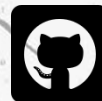


Thousand ways of stealing cryptocurrencies

DELIVERING CYBERSECURITY BEYOND EXPECTATIONS

Indrajeet Bhuyan



@numencyber

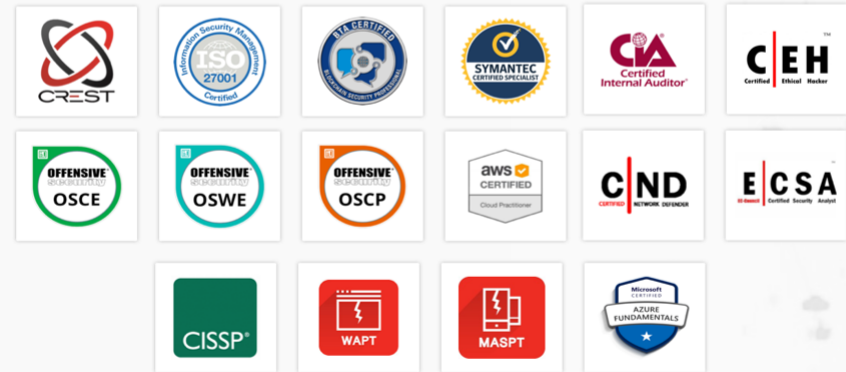
Numen Cyber Technology

A Cybersecurity solution provider based in Singapore. We dedicate ourselves in Threat Detection & Response for Web3 business.



Numen Cyber Labs

Numen Cyber Labs comprises a team of Elite that specialized in Blockchain Security, Ethical Hacking, Vulnerability Research & Threat Analyzing. We pledge ourselves to stay ahead of the technology trend and bring cyber security to a new level.



Shameless Self Promotion



- Security Consultant at Numen Cyber Technology, Singapore
- Contributed security to Samsung, HCL, Whatsapp, Photobucket, Digit, TVF and many more.
- Developed smallest possible (2kb) code which could crash Whatsapp
- Created wannasmile which was used to protect users from wannacry
- Invited to speak at NullCon, ToorCon, AndSec, G0S, BPM etc.
- Helped Indian Government detect and fix sites affected from Crypto Jacking
-

Previous Research on Cryptocurrencies

My Previous research in cryptocurrency and cryptojacking got featured in



HUFFPOST



TNW
THE NEXT WEB



THE ECONOMIC TIMES



infoRisk
TODAY




DECCAN
Chronicle



THE COINTELEGRAPH
future of money

Previous Research on Cryptocurrencies



Got featured in a documentary by 

Disclaimers



This is not a financial advice

This presentation is only for educational purpose

What is Blockchain ?

- Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network.
- Anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

What is Smart Contract ?

- Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met.
- It allows developers to build dapps that take advantage of blockchain security, reliability and accessibility

What is Smart Contract ?

The screenshot displays a smart contract verification page. At the top, it shows the contract holder's address (0x2170ed0880ac9a755fd29b2688956bd959f933f8), the contract's balance (241,763,838.552388744111704326 SHIB), and its value (\$2,074.33). Below this, there are tabs for 'Transfers', 'Info', 'Contract', and 'Analytics'. The 'Contract' tab is active, showing options to 'Read Contract' or 'Write Contract'. A search bar for source code is present. A green checkmark indicates 'Contract Source Code Verified (Exact Match)'. Contract details include the name 'TokenMintERC20Token', compiler version 'v0.5.0+commit.1d4f565a', and optimization settings. The main section displays the Solidity source code for the contract, including functions like 'transfer' and 'allowance'.

Contract Source Code Verified (Exact Match)

Contract Name: **TokenMintERC20Token** Optimization Enabled: **No with 200 runs**

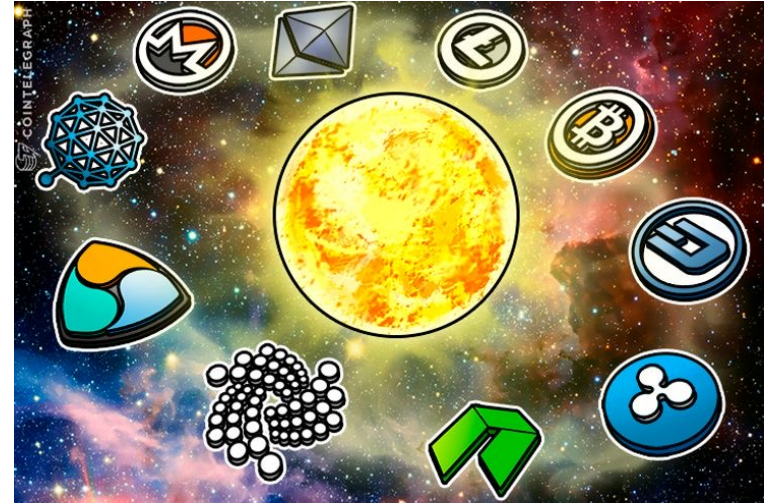
Compiler Version: **v0.5.0+commit.1d4f565a** Other Settings: **default evmVersion, None license**

Contract Source Code (Solidity)

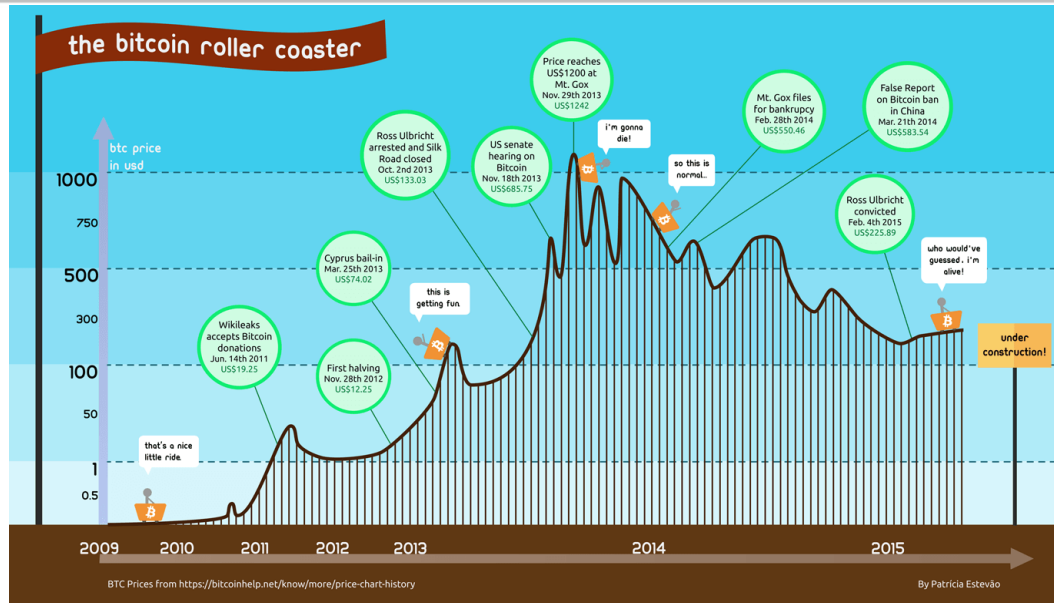
```
29  * @dev Moves `amount` tokens from the caller's account to `recipient`.
30  *
31  * Returns a boolean value indicating whether the operation succeeded.
32  *
33  * Emits a `Transfer` event.
34  */
35  function transfer(address recipient, uint256 amount) external returns (bool);
36
37  /**
38   * @dev Returns the remaining number of tokens that `spender` will be
39   * allowed to spend on behalf of `owner` through `transferFrom`. This is
40   * zero by default.
41   *
42   * This value changes when `approve` or `transferFrom` are called.
43   */
44  function allowance(address owner, address spender) external view returns (uint256);
45
46  /**
47   * @dev Sets `amount` as the allowance of `spender` over the caller's tokens.
48   *
49   * Returns a boolean value indicating whether the operation succeeded.
50   *
51   * > Beware that changing an allowance with this method brings the risk
52   * that someone may use both the old and the new allowance by unfortunate
53   * transaction ordering. One possible solution to mitigate this race
```

What is cryptocurrency ?

- Cryptocurrency is a digital asset that can be exchanged.
- The "crypto" part stems from the use of cryptography for security and verification purposes during transactions.



What people are going crazy about it ??



Value of Bitcoin in 2010 – 0.1 USD

Value of Bitcoin in 2021 – 68,000 USD

Why hackers love it ?

Because it is :

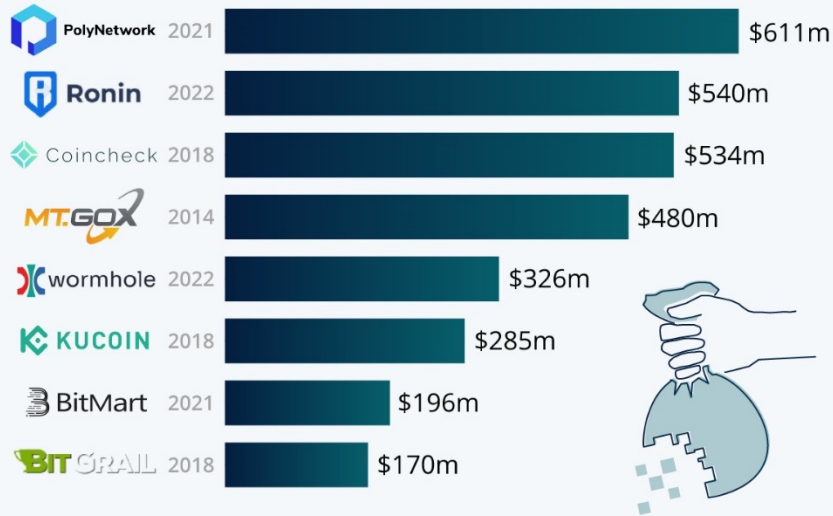
- Digital
- Decentralized
- Global
- Unregulated
- **Anonymous**



Outcome !!

The Biggest Crypto Heists

Largest known crypto currency thefts by estimated losses*



* According to crypto currency exchange rates at time of theft

Sources: Reuters, Blockchain Companion, Decrypt



statista

- January to November 2022, hackers stole \$4.3 billion worth of cryptocurrency
- Americans lost \$329 million to cryptocurrency scams in Q1 2022
- Investors in Hong Kong have lost \$50 million to cryptocurrency scams in 2022.
- Young people (20 to 40) are more susceptible to crypto scams.



Some top hacks of 2022 !!

- Qubit Finance **bridge** exploit – \$80M
- Harmony **bridge** hack – \$100M
- BNB Chain **bridge** exploit – \$100M
- Nomad token **bridge** exploit – 190M
- Wormhole **bridge** exploit – \$321M
- Ronin **bridge** hack – \$612M

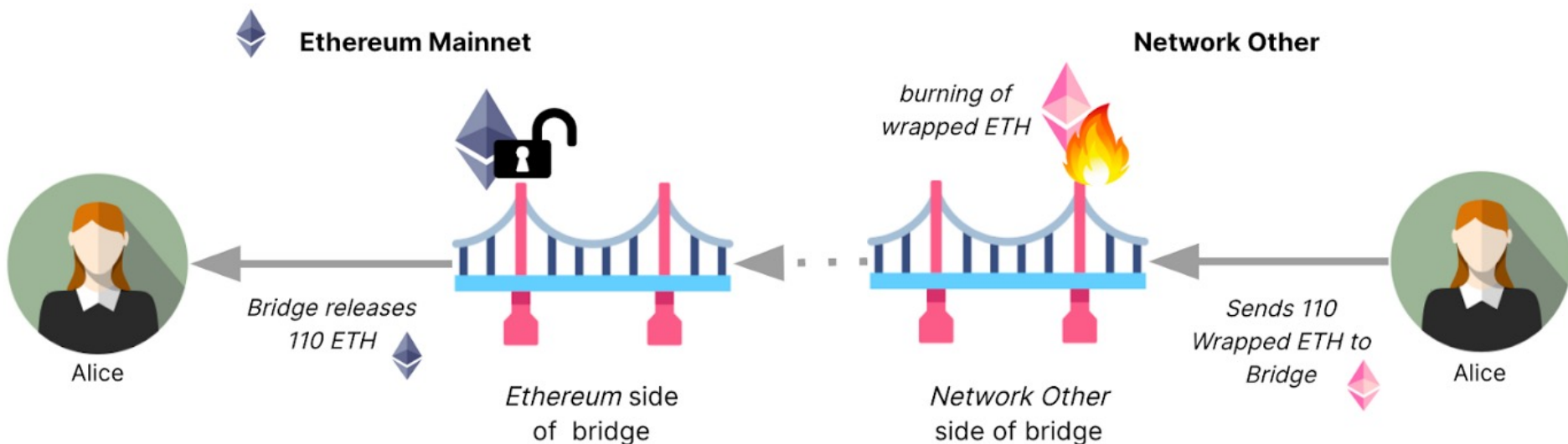


What is Bridge

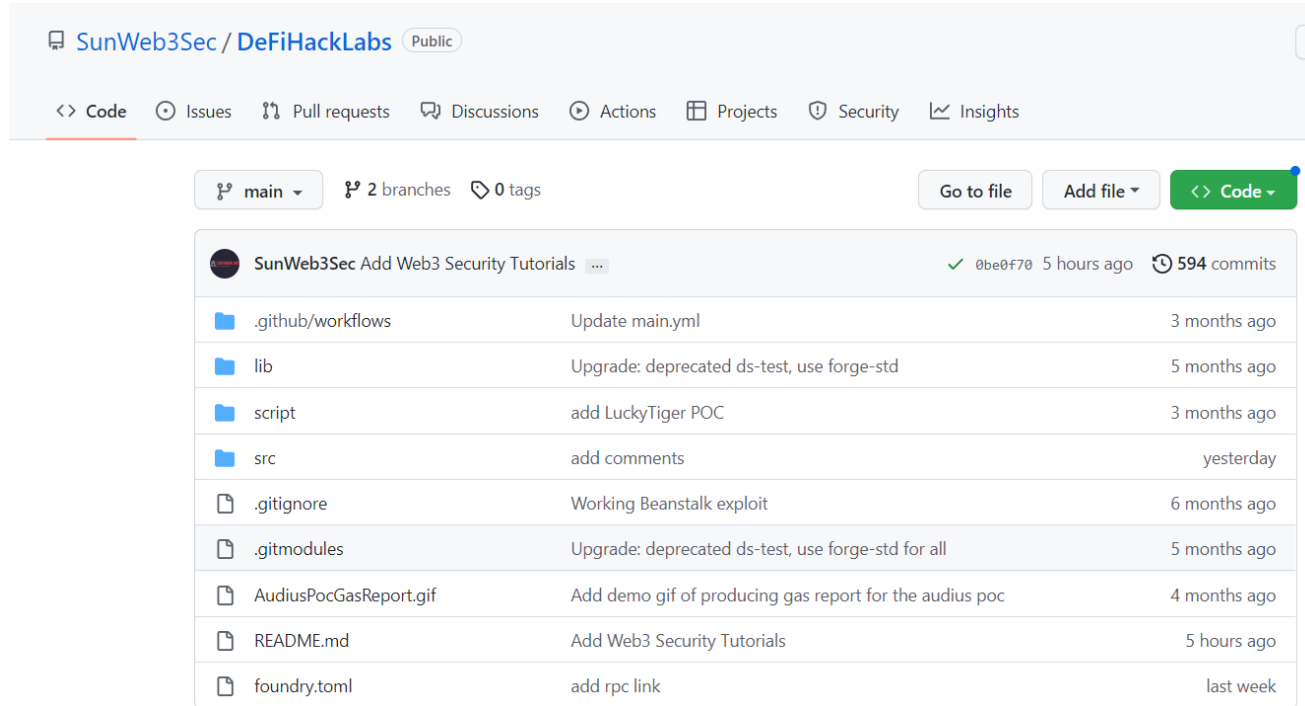


What is Bridge

Bridge allows users to transfer value from one chain to the other. if you have bitcoin but want to use it on ethereum, you can do that through a bridge.



Bridge Hack POC



SunWeb3Sec / DeFiHackLabs Public

<> Code Issues Pull requests Discussions Actions Projects Security Insights

main 2 branches 0 tags Go to file Add file Code

SunWeb3Sec Add Web3 Security Tutorials ... ✓ 0be0f70 5 hours ago 594 commits

github/workflows	Update main.yml	3 months ago
lib	Upgrade: deprecated ds-test, use forge-std	5 months ago
script	add LuckyTiger POC	3 months ago
src	add comments	yesterday
.gitignore	Working Beanstalk exploit	6 months ago
.gitmodules	Upgrade: deprecated ds-test, use forge-std for all	5 months ago
AudiusPocGasReport.gif	Add demo gif of producing gas report for the audius poc	4 months ago
README.md	Add Web3 Security Tutorials	5 hours ago
foundry.toml	add rpc link	last week

<https://github.com/SunWeb3Sec/DeFiHackLabs>

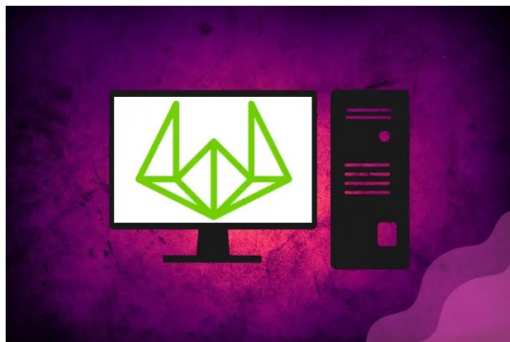


Bridge Hack Technical Analysis

 Numen Cyber Labs [Follow](#)
Sep 23, 2022 · 5 min read · [Listen](#)

[Save](#) [Twitter](#) [Facebook](#) [LinkedIn](#) [Link](#)

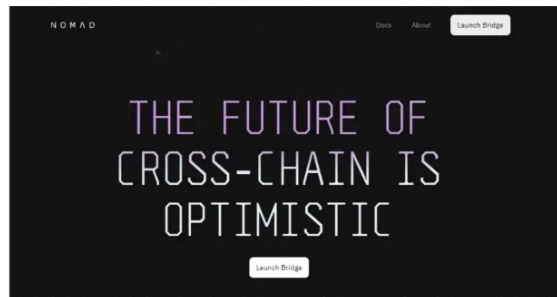
An Analysis of Wintermute's USD\$160 Million Hacking



 Numen Cyber Labs [Follow](#)
Aug 2, 2022 · 3 min read · [Listen](#)

[Save](#) [Twitter](#) [Facebook](#) [LinkedIn](#) [Link](#)

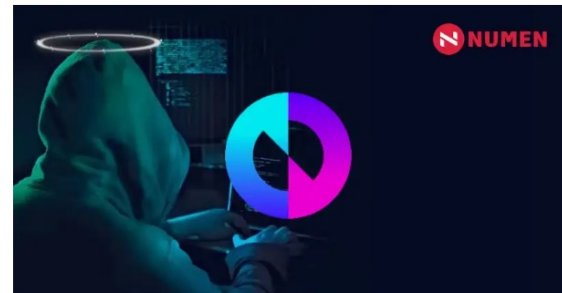
Nomad Bridge Attack Incident Analysis



 Numen Cyber Labs [Follow](#)
Nov 11, 2022 · 3 min read · [Listen](#)

[Save](#) [Twitter](#) [Facebook](#) [LinkedIn](#) [Link](#)

DFX Finance US\$4 Million Smart Contract Attack Analysis



Read the technical analysis of various bridge hack at Numen Cyber Blog

<https://medium.com/@numencyberlabs>

Fun Fact



Web3 fun fact

Can you guess the bug bounty amount given by Wormhole ?



Web3 fun fact

Can you guess the bug bounty amount given by Wormhole ?

USD 10 Million for 1 bug

The world of crypto scams



Bo Shen

Founder of Fenbushi Capital



Bo Shen 
@boshen1011



A total of 42M worth of crypto assets, including 38M in USDC were stolen from my personal wallet ending in 894 in the early morning of November 10 EST.

The stolen assets are personal funds and do not affect on Fenbushi related entities.

11:57 AM · Nov 23, 2022



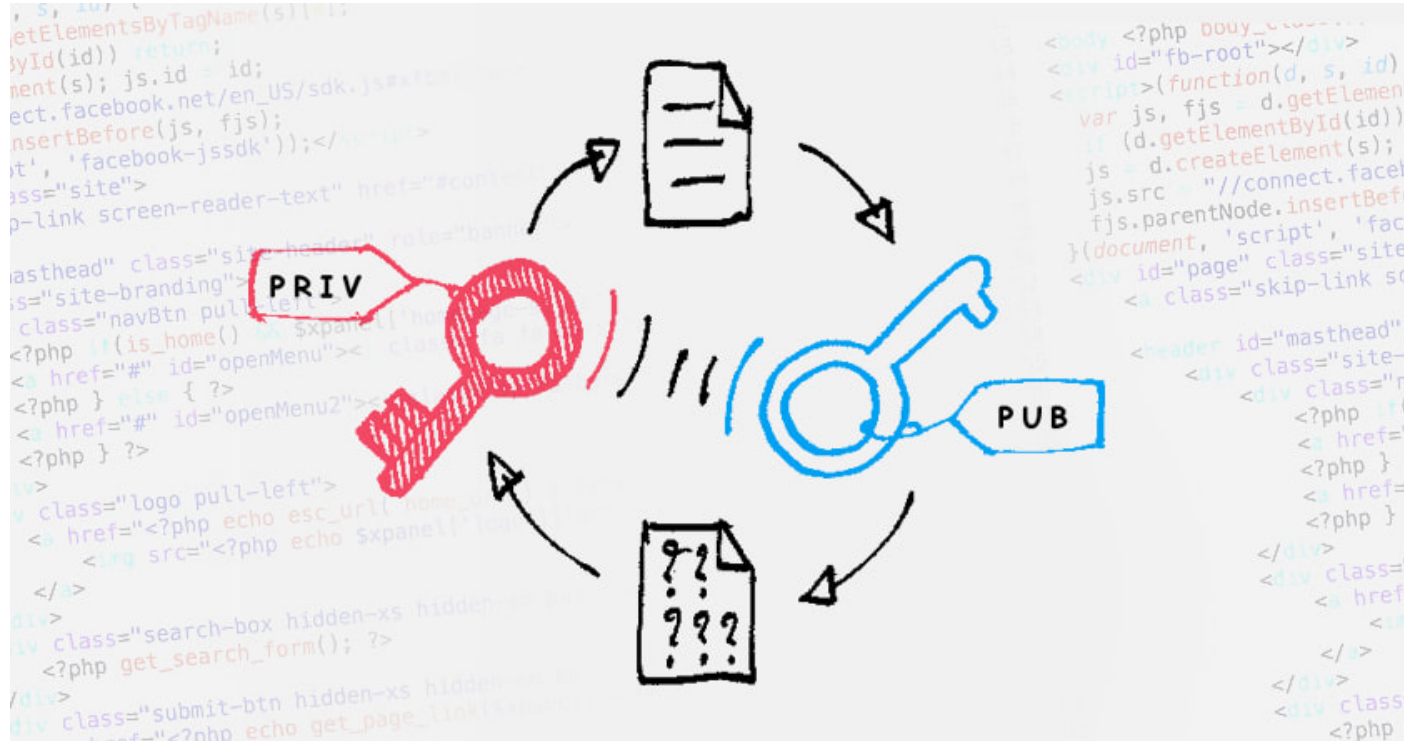
The world of crypto scams



Luke Dashjr
Bitcoin Developer

Crypto stolen : 200 BTC

Public Key and Private Key



Different types of wallets

CRYPTOCURRENCY WALLET



WEB



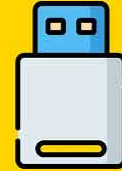
MOBILE



DESKTOP



PAPER



HARDWARE

How cryptocurrencies are stolen

Run an exchange – Just kidding



Clipper Change

- Attacker infects Known browser plugins .
- These Plugins detects cryptocurrency address and change the address to attacker address in clipboard

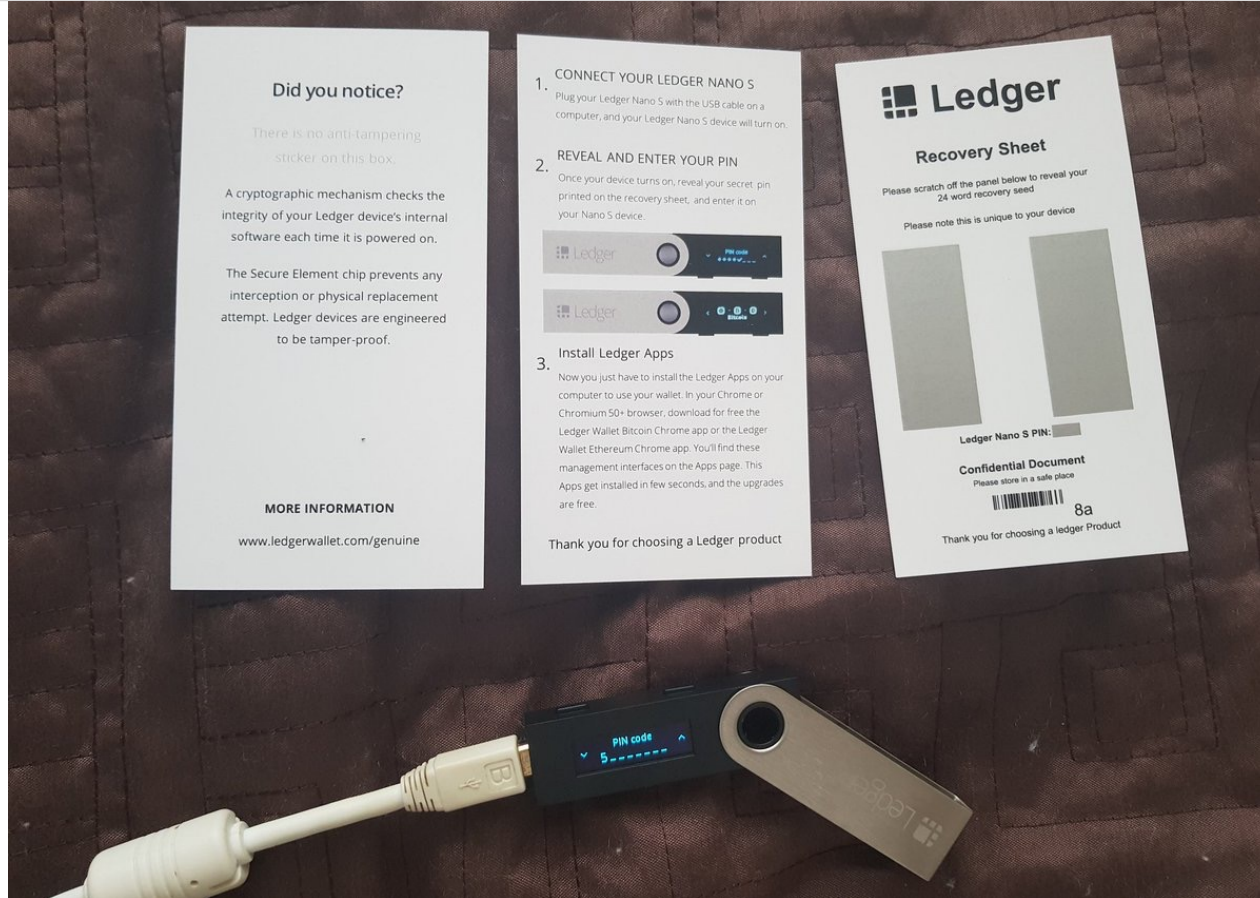


The image shows a screenshot of the Coingeograph website. At the top, there is a dark navigation bar with the Coingeograph logo and the tagline "The future of money". To the right of the logo, there is a table of cryptocurrency prices:

	BTC	XRP	ETH	BCH
Price	\$ 3,735	\$ 0.33	\$ 124	\$ 12
Change	+1.86%	+0.82%	+1.93%	+1.2%

Below the navigation bar, there is a yellow menu bar with links for "News", "Features", "Price Analysis", "Market Tools", "Cryptopedia", and "Inc". Below the menu bar, there is a dark banner with the text "Bitcoin Daily Trading Race.1 BTC Daily Grand". Below the banner, there is a profile picture of William Suberg and the text "By William Suberg" and "JUL 02". Below the profile picture, there is a large headline: "Report: 2.3 Million Bitcoin Addresses Targeted by Malware That 'Hijacks' Windows Clipboard".

Hardware Wallet seed attack



Cracking Private Key

In September 2022, users of Profanity, a vanity address generator for Ethereum, were the targets of a private key cracking attack.

Attackers took advantage of a weakness in the wallet's key generation process to access and drain millions in tokens from users' wallets.

Crypto stolen : USD 3.3 million

Cracking Private Key

While most Ethereum wallet addresses are random, these vanity addresses are designed to contain a particular word, such as someone's name, somewhere within the address

Generation of random values, such as private keys, is commonly performed using a cryptographic pseudorandom number generator (CPRNG) seeded with a random value.

In this case, Profanity seeded the CPRNG with an unsigned integer, meaning that there were only 2^{32} (about 4.3 billion) possible seed values.

Cracking Private Key



A set of 1,000 GPUs could theoretically brute force the private keys of every 7-character vanity address generated using Profanity within 50 days.

And while this operation would be expensive, the return on investment could be significant.

Hacked Mobile Apps

- Attackers compromise known crypto apps or make clone apps to get information like :
 - Private keys
 - 2FA
 - OTP , etc



Hackers are using blacklisted bitcoin apps to steal money and personal data, according to research

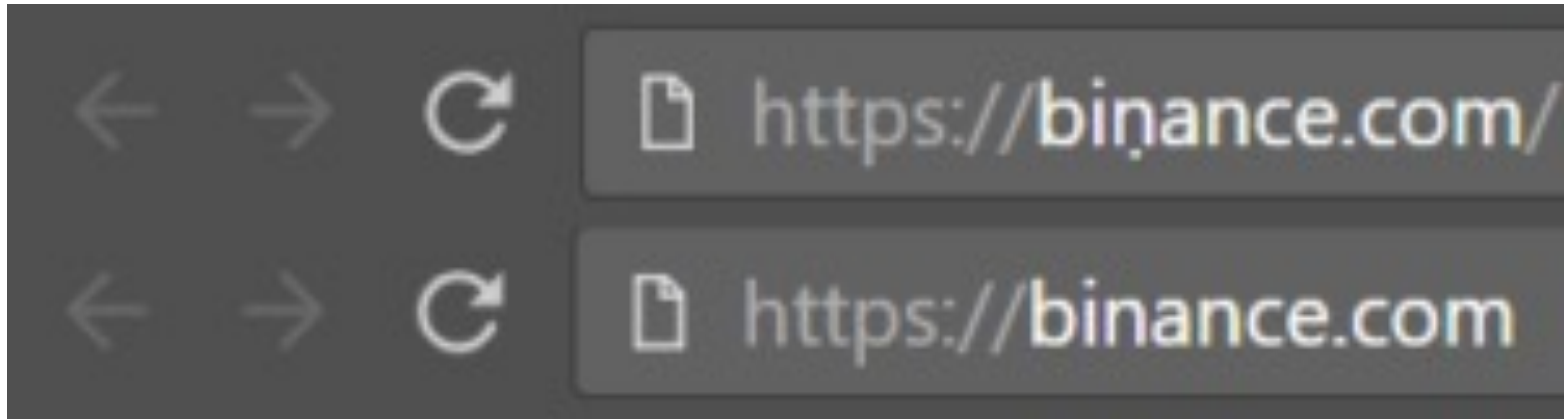
- The research found that 661 blacklisted cryptocurrency apps were found across 20 app stores including Apple's App Store, Google Play and others.
- Google Play hosted the highest amount of malicious crypto apps, the report said, with 272 available for download on the app store.
- Hackers have used apps including phrases like "bitcoin exchange," "bitcoin wallet" and "cryptocurrency" to lure potential victims, according to the report.

Ryan Browne | [@Ryan_Browne_](#)

Published 6:06 AM ET Wed, 24 Jan 2018 | Updated 8:50 AM ET Wed, 24 Jan 2018



Phishing / Clone sites



Private Key reveal Attack

- Attacker gives his private key victim (Mostly Ethereum)
- Account is loaded with ERC 20 tokens worth thousands of dollar
- Victim falls into the trap as the account contains thousands of dollar worth tokens



Private Key reveal Attack

- Victim fails to transfer it as Ethereum is needed to transfer ERC 20 based tokens.
- Victim transfers few ethereum to the account in the hope of getting the tokens
- Once ethereum is sent to the account, it gets auto transferred to some other account of the attacker



Fake Account (Social Engineering)



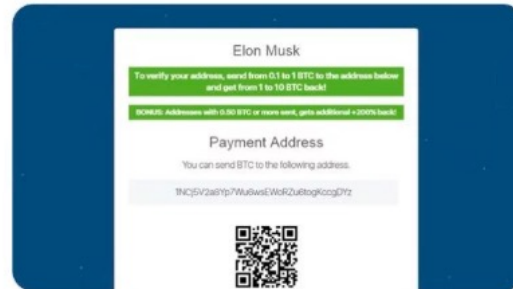
Elon Musk  [@patheuk](#)

I'm giving 10 000 Bitcoic (BTC) to all community!

I left the post of director of Tesla, thank you all for your support!

I decided to make the biggest crypto-giveaway in the world, for all my readers who use Bitcoin.

Participate in giveaway - [spacex.plus](#)

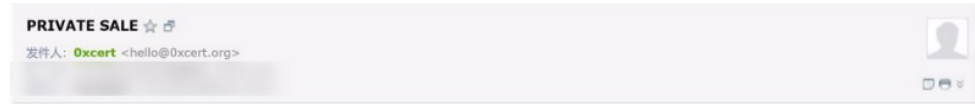
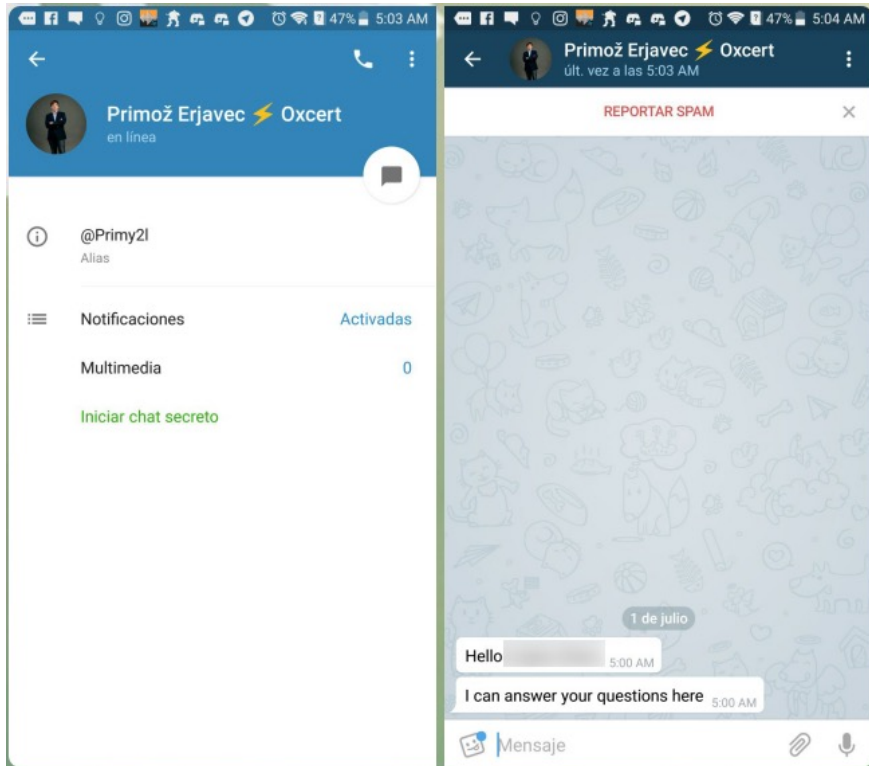


200 339 1,284

 Promoted



Telegram DM / Compromised Email List



Congratulations!

You are now ready to contribute in the **PRIVATE SALE** and **earn a bonus of 40%**

Important

- SEND your investment amount to the ETH address below.
- You shall receive a token purchase confirmation via email.

Scan QR code to send ETH or send to address below QR code



Google Ads

The image shows a Google search interface for the term "shapeshift". The search bar contains the text "shapeshift" and has a microphone icon and a search icon to its right. Below the search bar are navigation tabs for "All", "News", "Images", "Videos", "Maps", "More", "Settings", and "Tools". The "All" tab is selected. Below the tabs, it says "About 2,670,000 results (0.36 seconds)".

The search results are as follows:

- ShapeShift Bitcoin Exchange - How to work ShapeShift**
www.shapeshift-io.com/ ▼
ShapeShift is revolutionary part of the cryptocurrency ecosystem
BTC Cash, Ethereum Classic · Bitcoin, Ethereum, Monero
- ShapeShift | Cryptocurrency Exchange | Simple Coin Conversion** ✓
<https://shapeshift.io/> ▼
ShapeShift.io is the leading instant digital asset exchange, supporting dozens of blockchain tokens including Bitcoin, Ethereum, Monero, Zcash, Dash, Dogecoin ...

On the right side, there is a knowledge panel for "ShapeShift Company".

How to secure your cryptocurrencies in 2023

***NOT YOUR KEYS.
NOT YOUR COINS.***

Hardware wallets





Thank you
for your attention

Contact us at

+65 6355 5555

contact@numencyber.com

Find us at

