Cryptocurrency Racket: The Growing Perils of Investing in Mysterious Cryptocurrencies

A comprehensive study into how cryptocurrency fraud is on the rise, and how consumers are being deceived into losing their highly elusive cryptocurrency through multifarious ruses.

Authors: Abhinav Pandey and Suchita Katira

Editor: Deepanjli Paulraj

Table of Contents

Overview of the Cryptocurrency Frauds on Global Crypto Exchanges

Cryptocurrencies have acquired the heed of the world. It has been a one-stop investment mode for all investors, from wealth managers, financial leaders, and Institutional investors to newbie investors, hatching on their first investments. This status of market fascination has drawn adversarial actors into the game.

According to the Federal Trade Commission (FTC) Consumer Sentinel, from October 2020 to March 31, 2021, reports of crypto-related scams zoomed to nearly 7,000 people reporting losses of more than 80 million USD, depicting a menacing picture of cryptocurrency fraud revolving around investors.

CloudSEK's Threat Intelligence Team conducted a thoroughgoing analysis of the myriad digit of ways in which crypto users are targeted, and in this paper, we delve into the data collected between 1 January 2021 and 30 June 2022.

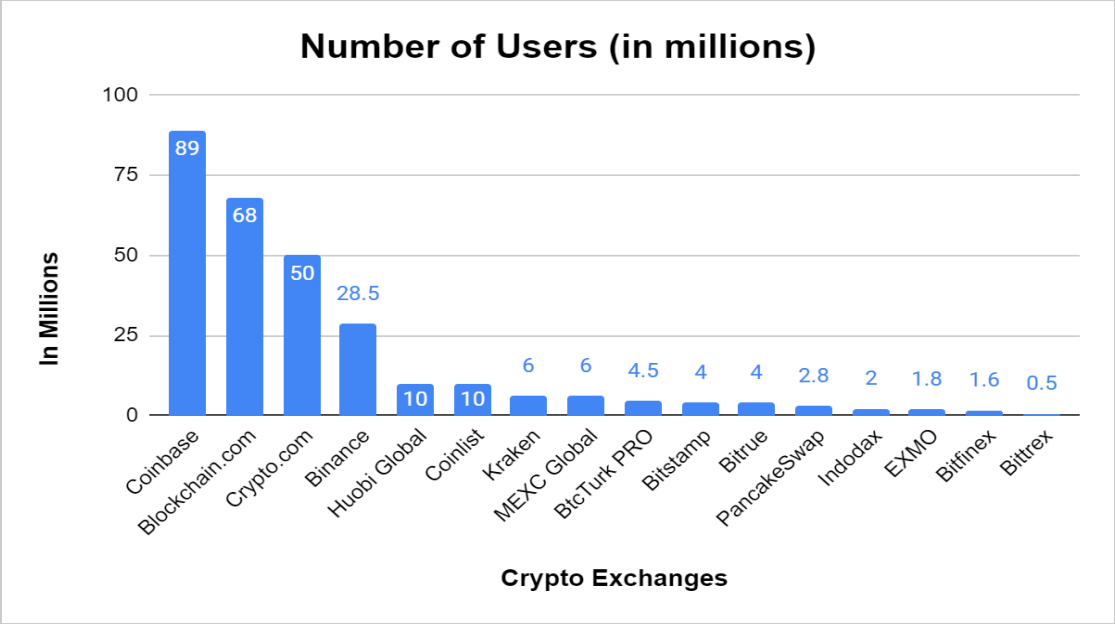
In this report, we also explore:

- Introduction to the world of Crypto
- Number of crypto users globally and in India
- Various threats targeting crypto exchanges and crypto users
- Scams running on the crypto exchanges
- Fake domains on the crypto exchanges
- Mitigation and recommendations to avoid scams

Introduction to the Crypto World and its Common Terminology

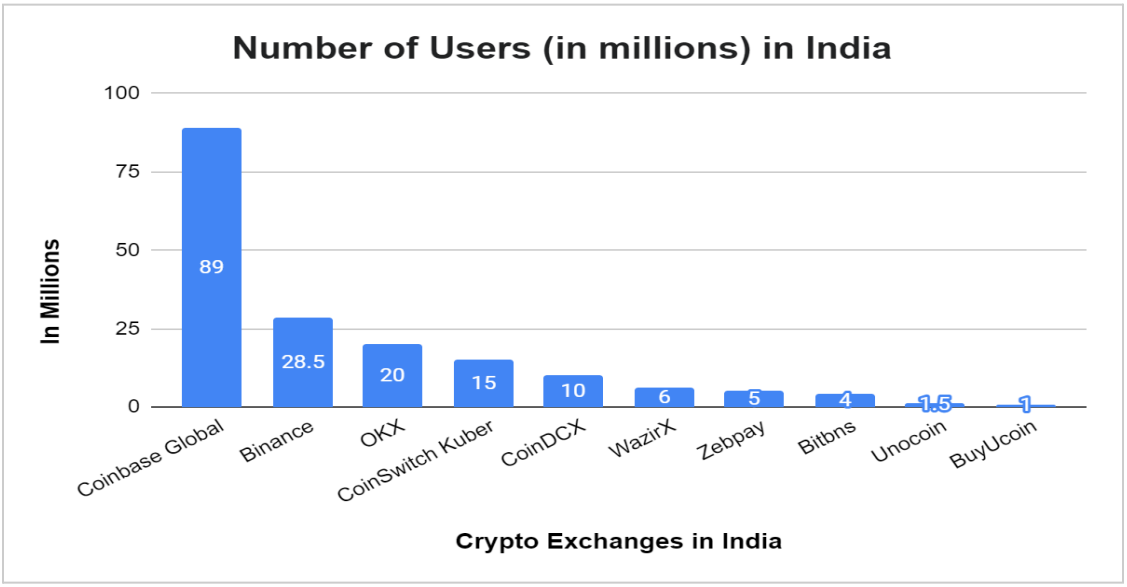
Cryptocurrency is a modern-day barter currency, a digital asset, or a digital form of money built on revolutionary blockchain technology. While bitcoin dominates the cryptocurrency market, Ethereum, and Ripple follows along in the market share. The trading of these cryptocurrencies takes place on exchanges where users buy, sell and trade their cryptocurrencies. Top exchanges include Binance, Coinbase, and Kraken followed by many other crypto exchanges.

As of Q1 2022, there are approximately 300 million identity-verified cryptocurrency users globally, where Coinbase, Blockchain[.]com, Crypto[.]com, and Binance monopolize the crypto market as depicted in the following chart.



Number of Users on Crypto Exchanges Globally

The below chart illustrates the Top 10 Crypto exchanges in India in 2022 in context with the number of registered users, where Coinbase overshadows every other exchange followed by Binance. For this paper, based on active users we will primarily focus on Coinbase and Binance when providing instances of scams and phishing attacks.



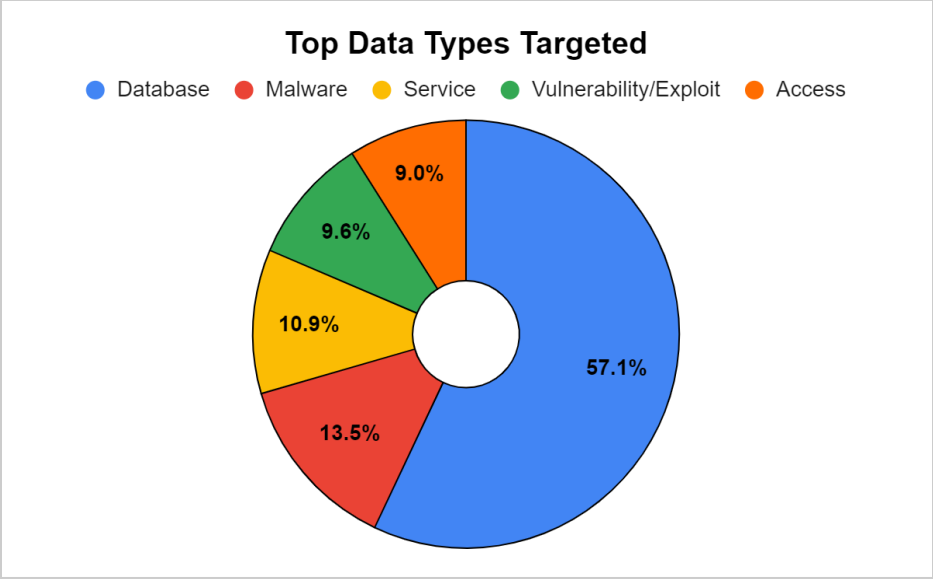
Number of Users on Crypto Exchanges in India

Threat and Trouble in the Crypto World

Cryptocurrency, being a decentralized, unregulated currency, provides numerous benefits to individuals in multiple ways. However, the glimmer of cryptocurrency is impeded by the ever-increasing concerns in the crypto market. In general terms, these cryptocurrency scams fall into two broad, discrete categories:

1. Transfer of cryptocurrency straight into a scammer's wallet using phishing or other deceitful techniques.
2. Theft of victims' digital wallets or login credentials by scammers or threat actors.

Alone in 2021, Crypto criminals stole a record 3.2 billion USD worth of cryptocurrency according to Chainalysis, more than the GDP of 39 countries in the world. This was a fivefold increase from that in 2020. Nevertheless, fraudulent schemes continue to surpass theft as a major threat, enabling scammers to lure a whopping 7.8 billion USD worth of cryptocurrency from gullible victims.



Data Types' Targeted Numbers

Based on activities tracked and data collected by CloudSEK's contextual AI digital risk platform XVigil, Databases were the prime target of crypto criminals followed by Malware, Services offered for hacking or scam, vulnerability or exploits of various web and mobile crypto-related applications, and Access to wallets and accounts. All of them have been explained below thoroughly:

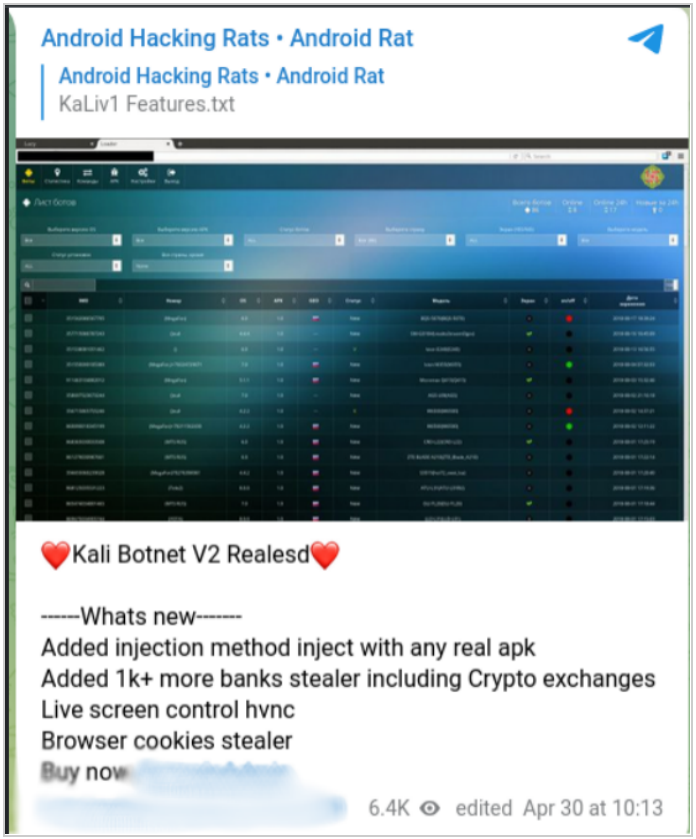
Database

Occupying more than half of the threats being targeted, Databases can be considered a lucrative means for crypto criminals that open an unmediated and direct gateway to users' sensitive information including PII such as name, address, phone number, and secret keys to their crypto accounts and wallets.

Example of a database leak on an underground forum

Malware

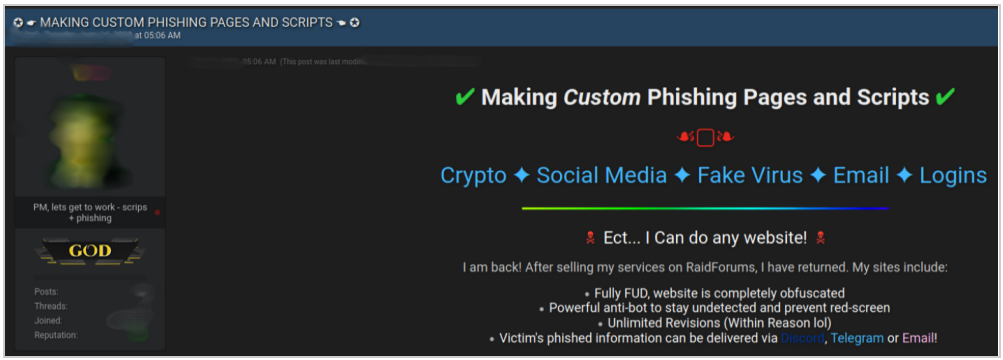
Utilizing the above-mentioned services, primarily phishing, threat actors lure a user into clicking on an infected link containing malware. Once the link is clicked, the malware gets deployed. The contents of a user's crypto wallet are altered using the wallet address, and the funds are redirected to the threat actor's account using an open-source command-line tool. This is a description of an uncomplicated instance of malware, however, advanced malware with complex mechanisms of evasions, and persistence exist and are actively exploited by threat actors to operate such crypto thievery.



Example of a malware bot available on an underground forum

Service

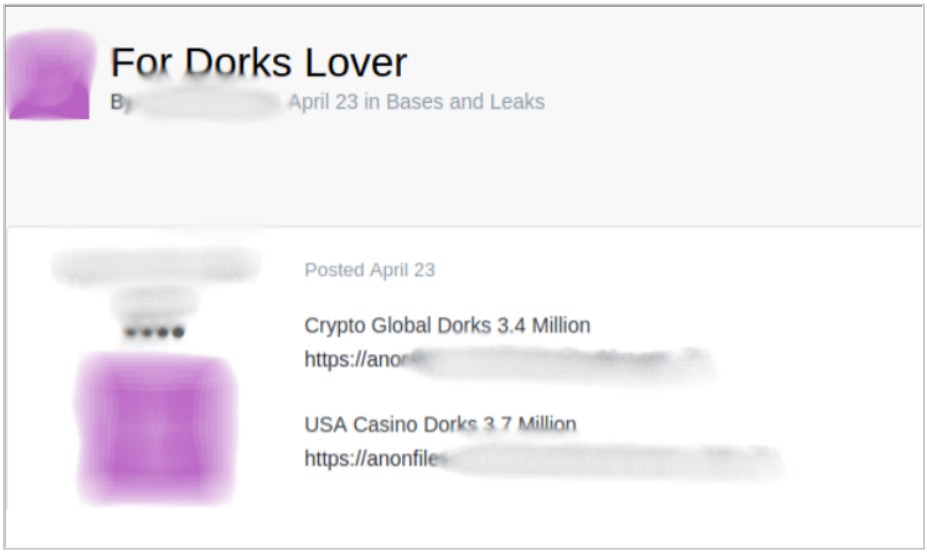
With the dark web being a functional partaker in the malicious activities, threat actors offer numerous services on such forums, proposing to gain access to users' cryptocurrency on a particular exchange or advancing the predominating phishing scams and campaigns to hoodwink users into giving up their credentials, backup keys or other sensitive information relating to their wallets. Identical duplicates of authentic websites of wallets and cryptocurrencies are devised by the threat actors, with the use of techniques such as IDN homograph to steal the digital assets of users.



Example of a Phishing Service available on an underground forum

Vulnerability or Exploit

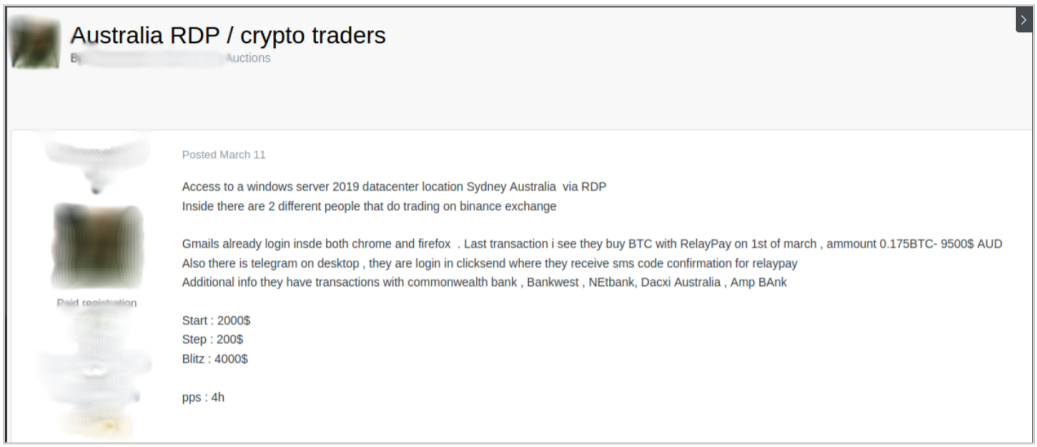
Threat actors wait for these “vulnerability waves” to ride on and as soon as a Zero-day vulnerability pops up, they begin exploiting it to gain access to users' crypto accounts and wallets. These exploits or Zero days are shared on dark web forums, where for some credits, actors provide PoC for other users to exploit the given zero-day.



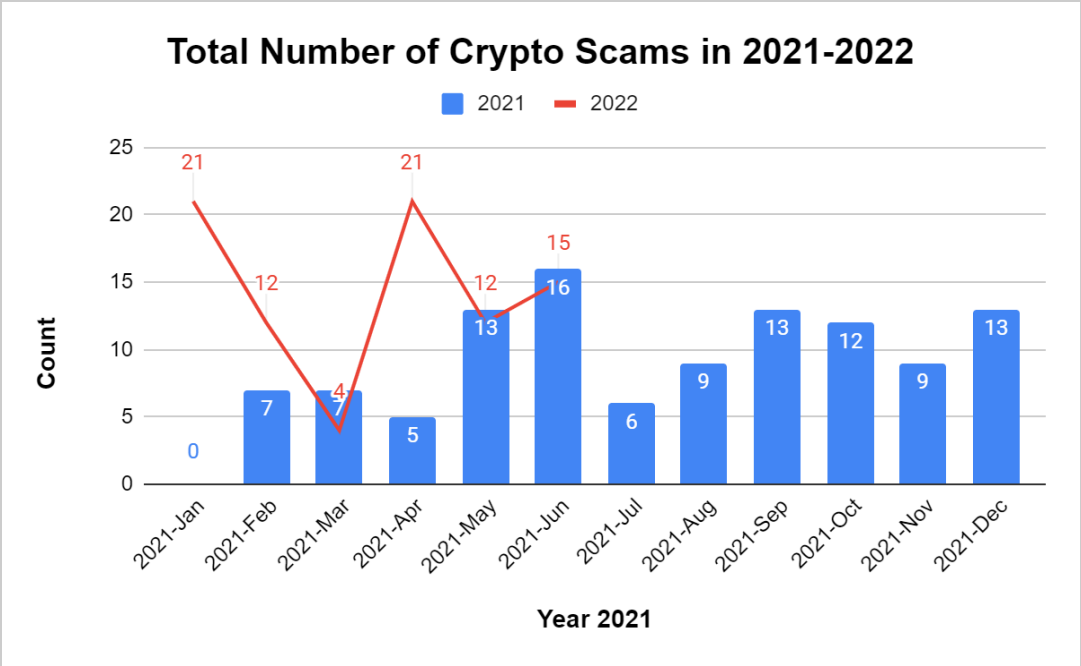
Example of an exploit available on an underground forum

Access

Once login credentials are obtained from the victims through nefarious methods such as an ongoing phishing campaign, access to relevant crypto wallets or exchanges are seized, where a portion of them are sold on the dark web, either for reputation or for other malicious services to other threat actors which are then used to transfer stolen cryptocurrencies into those accounts.



Example of Access to a crypto exchange available on an underground forum



Total Number of Scams in 2021-22

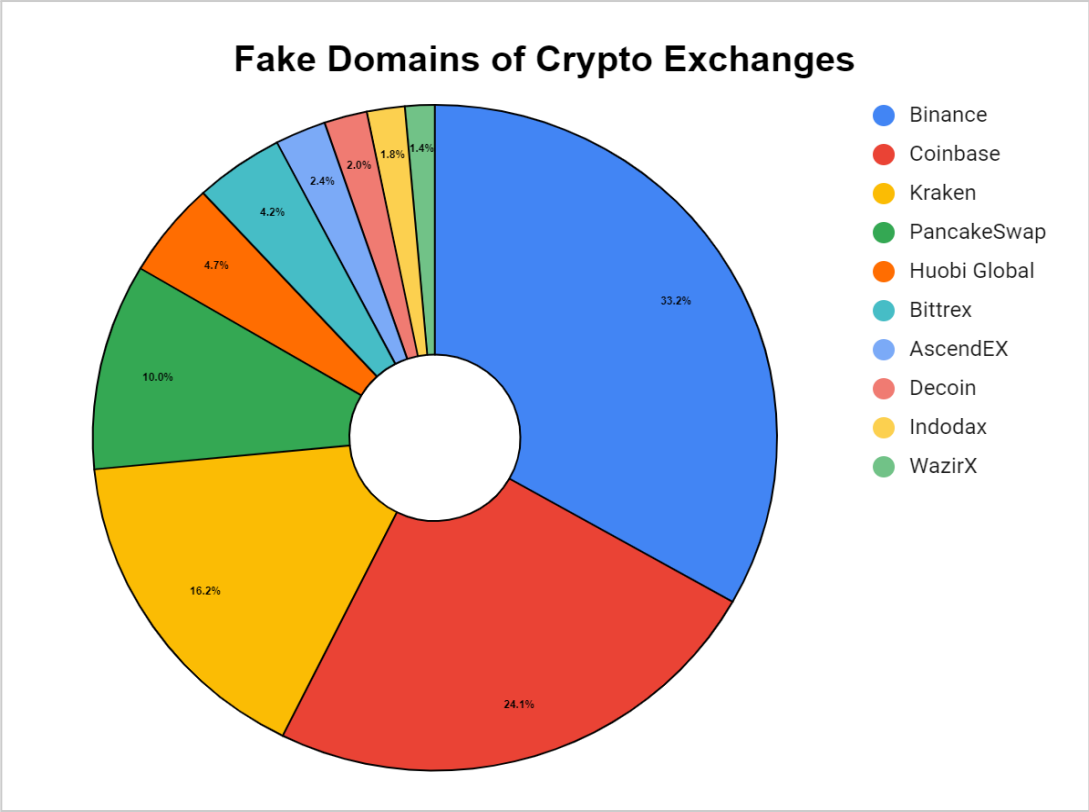
Crypto Scams and their Underworld Ties

Blockchain, primarily for cryptocurrencies, offered anonymity in transactions, incredible security, transactional freedom, and cross-border transactions which facilitated its growth to the pinnacle, furthermore as an assumed alternative to the already existing Global financial system. However, deceitful scams and abuse for disreputable activities impeded its posture as an alternative to the International financial system, including its use as a payment gateway on the dark web for selling and buying illegal items such as guns or drugs or for digital scams and thievery. The idea of a decentralized currency made cryptocurrency a revolutionary success; however, the same idea facilitated the operation of criminal activities by providing them anonymity, hindering and raising doubts in the minds of numerous people about cryptocurrencies.

The use of such illicit transactions for nefarious purposes enabled a comprehensive ecosystem where threat actors bought domains, phishing services, malware, and PoCs for vulnerabilities using cryptocurrencies, primarily Bitcoin, and conducted scams against people, deceiving them to lose their highly elusive cryptocurrency.

Fake domains impersonating authentic exchanges such as Binance or Coinbase popped up in no time, causing serious damage to naive users in financial terms, and reputational damage to the mentioned exchanges.

CloudSEK's researchers investigated numerous fake domains impersonating multiple crypto exchanges where a major chunk of the domains replicated Binance and Coinbase followed by Kraken and PancakeSwap.



Percentage comparison of Fake Domains of Crypto Exchanges

Investigation of Prevalent Scams

A thorough investigation unearthed numerous fake domains that were being used to deceive and scam people to gain access to their accounts and their digital assets. Some of the prominent ones include:

1) **bbinance.com being used to impersonate the binance.com domain**: The depicted domain (bbinance[.]com) is a phishing website identified during analysis by CloudSEK Researchers.

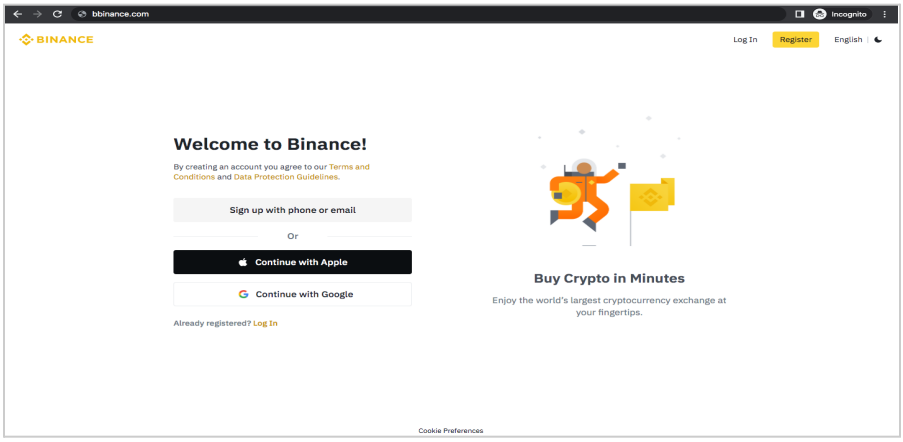


Image depicting bbinance phishing website with login and signup page.

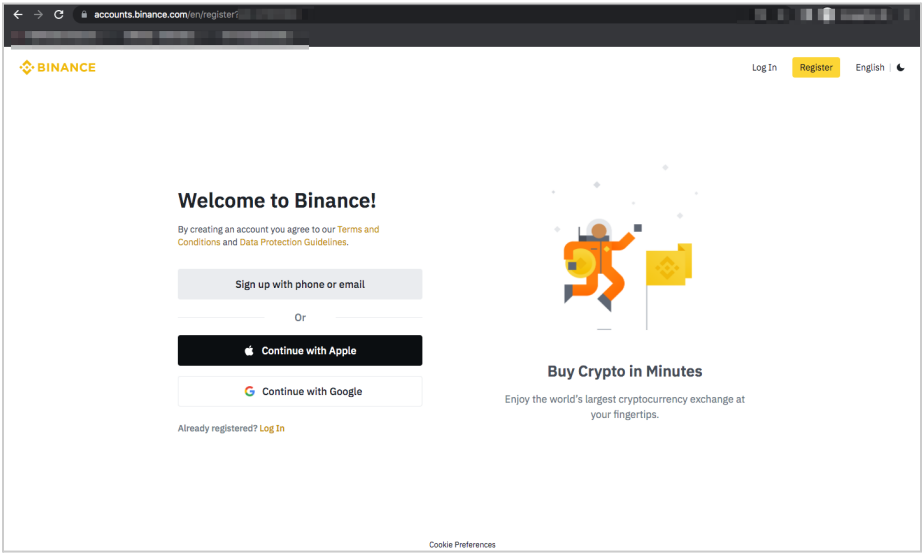
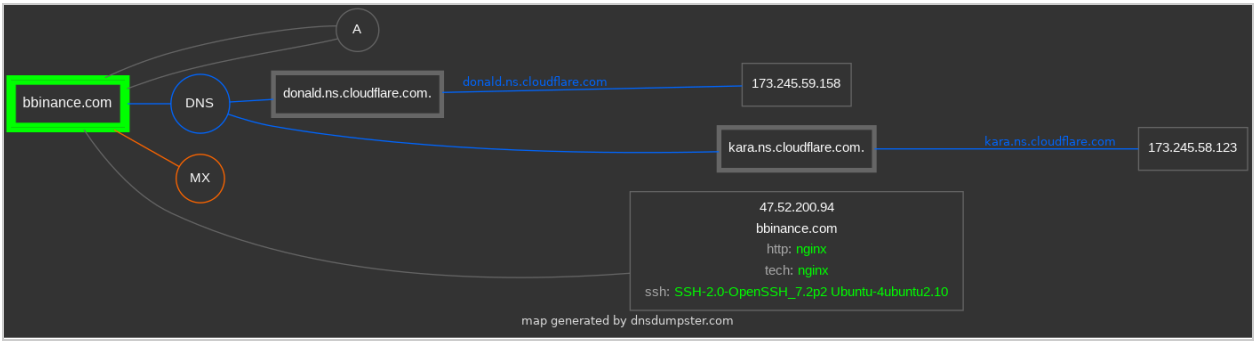


Image depicting binance real website with login and signup page.

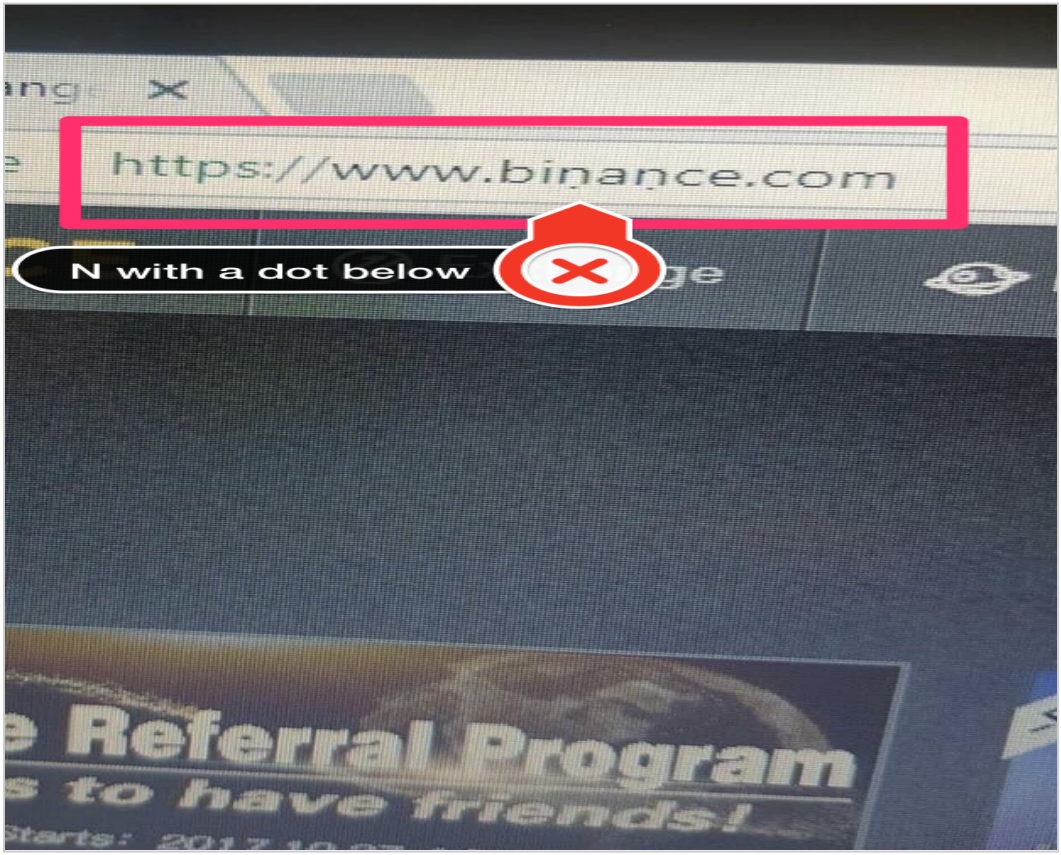
The bbinance domain is still active and at present redirects a user to an accounts subdomain of the authentic binance domain and prompts users to register or login into their accounts.

Additional analysis of the domain revealed two DNS servers being used named, donald.ns.cloudflare.com and kara.ns.cloudflare.com. The bbinance.com website has 47.52.200.94 as its IP address, hosted on the Alibaba cloud whereas the Cloudflare servers were located in the USA.



Domain information chart of bbinance.com

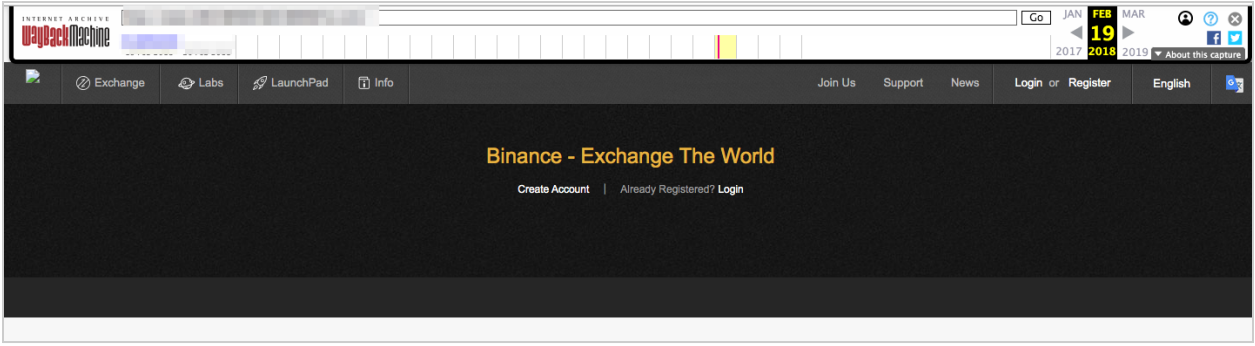
2) **IDN homograph Binance.com domain**: The below image impersonates the binance.com domain and is a case in point for the IDN homograph attack. It is a malicious way of misleading a computer user with a lookalike domain name and cloning the website with the same elements and design, for the user to believe it to be a real website.



Binance.com domain with special characters

The above domain is unrecognizable by common internet users and the two special characters 'ɳ' being manipulated will not be clearly visible to the direct sights of a user. This makes the attack even more detrimental as even aware users might fall prey to this.

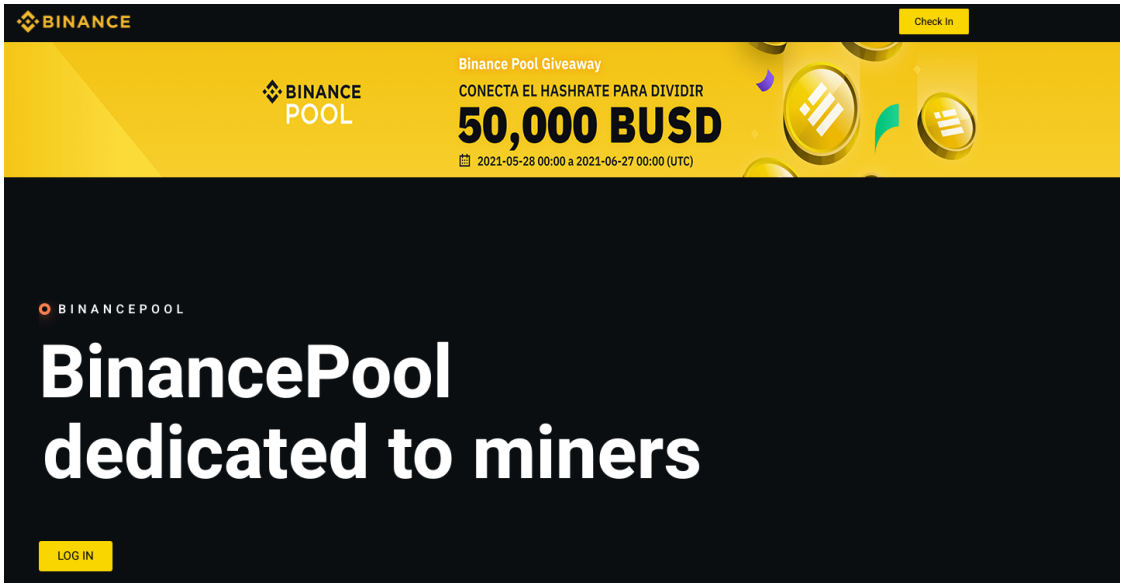
The website at the moment of research was taken down but our researchers were able to discover a WayBack instance of the domain being used at a point in time implying its use for nefarious purposes.



Wayback instance of the domain Binance.com with special characters

Such IDN homograph domains are used to fabricate phishing scams by creating a homologous domain name similar to the original domain name as in the case of Binance.

3) **Binance pool giveaway scam:** Such pool giveaway scams are usually social engineering attacks where users, in the lure of giveaways, are deceived into populating their sensitive credentials on such phishing websites.
    a) Once a certain number of credentials are extracted, some are used to log in and take over the account, transferring the assets to the actor's wallet while most of them are sold on dark web forums for forum currency or reputation.



A phishing website scamming people in context with Binance pool giveaway

b) A similar instance was discovered by CloudSEK where threat actors were using the real Binance pool giveaway contest to scam people and take over their credentials.

c) The catch here is that a user must first deposit a definite amount of cryptocurrency to a giveaway address in order to verify their wallet before they can enter the giveaway. The transaction is irreversible and the harm is done as soon as the victim transfers money to the actor at their address.

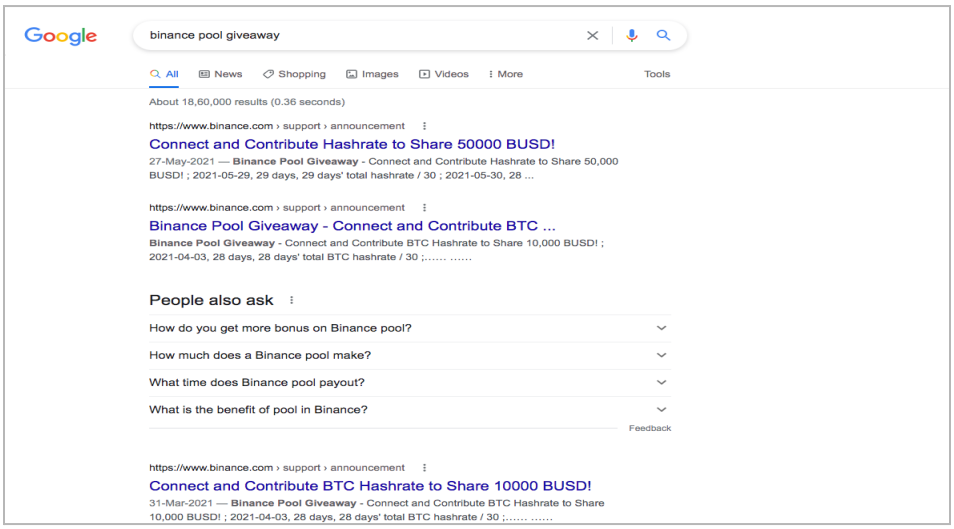
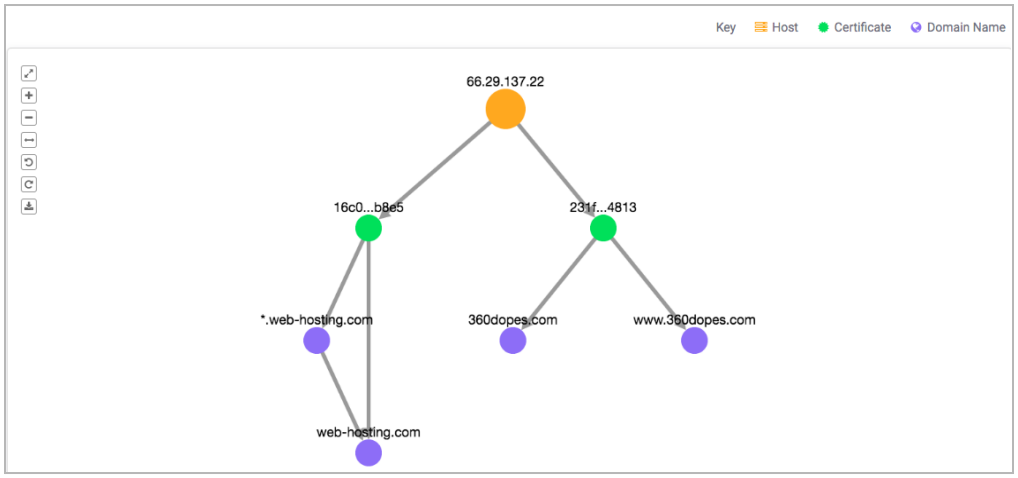


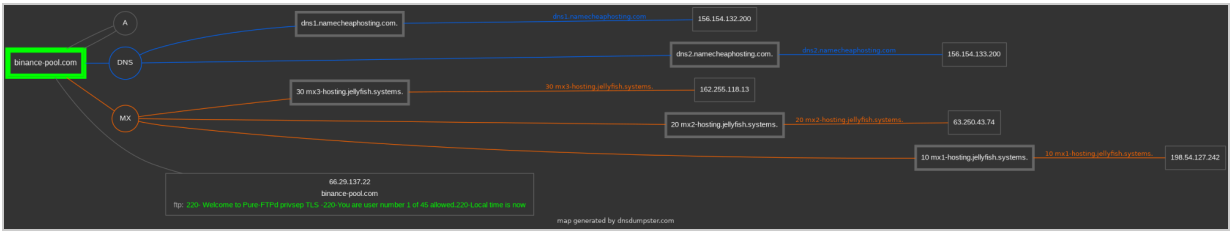
Image depicting a typical Google search in the context of a Real Binance Pool giveaway

An In-depth analysis of the domain revealed two DNS servers being used, with the domain IP address being 66.29.137.22, located in Reykjavik, the capital city of Iceland. Along with this, various other websites were hosted on the same IP implying its use for shady objectives.



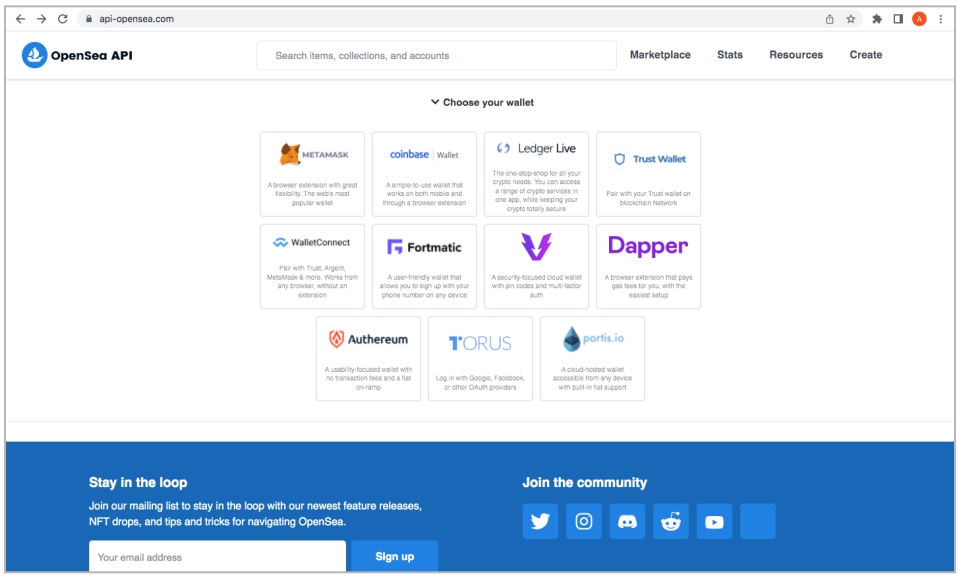
Binance-pool giveaway domain IP hosting other sites

The binance-pool domain has no A records but as mentioned two DNS servers with names as straightforward as dns1[.]namecheaphosting[.]com and dns2[.]namecheaphosting[.]com.



Binance-pool giveaway domain information

4) **OpenSea Account deceitful recovery domain:** This phishing website of “OpenSea API”, was uncovered during our research, and replicated equivalent designs as of authentic Open Sea website. It prompted users to select a wallet for which they wanted to recover their account which included MetaMask, Coinbase, Ledger, Trust Wallet, Dapper, and many more.
    a) Once a user clicks on any of these, the user is redirected to a page and mentioned to enter the recovery phase of their wallet. It is important to mention that the redirected website does not take a user to the original domain, but to another fake one.
    b) Once the user enters the recovery phase and presses submit, the page shows no change but the user's recovery credentials are taken by the actors.



OpenSea API displays many wallets

A live instance of how these recovery phrases (or seed phrases) are employed by threat actors was discovered and is mentioned below, as in the case of MetaMask.

Crypto Frauds unearthed by CloudSEK Researchers in Business-As-Usual from Underground Cybercrime Forums

CloudSEK Platform has been proactive in discovering phishing and fraud incidents and has released Threat intelligence and feeds for countless such instances, some of them are mentioned below

1. **Phishing Scam on CoinEgg Crypto Exchange:**

   Comprehensive research article on the Phishing scam on CoinEgg Crypto Exchange.

2. **Hacking Incident on AscendEX Crypto Exchange:**
   The mentioned incident was identified by CloudSEK Platform at the time of the Press Release, Dec 12, 2021. Ascendex, a cryptocurrency exchange, incurred a security breach that allowed hackers to access the wallets of the users.
   - The attack occurred on hot wallets, where funds are kept as reserves for customers' withdrawals due to which AscendEX incurred estimated losses of around 77 million USD.

3. **Actors Exploiting CVE-2022-32969 to Exfiltrate Unencrypted Password Seeds from Metamask Crypto Wallet:**

   CloudSEK's Researchers discovered a threat actor selling Metamask seed phrases, which are secret recovery phrases that are used to generate and maintain accounts. A recovery phrase is a string of words produced by a cryptocurrency wallet that grants users access to the cryptocurrency linked to that wallet (also referred to as a seed phrase). CVE-2022-32969 is a vulnerability present in browser extensions of crypto wallets like Metamask and Phantom, dubbed as Demonic vulnerability which was being abused by threat actors to target the users of the above-mentioned crypto wallets. An exact TTP (Tactics, Techniques, and Procedures) is employed by the Seaflower Threat Actor group to exfiltrate these unencrypted password seeds from disk, or via remote access.
   - **Threat actor Draining Cryptocurrencies from MetaMask wallets using Password Seed Brute Forcing**: After three days of the discovery of the above trend, CloudSEK's DRP discovered a new post on an underground forum advertising the sale of a brute force seeding service for MeteMask and Atomic Crypto wall. The threat actor's prime objective was to drain the cryptocurrency from the respective wallets after brute forcing the password seed. There has been much heat concerning MetaMask since the browser

extension vulnerability (CVE-2022-32969) and phishing campaigns were launched to steal wallet seeds using KYC.

4. **Threat actor selling 1.2 Million Bank & Crypto target leads:**

CloudSEK's Researchers discovered a post on an underground forum where a threat actor was advertising the sale of 1.2 million bank & crypto leads. These leads, in the wrong hands, would be atrocious for crypto users and their wallets along with banks, as they can be used for spamming banks using Cpanel.

5. **MaliBot, a New Android Banking Trojan Disguised as a Cryptocurrency Miner:**

CloudSEK's Researchers flagged a trojan MaliBot that disguised itself as a Crypto mining app. The malware app was capable of carrying out web injection and overlay attacks. It stole the below-mentioned data from the users:

- MFA codes
- Authentication cookies
- Wallet data
- SMS messages

The malware could also provide VNC access to infected devices for remote access. MaliBot disguises itself as a cryptocurrency mining app named "Mining X" or "The CryptoApp", and occasionally assumes some other guises, such as "MySocialSecurity" and "Chrome".

6. **Crypto Drainer Template Facilitates Tens of Millions of Dollars In Theft:**

A threat actor was caught mentioning a crypto drainer template being responsible for the loss of over ETH 2,000. Crypto Drainers are phishing pages that lure victims into signing malicious transactions that allow the attacker to siphon their crypto and NFTs.

- The websites themselves are primarily promoted via spam campaigns on social networks and Discord channels. One of the ETH addresses associated with the website produced over USD 85K in revenue for the attacker in 10 days.

7. **Fake Wallet Developer:**

A threat actor was caught looking for a Fake Wallet Developer. The actor mentioned a budget of USD 5000 and asked for all the normal features of a wallet along with some extra functionalities, with the prominent ones being:

a. Instant rebranding feature Admin - Should be able to change the domain name, logo (manual upload), and website name everywhere throughout the website from within the admin panel.
b. Admins should be able to send a custom popup to any user
c. Automatic maintenance notice in case the site goes down
d. Ability to send email to all users at once (3rd party API can be used)

These features would allow the scammer to target multiple crypto entities and would seem professional and authentic to the gullible user.

8. **Coinbase 2022 Phishing Panel:**

A threat actor was discovered sharing a custom-made phishing panel for the Coinbase crypto exchange for free. The actor claimed that the panel was made for a Serbian phishing actor known as Jimbo Arrested/Panther/Pound aka Dusan Tomic.

a. The panel would use spoofed emails attaching the domain of the phishing campaign and spoof a call from Coinbase support telling them to check the emails. Once the victim checked the emails and visited the panel, it would allow them to bypass 2FA and then be able to generate API keys.

How Crypto Currency Frauds are Impacting Individuals

With countless ingenious and intricate fraud campaigns being executed day in day out, trepidation amongst investors is obvious. The greed for increased returns and the fear of failing out on an opportunity makes the scam game even more powerful. The changing security landscape and the exponentially expanding technological advancements create openings to fill as they transform and grow. Unfortunately, these voids are far from being sufficed, considering the attack surface, and the surge in attackers using 0-Days for attacks and the gullibility of the end user with such contemporary technology.

People, all over the globe, who have been robbed of their crypto currency are in fear of losing more or never getting back their money. For some investors, the invested money would be the extra they could afford to invest. However, for others, it may be what they had planned for their future life or child's education. Whichever form the investment might be, losing hard-earned money is hard on anyone.

A real-life example reported on BBC News:
Taxi driver Chris is obsessively checking his phone for updates.
"I'm set to lose almost 2,500 euros (£2,100) worth of cryptocurrency coins," he says.

Chris describes himself as "a small crypto-holder from Austria" and is one of many victims of a hack attack on cryptocurrency exchange Liquid Global in Aug 2021.
The company has insisted it will pay all customers who lost out in the $100m (£72.8m) attack.
But until they get the money back, many customers are worried.

A recent FTC investigation found that since early 2021, about 46,000 Americans have reported losing more than $1 billion in cryptocurrencies as a result of frauds.

More than 46,000 consumers have reported losing over $1 billion in cryptocurrency to scams since the beginning of 2022. This is around one out of every four dollars reported lost and is more than any other payment method. The three most popular cryptocurrencies that users claimed to have used to pay fraudsters were Bitcoin (70%) Tether (10%) and Ether (9 percent).

Recommendations and Mitigation Measures

How Investors Can Protect Their Cryptocurrency

- Crypto investments should make up less than 5% of an investor's portfolio, according to financial experts.
- Use security software to protect your PC and mobile device.
- Before investing in huge social media crypto schemes, do your homework by researching the scheme.
- Don't invest in or trade cryptocurrencies based on the advice of someone you've only communicated with over the internet.
- Protect your wallet. Keep wallet keys private, and in a secure place, preferable offline, where they would be difficult to hack.

Actions to take today to mitigate cyber threats to cryptocurrency:

- Patch all systems.
- Prioritize patching known exploited vulnerabilities.
- Train users to recognize and report phishing attempts and various scams.
- Use multi-factor authentication.

Conclusion

Although there is no right or wrong way to invest in cryptocurrencies, it is crucial to carefully weigh the advantages and disadvantages of doing so before making a decision. After all, it is every individual's hard-earned money at risk, either of doubling or decreasing or in the worst case scenario, disappearing.

References

- Beware of Cryptocurrency Scams (investopedia.com)
- Common crypto scams you should know about before diving into the crypto market | Business Insider India
- https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze
- https://www.inventiva.co.in/trends/top-10-crypto-exchanges-india-2022/
- https://www.coingecko.com/en/exchanges

About CloudSEK

CloudSEK is a contextual AI company that predicts Cyber Threats even before they occur. We combine the power of Cyber Crime monitoring, Brand Monitoring, Attack Surface monitoring, and Supply chain intelligence to provide context to our customer's digital risks. Our unified dashboard allows customers to triage and visualize all digital threats in one place. We also offer workflows and integrations to manage and remediate the identified threats. To learn more about CloudSEK, visit cloudsek.com.