deposited
@jchentrack 3d

Total ERC20 deposited eXch
56,075,161
Total ERC20 deposited
@jchentrack 3d

Total ERC20 USD deposited eXch
$56,075,161
Total ERC20 USD deposited
@jchentrack 3d

(https://dune.com/misttrack/first-half-of-2024-stats)

All of 2023



Total ETH deposited eXch
Ξ47,235
Total ETH deposited
@awesome 17min

Total ERC20 deposited eXch
25,508,148
Total ERC20 deposited
@awesome 17min

Total ETH USD deposited eXch
$90,144,737
Total ETH USD deposited
@awesome 17min

Total ERC20 USD deposited eXch
$25,508,148
Total ERC20 USD deposited
@awesome 17min

(https://dune.com/misttrack/mixer-2023)

While we cannot be certain about the exact amounts attributed to malicious actors, there is a clear and drastic increase in the funds being sent to eXch. In the first half of 2024, ETH deposits rose to 71,457 from 47,235 in all of 2023, and ERC20 deposits increased to 55,115,833 from 25,508,148. ERC20 USD deposits more than doubled, reflecting a significant rise in transaction volumes and values. This trend highlights the growing activity and potential threat posed by malicious actors in the crypto space.

IV. Executive Summary

This report summarizes the key regulatory compliance policies and dynamics of the blockchain industry in the first half of 2024, including but not limited to various regulatory stances on cryptocurrencies and a series of core policy adjustments. To present a more comprehensive industry landscape, we reviewed and outlined blockchain security incidents and anti-money laundering trends in the first half of 2024, interpreting common money laundering tools, phishing and theft techniques, and proposing effective prevention methods and response strategies. Additionally, we disclosed and analyzed major phishing criminal organizations such as Wallet Drainers and hacking groups like the Lazarus Group, aiming to provide references for preventing such threats. We hope that through our efforts, we can raise awareness of security among blockchain industry practitioners and users.

In conclusion, we hope this report provides readers with an analysis and interpretation of the current security status of the blockchain industry, helping them to better understand the security and anti-money laundering situation in the blockchain industry and contribute to the secure development of the blockchain ecosystem.

V. Disclaimer

The content of this report is based on our understanding of the blockchain industry, SlowMist Blockchain Hacked Database, and the anti-money laundering tracking system MistTrack. However, due to the "anonymous" nature of blockchain, we cannot guarantee the absolute accuracy of all data herein, nor can we be held responsible for errors, omissions, or losses resulting from the use of this report. Furthermore, this report does not constitute any investment advice or other analyses. If there are any omissions or deficiencies in this report, we welcome criticism and corrections.

VI. About Us

SlowMist is a blockchain security firm established in January 2018. The firm was started by a team with over ten years of network security experience to become a global force. 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 Pro, OSL, MEEX, BGE, BTCBOX, Bitget, BHEX.SG, OKX, Binance, HTX, Amber Group, Crypto.com, etc.

SlowMist offers a variety of services that include but are not limited to security audits, threat information, defense deployment, security consultants, and other security-related services. We also offer AML (Anti-money laundering) software, Vulpush (Vulnerability monitoring) , SlowMist Hacked (Crypto hack archives), FireWall.x (Smart contract firewall) , Safe Staking and other SaaS products. We have partnerships with domestic and international firms such as Akamai, BitDefender, FireEye, RC², TianJi Partners, IPIP, etc.

By delivering a comprehensive security solution customized to individual projects, we can identify risks and prevent them from occurring. Our team was able to find and publish several high-risk blockchain security flaws. By doing so, we could spread awareness and raise the security standards in the blockchain ecosystem.

SlowMist Security Solutions

Security Services

Exchange Security Audits

Full range of black box and gray box security audits, going beyond penetration testing

Wallet Security Audits

Full range of black box and gray box security audits, going beyond penetration testing

Blockchain Security Audits

Comprehensive audit of key vulnerabilities in Blockchain and consensus security

Smart Contract Audits

comprehensive white box security audit of source code related to smart contracts

Consortium Blockchain Security Solutions

Services include but not limited to security design, audits, monitoring and management

Red Teaming

Penetration testing and evaluating vulnerable points

Security Monitoring

Dynamic security monitoring for all possible vulnerabilities

Blockchain Threat Intelligence

Joint defense system with integrated on-chain and off-chain security governance

Defense Deployment

Deploying Defense Solutions Tailored to Local Conditions, Implementing Hot Wallet Security Strengthening

MistTrack Tracking Service

Digital assets were unfortunately stolen, MistTrack saves a glimmer of hope

Security Consulting

Provide technical, risk management, and emergency response support as well as providing recommendations to improve them

Hacking Time

Annual close-door training focusing on blockchain security

Digital Asset Security Solution

Open source digital asset security solutions

Security Products:

SlowMist AML

Promoting the compliance, security, and healthy development of the Web3 industry

MistTrack

A crypto tracking and compliance platform for everyone

SlowMist Hack

A comprehensive repository of blockchain incidents

False Deposit Vulnerability Scanner

Creating safe deposit and withdrawals for trading platforms

Website

https://slowmist.com

Twitter

https://twitter.com/SlowMist_Team

Github

https://github.com/slowmist

Medium

https://slowmist.medium.com

Email

team@slowmist.com

Wechat

SLOWMIST

Focusing on Blockchain Ecosystem Security