The State of BlockSec 2021:

The Good, The Bad, and The Ugly

Peter Kacherginsky, Blockchain Security Engineer @Coinbase

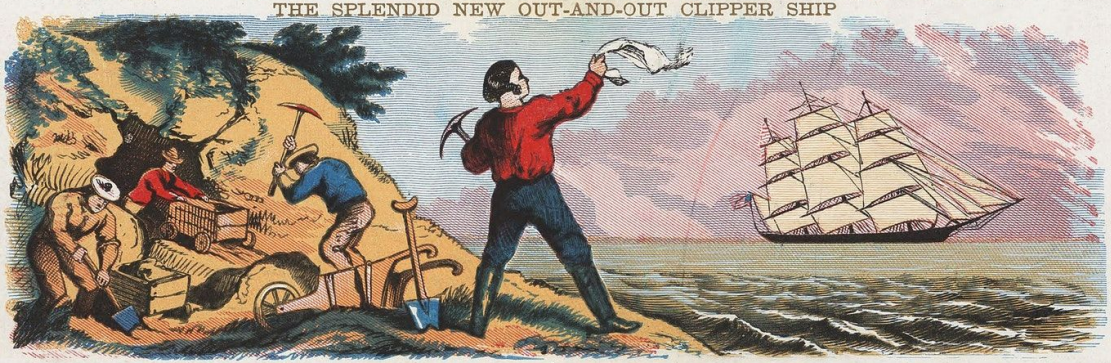
'UNCHAINED' BLOCKCHAIN SECURITY CONFERENCE 2021

A NEW AND MAGNIFICENT CLIPPER FOR SAN FRANCISCO.

MERCHANTS' EXPRESS LINE OF CLIPPER SHIPS!

Loading none but First-Class Vessels and Regularly Dispatching the greatest number.

THE SPLENDID NEW OUT-AND-OUT CLIPPER SHIP



CALIFORNIA

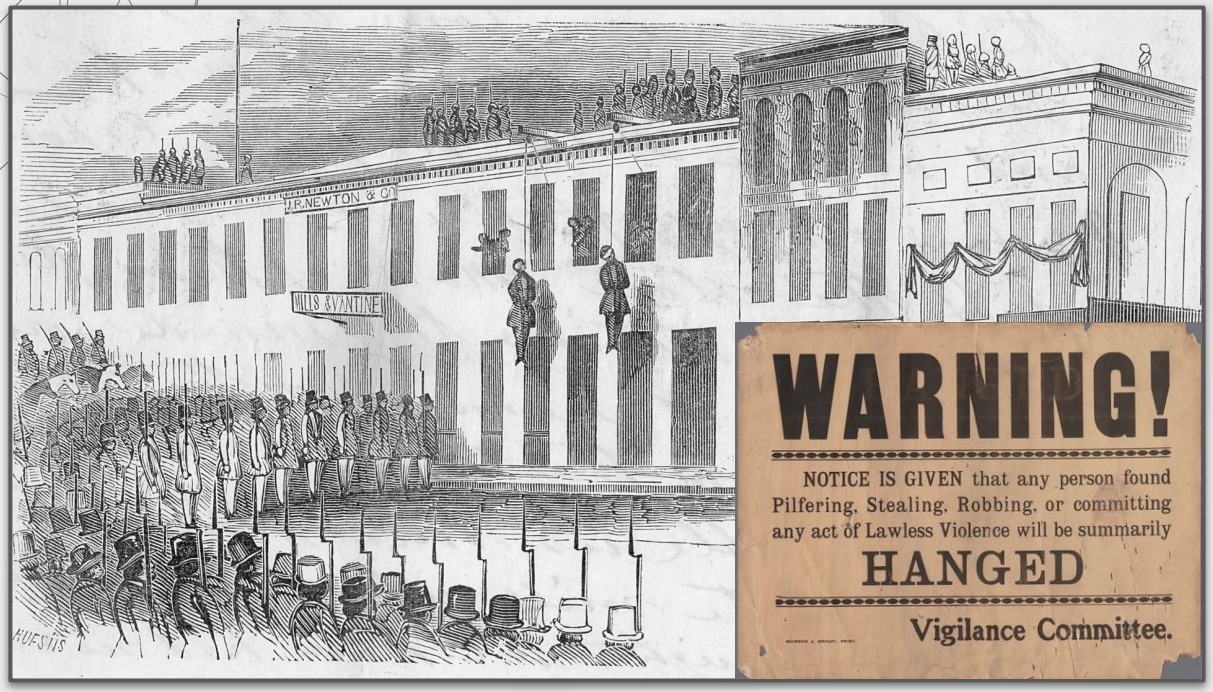
HENRY BARBER, Commander, AT PIER 13 EAST RIVER.

This elegant Clipper Ship was built expressly for this trade by Samuel Hall, Esq., of East Boston, the builder of the celebrated Clippers "SURPRISE," "GAMECOCK," "JOHN GILPIN," and others. **She will fully equal them in speed!** Unusually prompt dispatch and a very quick trip may be relied upon. Engagements should be completed at once.

Agents in San Francisco,
Messrs. DE WITT KITTLE & CO.

RANDOLPH M. COOLEY, 88 Wall Street, Tontine Building.

NESBITT & CO., PRINTERS.


J.R.NEWTON & CO
MILLS & VANTINE
HUESTIS
WARNING!
NOTICE IS GIVEN that any person found Pilfering, Stealing, Robbing, or committing any act of Lawless Violence will be summarily
HANGED
Vigilance Committee.

Peter Kacherginsky

Blockchain Security Engineer @Coinbase - BlockSec
- **Blockchain Threat Intelligence** newsletter
- **Capture the Coin** CTF @Defcon
- **Break** blockchains and smart contracts
- **Secure** and **monitor** blockchain systems
-

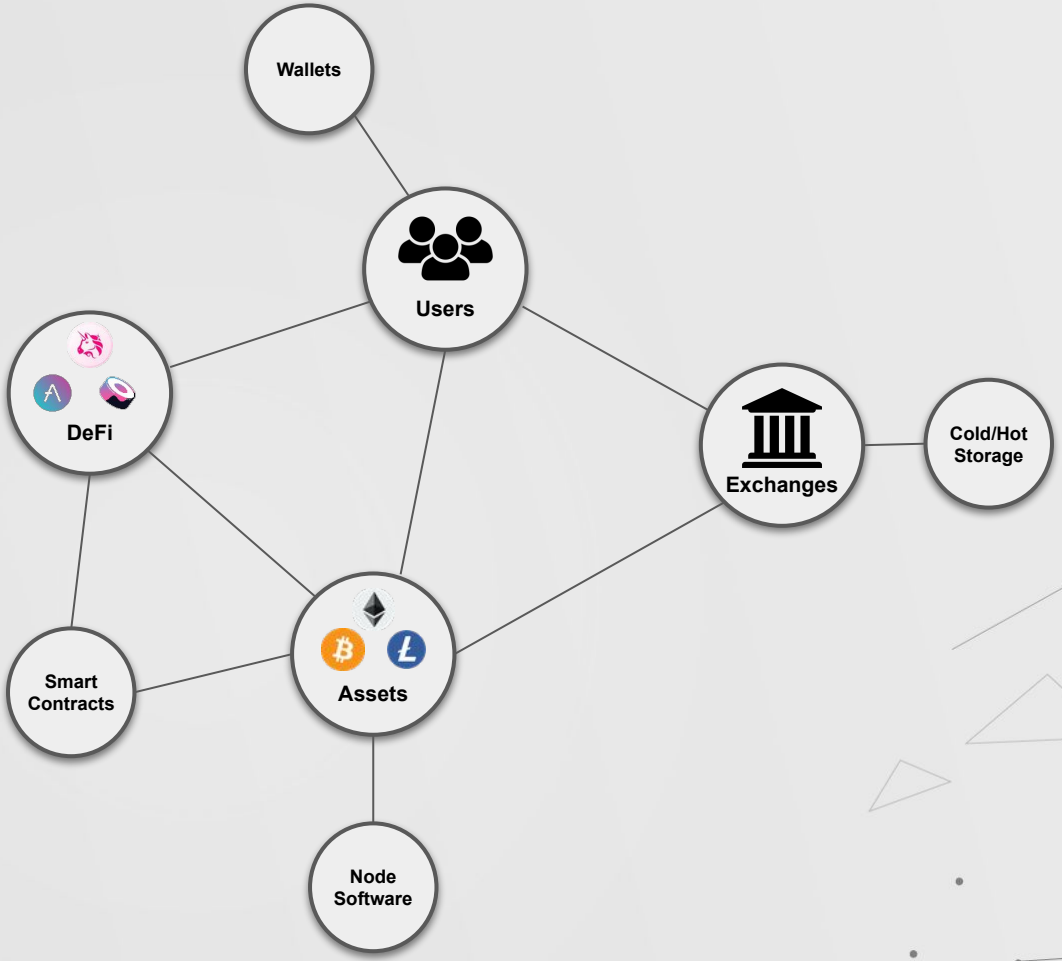
Malware Reverse Engineer @FireEye - FLARE Team
- FLARE VM, FakeNet-NG, Malware Training
- Lot's of APT **malware reversing**

Penetration Tester @Federal Reserve System - NIRT
- Password Analysis and Cracking Kit (PACK)
- **Breaking** Finance 1.0

@_iphelix

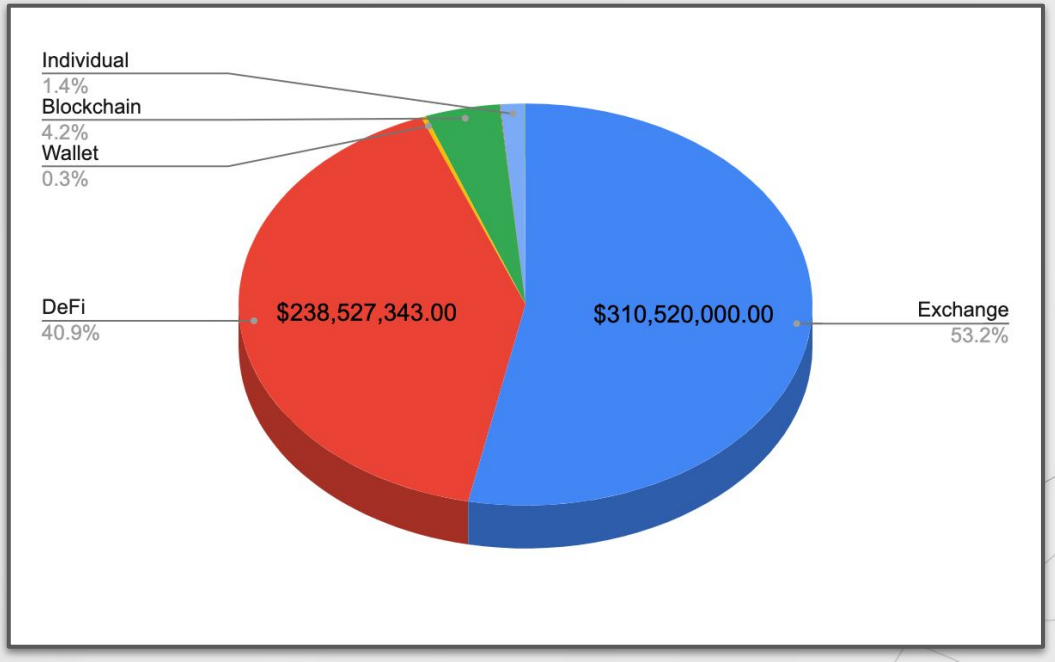
Blockchain Security

A new security field with the mission of securing and defending the cryptocurrency ecosystem.


Wallets
Users
DeFi
Exchanges
Cold/Hot Storage
Smart Contracts
Assets
Node Software


in THE GOOD,
THE BAD
AND THE UGLY

The Bad



Total stolen in 2020: $500M*

Exchange and Crypto Business Incidents: $310M

Exchange and Crypto Business Incidents

PII Theft

BLOCKFI

COINCHECK

BUYUCOIN

COINSQUARE

Stolen Funds

CASHAA

Exchange lost **$3.2M**. Employee laptop hacked.

ETERBASE

Exchange lost **$5.4M** in a hotwallet hack.

2GETHER

$1.3M stolen from the hotwallet

SHAPESHIFT

$1M stolen insider threat

Exchange and Crypto Business Incidents

LEDGER

1M+ emails and **292K** detailed customer PII stolen in two separate incidents.

KUCOIN

$281M stolen after the hotwallet was hacked. **Recovered 84%** of the lost assets.

FlyingAtom

$120K stolen and **two employees** injured in an armed robbery.

Exchange and Crypto Business Security Insights

- Are exchanges getting more secure?
  - **Increase** in the number of incidents since last year 2019 (21 vs. 11 in 2019)
  - **Increase** in the monetary damage ($310M* vs. $175M in 2019)

- Exchanges are working with **asset issuers to return the funds**. Who is liable?

- Attackers are getting creative (DNS infrastructure) and going after more than just a hotwallets (PII).

- **Insider** and **physical threats** are just as important to the overall exchange security.

DeFi Incidents: $230M

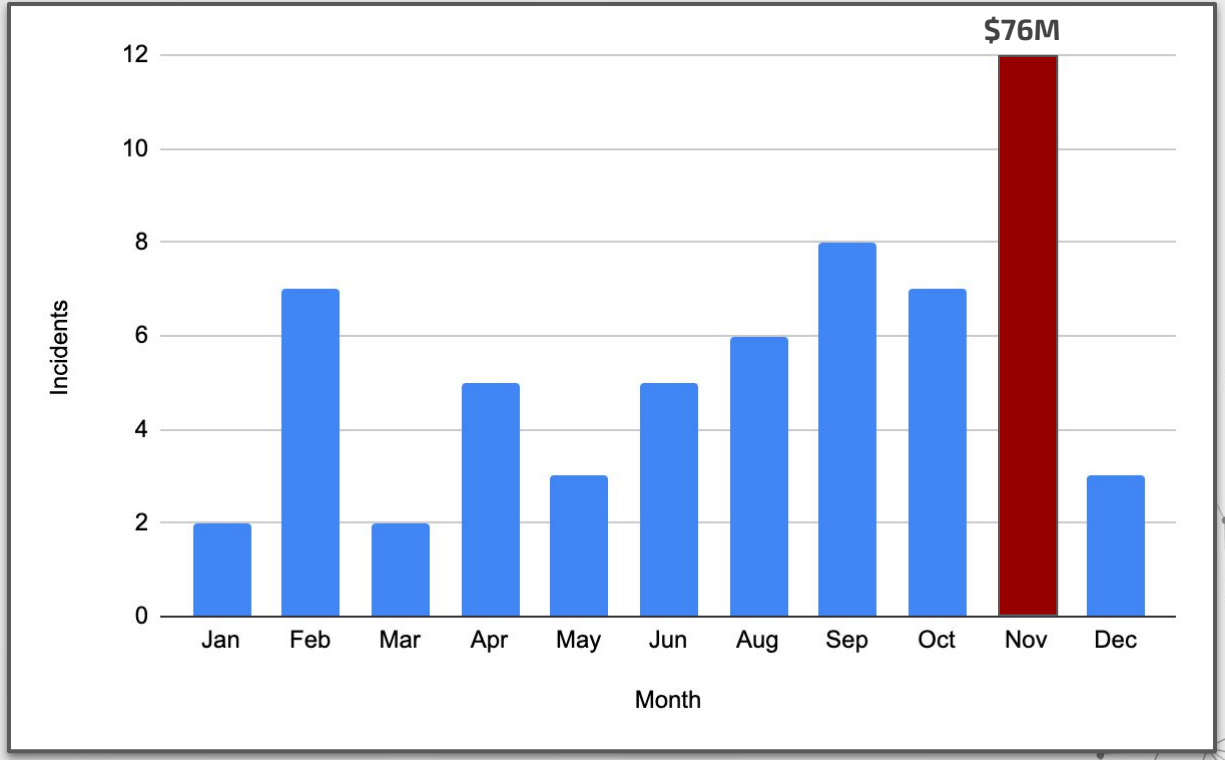
DeFi Incidents: 2020 H1 - $44M

Feb 12, 2020 - **MakerDAO $8.3M** liquidated.
Feb 15, 2020 - **bZx** relieved of **$350K**.
Feb 17, 2020 - **bZx** hacked again with **$630K** stolen.
Apr 18, 2020 - **Uniswap** imBTC LP drained of **$300K**.
Apr 19, 2020 - **dForce** Lendf.Me reentrancy exploit resulted in **$25M** theft.
Apr 25, 2020 - **Etheroll** exploited using chain forks with **$33K** stolen.
May 21, 2020 - **Hegic Options** was arbitraged out of **$3K**.
Jun 28, 2020 - **Balancer** exploited using deflationary tokens for **$500K**.
Jun 30, 2020 - **Vether** design flaw exploited for **$900K**.
Aug 04, 2020 - **OPYN** was double spent for **$371K**.

DeFi Incidents: 2020 H2 - $101M

Sep 03, 2020 - **SYFI** rebase mechanism exploited for **$280K**.
Sep 13, 2020 - **bZx** money printing bug resulted in **$8.1M** loss.
Sep 20, 2020 - **Soda Finance** exploited for **$160K**.
Sep 28, 2020 - **Eminence Finance** exploited for **$15M**.
Oct 25, 2020 - **Harvest Finance** exploited for **$24M**.
Nov 07, 2020 - **BSV Multi-sig** implementation exploited with **$90K** stolen.
Nov 12, 2020 - **Akropolis** reentrancy bug was used to steal **$2M**.
Nov 14, 2020 - **Value DeFi** hacked for **$7.4M**.
Nov 16, 2020 - **Origin Protocol** reentrancy bug exploited for **$7.7M**.
Nov 17, 2020 - **88mph** money printing bug hacked for **$100K**.
Nov 21, 2020 - **Pickle Finance** was relieved of **$19.7M**.
Nov 29, 2020 - **SushiSwap** “accidentally” exploited for **$15K**.
Dec 17, 2020 - **Warp Finance** oracle weakness exploited for **$7.8M**.
Dec 28, 2020 - **Cover Protocol** minting bug exploited for **$9.4M**.

Bloody November



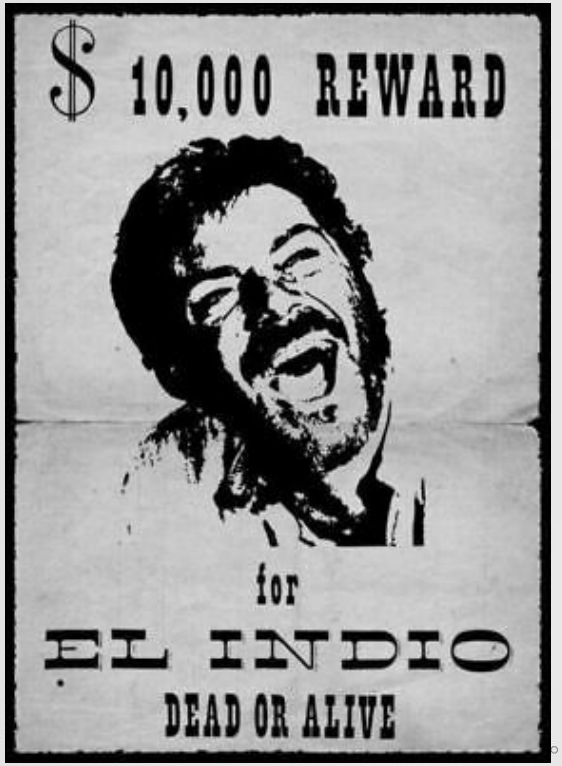
DeFi Incidents: 2021 Q1 - $63M

Jan 01, 2021 - **yCredit Finance** minting vulnerability. **$11M** lost.
Jan 19, 2021 - **Saddle Finance** high slippage exploited. **$275K** stolen.
Jan 27, 2021 - **SushiSwap** exploited for **$100K** due to misconfiguration.
Feb 04, 2021 - **Yearn** yDAI exploited for **$11M**.
Feb 08, 2021 - **Growth DeFi** rAAVE pool exploited for **$1.3M**.
Feb 09, 2021 - **BT.Finance** lost **$1.7M**.
Feb 12, 2021 - **Alpha Homora** v2 exploited. **$38M** stolen.

DeFi Incident Patterns

- **Oracle manipulation** (Warp Finance, Harvest Finance, etc.)
- **Arbitrage/Slippage** (Saddle Finance, Hegic Options)
- **Composability Attacks** (Uniswap imBTC, Balancer, etc.)
- **Logic Errors** (Pickle Finance, 88mph, Cover Protocol, bZx)
- Other smart contract vulnerabilities (e.g. reentrancy, bad math, etc.)
- **Flash loans** are not vulnerabilities.

Last week's bounty....



PRIMITIVE

Hacked its own contracts after vulnerability reported through ImmuneFi

HASHMASK

Patched NFT minting vulnerability after responsibly disclosed by samczsun

FORTUBE

Fixed permission bypass vulnerability after responsibly disclosed by samczsun

DEXTER

Whitehat hack of a vulnerability in Dexter to save users' funds.

DeFi Security Insights

- The year of DeFi hacks. **$230M+** stolen across **60 incidents**.
- About half were responsibly disclosed. **Bug bounties work!**
- Complex code and interactions between DeFi components introduce new classes of bugs.
- Going to see more unique smart contract targets (e.g. **NFTs**)


Netscape: Find what you're looking for - Netscape Search the Web
Back
Forward
Reload
Home
Search
Netscape
Images
Print
Security
Stop
Location: http://channels.netscape.com/search/searchtools.jsp
What's Related
cgisecurity.com
Web application news, and more
Web Application Security Services
Cross-site Scripting
Cross-site Request Forgery
SQL Injection
HOME
ABOUT CGISECURITY
SUBSCRIBE TO THIS SITE
« My experience coleading purple team | Main
Topics
Advertising
About
Contact
FAQ
Links
Books
Papers
Advisories
Contributions
Security Services
RFCs
Submit News
Tags
Announcements (78)
Articles (51)
Blue Team (1)
Books (1)
Browsers (77)
20 years of CGISecurity: What appsec looked like in the year 2000
Just realized that 20 years have passed since I started this site to learn more about web security threats.
What 'appsec' looked like in 2000
OWASP didn't exist yet, nor did WASC
Vulnerability disclosure was the wild west. Rain forest puppy (RFP) (that guy who discovered sqli) had just created the first attempt at vuln disclosure.
Nobody even had the concept of a bug bounty. Most of us were scared we'd go to jail (myself included) for reporting vulns.
There were no real web scanners (DAST) back then. The only one I was aware of was written by Bronc Buster
Static analysis tools like Fortify didn't exist.
The term blog wasn't used. Hence, I first called this a
ENHANCED BY Google
Search
Recent entries...
- 20 years of CGISecurity: What appsec looked like in the year 2000
- My experience coleading purple team
- oAuth nightmares talk
- Extensive IOS hacking guide released by Security Innovation
- Presentation: Problems you'll face when building a software security program
- Google's intentions are good, but implementation leave MORE users vulnerable to hacking than before
- My experience with developer security training
- A reminder that what you say at events may show up in unexpected places (like the news)
- Malicious CA's continue to cause

Blockchain Incidents: $20M

Blockchain Network Incidents: 2020

Bitcoin Gold

January 23-24, 2020
.Two 51% attacks with **29 block reorg**. 7167 BTG double spent.

Bitcoin Gold

July 10, 2020
Attempted 51% attack with a **1300 block reorg**. Notified by NiceHash miner. Issued **secret node with a checkpoint**.

Ethereum Classic

August 1, 2020
51% attack resulting in a **3692 block** reorg. **$5.8M** double spent.

Ethereum Classic

August 5, 2020
51% attack resulting in a **4244 block reorg**. **$3.2M** double spent.

Ethereum Classic

August 29, 2020
51% attack resulting in **a massive 7088 block reorg**. **$5M** double spent.

Blockchain Network Incidents: 2021

VERGE

560,000 block reorg (200 days). Hard-forked to add a checkpoint.

FIRO (ZCOIN)

360 block reorg. **$4M** double spent. **Locked** attacker's funds and **compensated Binance with a hard-fork**.

Blockchain Incidents

- PoW coins with **easily rentable GPU hashpower** will continue getting 51% attacked.
- Bitcoin Gold **working with miners** to secretly deploy a checkpoints is a new pattern.
- **Checkpoints** and **hard-forks** to mitigate reorgs.
- Will blockchains be **liable to compensate** exchanges if hacked?

More Blockchain Incidents

SteemIt

Tron and a number of **exchanges colluded** to vote in a controlling set of validators. First of a kind DPoS attack.

Ethereum

Mempool manipulation to cause congestion to win **1000 zero-bid MakerDAO auctions**.

.

Bitcoin Cash ABC

Griefing attack against Bitcoin Cash ABC even at a **personal loss**.

.

Monero

Monero Sybil attack likely connected to **U.S. Treasury bounty** to deanonymize the network.

.

More Blockchain Incidents

- SteemIt attack opens up **a new era of PoS and governance attacks**.
- Attackers are getting more creative (e.g. **mempool manipulation**)
- Not all attackers are **financially motivated**.
- Did we just witness the first **state sponsored attack**?

Blockchain Software Incidents: $6.7M

Node Incidents

SOLANA

Solana **testnet** node failed to validate transaction signatures. 500M SOL were stolen.

Tendermint

Multiple Tendermint DoS vulnerabilities when parsing invalid blocks. Results in a network halt.

.

FileCoin

Inflation bug discovered and exploited on **testnet**. 9B FIL minted.

.

Ethereum Parity

DoS vulnerability **exploited** disabling 13% of the network.

.

Ethereum Geth

DoS vulnerability **exploited** causing mass network outages including **Infura.**

.

Wallet Incidents

Monero Wallet

Monero wallet was **incorrectly parsing specially crafted coinbase transactions**. May result in invalid deposits displayed.

Lightning Network

Continuous stream of vulnerabilities disclosed which could lead to channel partner losing BTC.

.

Argent Wallet

Wallet takeover vulnerability was patched after responsibly disclosed by OpenZeppelin.

Ledger Live

RBF transaction mishandling may lead to social engineering attacks.

Supply Chain Attacks

Trinity Wallet

February 12, 2020
Wallet backdoored through a **3rd party dependency** to steal funds. **$1.6M** stolen.

RavenCoin

July 4, 2020
Inflation bug emergency patch. Bug was **maliciously introduced**. **$5.1M** minted and sold on exchanges.

Blockchain Software Security Insights

- RavenCoin stealth commit and Trinity **supply chain threats** will likely happen again.
- **Silently patching** vulnerabilities can backfire (Ethereum, Bitcoin).
- Node flaws are still rare. **Are there enough eyes?**

User Incidents: $8M (or Billions)

Ponzi Schemes

Wotoken Scam

Chinese police busted MLM scam organizers. **$1B** worth of crypto stolen from 715,000 victims.

Mirror Trading International

$589M in deposits stolen after MTI CEO disappeared with investor funds.

Crypto Giveaway Scams

SpaceX Scam

June 4, 2020

$200,000 worth of crypto lost in BTC giveaway scams on Youtube.

Twitter Hack

July 15, 2020

Attackers hijacked **130** exchange, celebrity, corporate accounts compromised to advertise BTC giveaway scam. **$120K** profit.

DeFi Scams - Backdoors and Phishing

- Jan 28, 2020 - Fake **MakerDAO** phishing website.
- Aug 24, 2020 - **Chicken Finance** owners stole deposits with a backdoor.
- Sep 23, 2020 - **UniCats** phished users with infinite allow. **$140K** stolen.
- Nov 02, 2020 - **Axion Network** backdoor used to steal **$24M**.
- Nov 29, 2020 - **Compounder Finance** backdoor used to steal **$12M**.

DeFi Scams - Exit Scams and Fake Tokens

- Sep 05, 2020 - **SushiSwap** creator **Chef Nomi** has ran off from the project.
- Oct 10, 2020 - **Blue Curby** pulled an exit scam with the **Off Blue** project.
- Nov 22, 2020 - **Fake Uniswap LP tokens** net scammers $52K.

More User Incidents

LEDGER DB Leak

1M+ emails + 292K detailed customer PII stolen in two separate incidents **leaked on a hacker forum.**

Backdoored Wallets

Trust Wallet fake in **Google Play Store**. Harry's epic hack to get users' funds back.

NM Founder Hack

$8M stolen after a personal computer targeted and **hacked** to install **backdoored wallet** software.

User Security Insights

- Highly **targeted** and **sophisticated** attacks on high net worth individuals.
- Technical and non-technical **scams on the rise**.
- **PII leaks** are powering phishing campaigns.
- MLM schemes are incredibly profitable ($1B Wotoken, $4B PlusToken).

The Ugly

Bad Actors

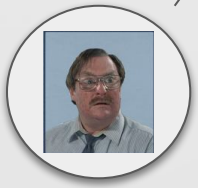
Backhats

State Sponsored

APTs

CryptoCore

Script Kiddies



Insiders

Fin/Ransomware Groups

Nation State APTs

Lazarus
(APT38)

Wicked
Panda
(APT41)

Ocean
Lotus
(APT32)

Criminal APTs

$350M*

Maze

NetWalker

REvil

TA505

$200M*

CryptoCore

* Chainalysis Crypto Crime 2021 Report

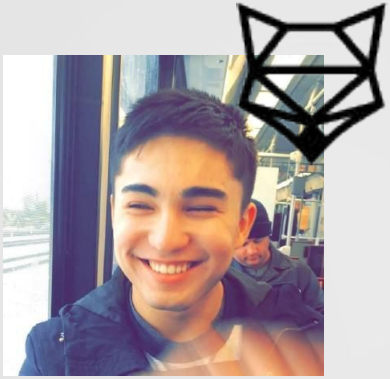
* ClearSky report on CryptoCore

Script Kiddie Threat

Twitter Hackers
“OGUsers”

“The Community” SIM swapping group

Insider Threat



Insider stole **$1M** from **Shapeshift**

Insider suspected in **$38M** heist from **Alpha Homora**

$3.2M stolen after employee's personal laptop with exchange wallet was hacked

DeFi Blackhats

Sergej Kunz, the CEO of 1inch.exchange — a decentralized exchange aggregator that the hacker used to exchange some of the funds — explained to Cointelegraph that the cybercriminal leaked important metadata about himself by directly using its web-based content delivery network, instead of the IPFS-based frontend.

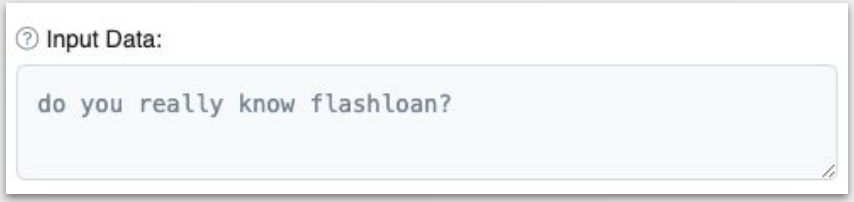
Specifically, all three exchange requests came from a single Chinese IP address, which suggests that the hacker did not use a decentralized network like Tor. Kunz theorized that this is a VPN or a proxy server, which may be liable to subpoenas.

The hacker is also known to have been using a Mac, revealing his screen's resolution and system language, which was set to "en-us."

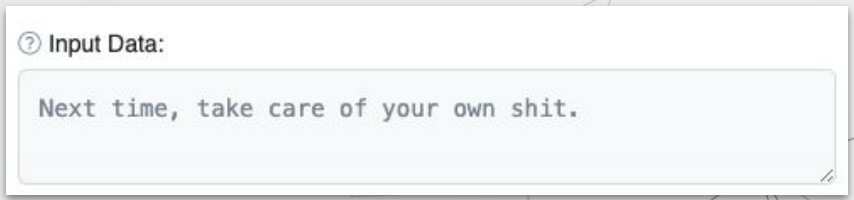
It is worth noting that this data is trivial to obfuscate, but the high amount of uncommon details in this metadata suggested to 1inch that it was simply an oversight. He concluded:

> **"He seems to be a good programmer, but an inexperienced hacker."**

dForce



Value DeFi



Cover Protocol

The Good

samczsun

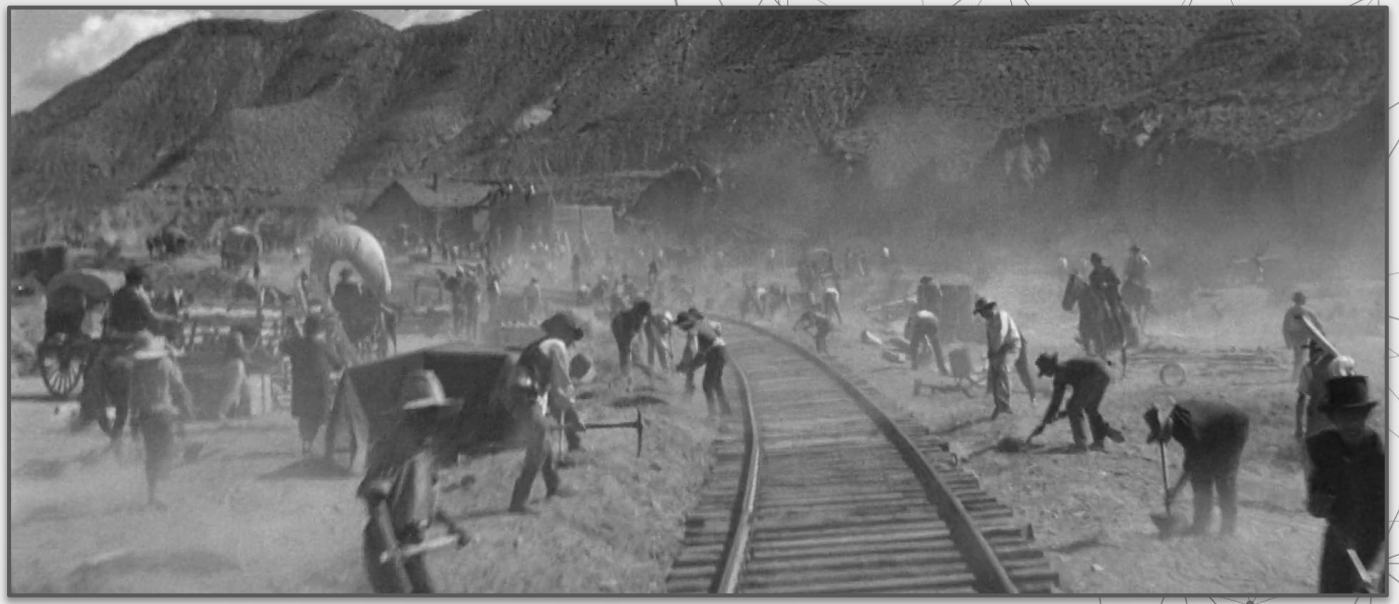
- Reported and helped fix vulnerabilities in **18** DeFi projects in 2020.
- He and a group of whitehats r**escued $9.6M** in a vulnerable project.
- Published a number of **blogs** and helped organize **Paradigm CTF** to share his knowledge with the community.

Harry Danley

- Intercepted and return **$5,000** worth of crypto from **Trust Wallet** phishers.
- Returned **$10,000** worth of crypto from two fake **Uniswap** and **Balancer** phishing campaigns.
- Helped take down countless fake apps and domains. Runs multiple projects such as **CryptoPhishing bot**, **CryptoScamDB**, and others.

Consensys Diligence

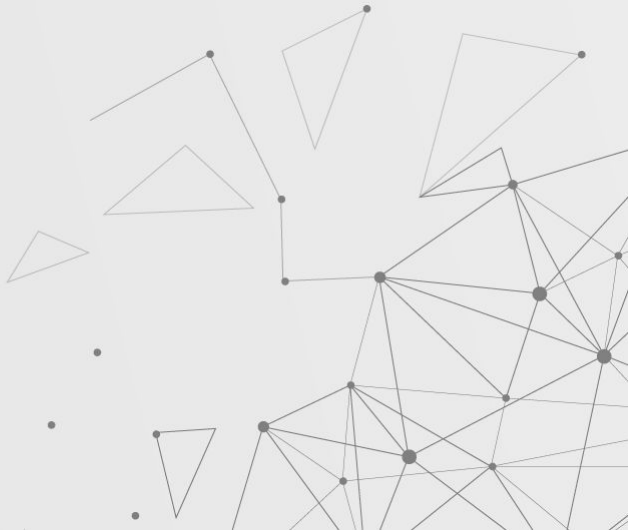
- Developed and freely released a number of tools and projects to the community: **Scribble**, **Teatime**, **Legions**, **Blockchain Security Database**, and a whole bunch of **VSCode extensions**.



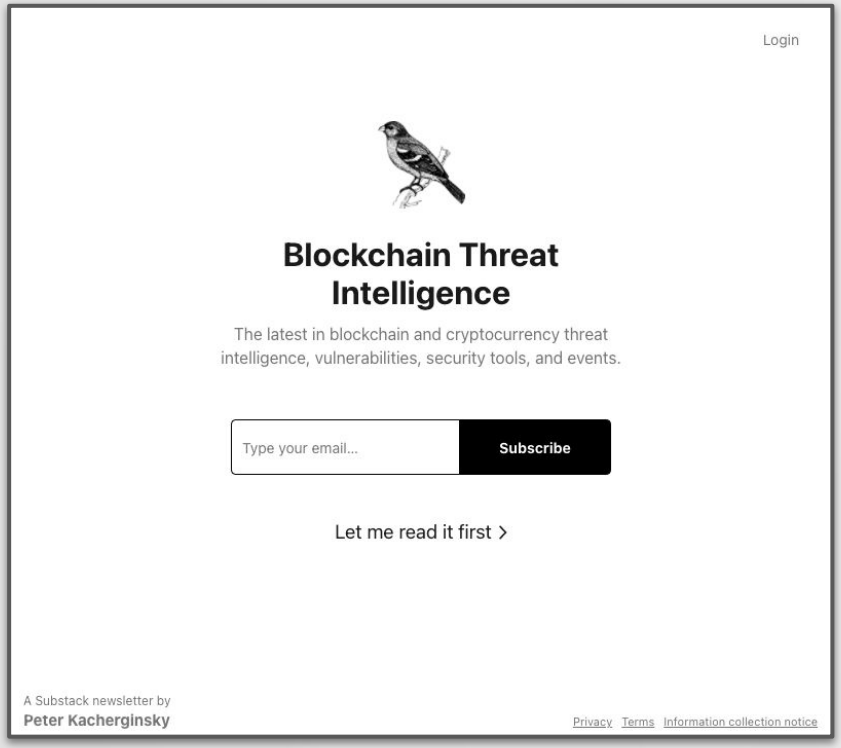
Building the frontier

Building the future together

- Develop guidelines, testing methodology, and tools for:
    - Stand-alone blockchains
    - Node configuration and operation
    - Hot/Cold storage
    - Key management
    - Protocol design
    - Wallet design
    - Blockchain forensics
    - User security
- Educational Resources, CTF Competitions, Trainings.
- More security professionals, bug bounty hunters, consulting companies.

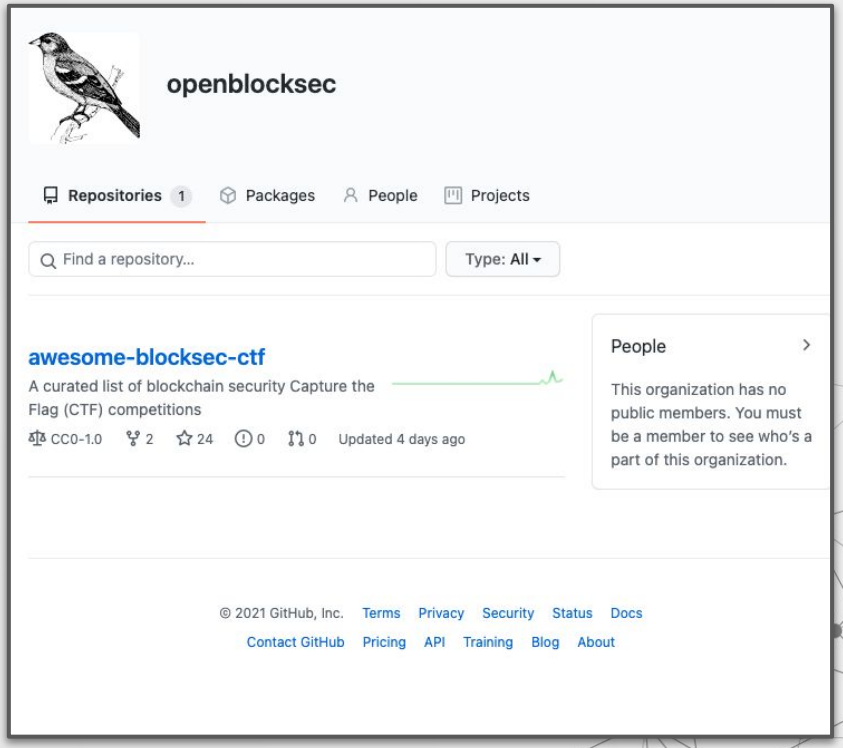


BlockThreat



http://blockthreat.substack.com

OpenBlockSec



http://github.com/openblocksec/


THE END