Stony Brook University

PragSec Lab

Double and Nothing:

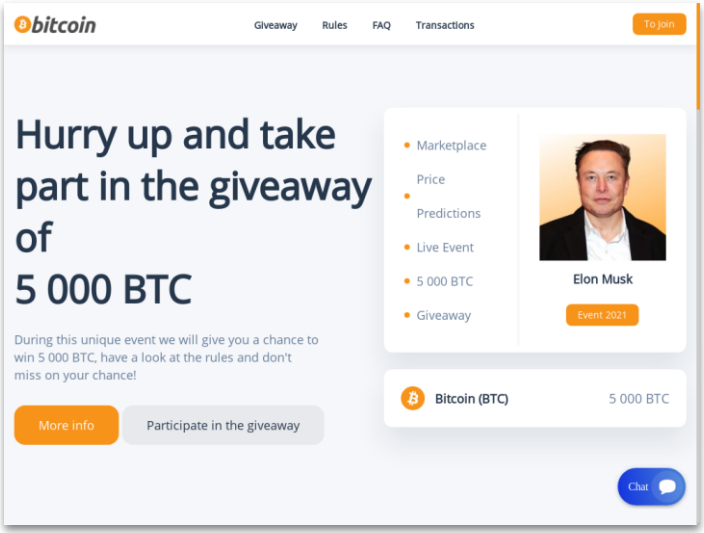
Understanding and Detecting Cryptocurrency Giveaway Scams

Xigao Li, Anurag Yepuri, Nick Nikiforakis

NDSS 2023

Introducing Cryptocurrency Giveaway Scams

- Professional-looking websites
- Abuse names and images of celebrities
- Advertise “giveaway events” that promise to multiply user funds
- Require cryptocurrency fund transfers to specific wallet addresses



Do you believe that?

No!

What if Obama and Biden said so?

Well …

A screenshot of (compromised) Obama's Twitter, posting scam messages during 2020 Twitter hack

- 2020 Twitter hack
  - 130 twitter accounts belonging to high profile individuals tweeting the scam
  - Celebrities affected: Barack Obama, Joe Biden, Bill Gates, Warren Buffett, etc.
  - More than US $110,000 were stolen

A screenshot of (compromised) Obama's Twitter, posting scam messages during 2020 Twitter hack

- 2020 Twitter hack
  - 130 twitter accounts belonging to high profile individuals tweeting the scam
  - Celebrities affected: Barack Obama, Joe Biden, Bill Gates, Warren Buffett, etc.
  - More than US $110,000 were stolen

Scammers advertise scams
through social media accounts and YouTube channels.

No existing large-scale studies of giveaway scams.

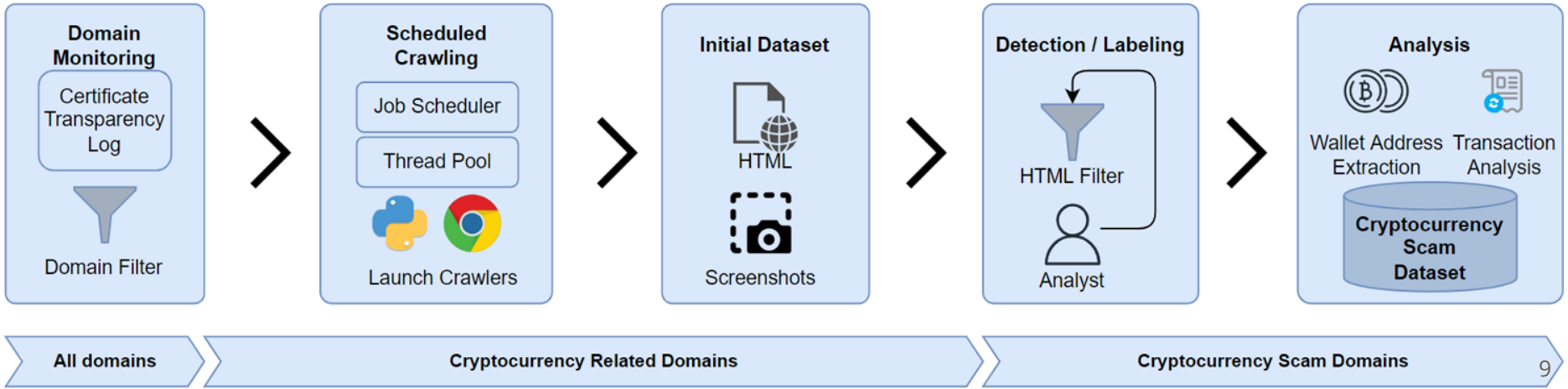
Overview

- First large-scale study of cryptocurrency scam websites
  - We design and implement **CryptoScamTracker**
  - Captured 10,079 scam websites in 6 months
- First quantitative analysis of cryptocurrency scams
  - Tens of millions of dollars stolen
  - Discovered clear signs of automation in setting up scam pages

 Our dataset is available at: *https://double-and-nothing.github.io/*

CryptoScamTracker Design

- CryptoScamTracker is composed of 3 modules:
  - Domain monitoring module
  - Crawling and detection module
  - Analysis module



CryptoScamTracker Design

- **Domain monitoring module**
  - Monitor Certificate Transparency (CT) logs with a keyword filter

CT Logs:
- *Append-only ledgers of certificates*
- *CAs add new entries when issuing new TLS certificates to websites*
- *Publicly available (anyone can monitor/verify)*

CryptoScamTracker Design

- **Domain monitoring module**
  - Monitor Certificate Transparency (CT) logs with a keyword filter
- **Crawling and detection module**
  - Send requests to suspicious scam domains, retrieve HTML code and screenshots of web pages, acquire domain information from WHOIS
  - Detect and store scam webpages by scam keyword filter
  - Extract cryptocurrency wallet addresses

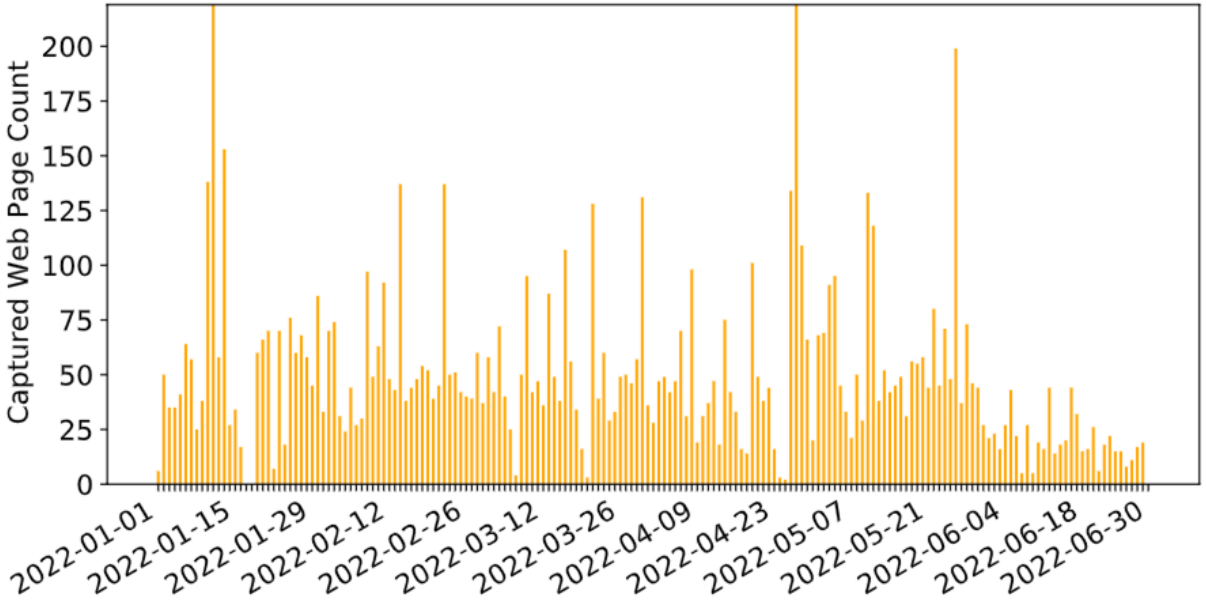
CryptoScamTracker Design

- **Domain monitoring module**
  - Monitor Certificate Transparency (CT) logs with a keyword filter
- **Crawling and detection module**
  - Send requests to suspicious scam domains, retrieve HTML code and screenshots of web pages, acquire domain information from WHOIS
  - Detect and store scam webpages by scam keyword filter
- **Analysis module**
  - Analyze HTML code, images, transactions, etc.

Dataset Collection

- Collected 6 months of data from January 1, 2022 to July 1, 2022.
- 10,079 cryptocurrency scam web pages
- 3,863 domains, 2,712 IP addresses
- 2,266 scammer wallet addresses extracted

Traffic Analysis



- Average of 55.7 new scam web pages each day

Domain analysis: domain name

- Scam operators prefer traditional gTLDs
  - .com, .org, .net
  - Total registration cost: $22,000+

TLD	Domain Count	Total estimated cost
com	1435	10274.6
org	762	5836.92
net	618	3083.82
us	156	154.44
info	127	247.65
live	113	212.44
io	74	2126.76
online	49	48.51
gift	42	556.08
tech	36	79.2
(Total)	3412	22620.42

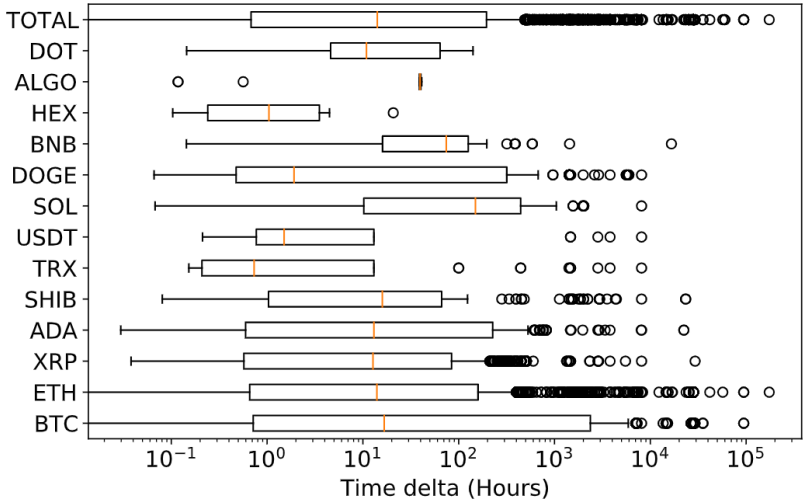
Domain analysis: domain name

- Scam operators prefer traditional gTLDs
  - .com, .org, .net
  - Total registration cost: $22,000+
- Scam domains tend to use certain keywords
  - 22-shib.com, 2022-ethereum.org
  - 38% domains contain “22” or “2022”,
  - 0.31% contain “21” or “2021”
  - 34.89% domains contain multipliers like “2x” or “3x”

TLD	Domain Count	Total estimated cost
com	1435	10274.6
org	762	5836.92
net	618	3083.82
us	156	154.44
info	127	247.65
live	113	212.44
io	74	2126.76
online	49	48.51
gift	42	556.08
tech	36	79.2
(Total)	3412	22620.42

Domain analysis: registration info

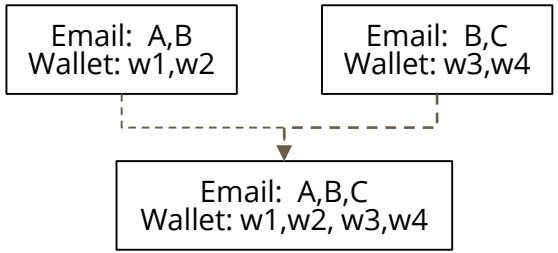
- Cryptocurrency scam websites rely on less popular hosting providers
  - Reg.ru, DDoS-Guard, etc.
    - Possibly bulletproof providers
  - DDoS-GUARD hosting 9.47% of all scam websites yet only 0.05% of benign top 10K websites
- Most domains have short “lifespan”
  - 50% websites have lifespan less than 26 hours
- Some names / personal emails are available in WHOIS info
  - Can be used for clustering scams into campaigns



Cryptocurrency Campaigns

Connect Emails / Wallet Addresses together

- Union-Find algorithm
- Join two clusters together if they share the same Email / cryptocurrency wallet addresses

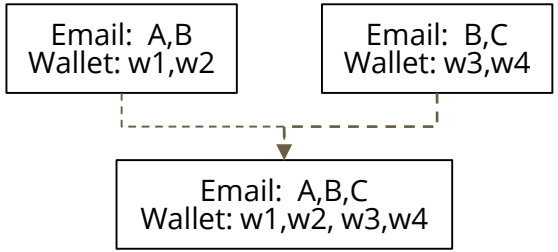


Campaign ID	# Sites	# Domains Involved	# Emails	# Wallet Addresses	# Cryptocurrencies Involved
1	1,621	3	1	2	2
2	1,360	835	46	395	10
3	155	69	6	21	7
4	116	19	1	30	6
5	71	36	1	9	7
6	69	35	2	18	5
7	63	16	4	11	3
8	45	21	2	11	3
9	45	15	2	8	5
10	41	30	5	21	6
(Total)	3,586	1,079	70	526	-

Cryptocurrency Campaigns

Connect Emails / Wallet Addresses together

- Union-Find algorithm
- Join two clusters together if they share the same Email / cryptocurrency wallet addresses

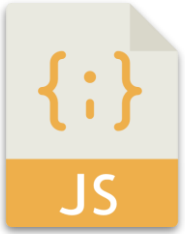


Campaign ID	# Sites	# Domains Involved	# Emails	# Wallet Addresses	# Cryptocurrencies Involved
1	1,621	3	1	2	2
2	1,360	835	46	395	10
3	155	69	6	21	7
4	116	19	1	30	6
5	71	36	1	9	7
6	69	35	2	18	5
7	63	16	4	11	3
8	45	21	2	11	3
9	45	15	2	8	5
10	41	30	5	21	6
(Total)	3,586	1,079	70	526	-

Cryptocurrency scam campaigns

- Greatest campaign: 1,621 websites
- Most widely registered: 835 domains

Webpage analysis: JavaScript



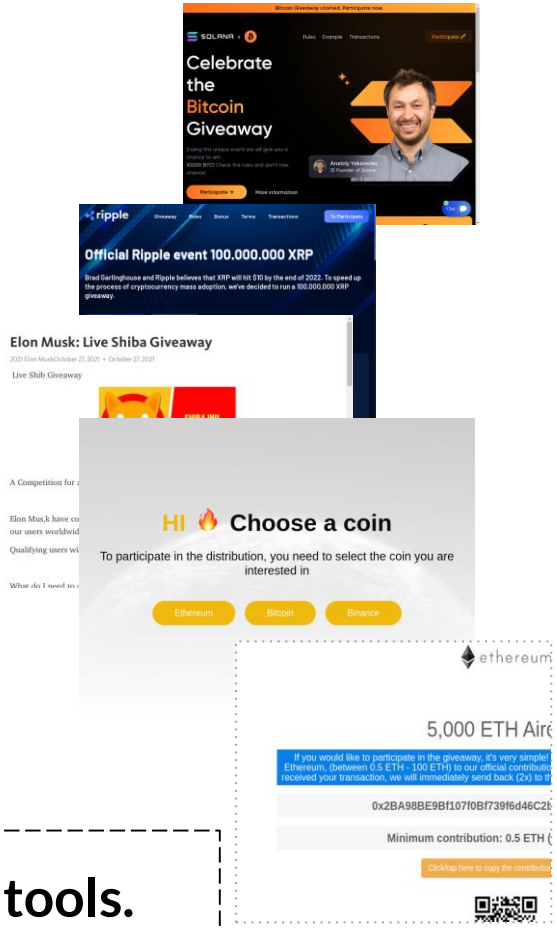
- Common JavaScripts are identified from scam web pages.
  - JQuery (12,795) - basic JavaScript library
  - **Live chat services (8,372)** - free chat-as-a-service library, which scammers used for persuading victim users
  - Animation Libraries (2363) - present smooth animation
  - Analytics (399) - Google / Yandex analytic metrics
  - Website Obscurity (476) - prevents user to inspect web page source

Third-party JS providers have the ability to detect scams, early in their lifetime

Image analysis: Webpage Layout

- Use perceptual hashing over 3,832 screenshots
  - Ultimately group screenshots into 139 clusters
- Image Clusters have 5 different styles

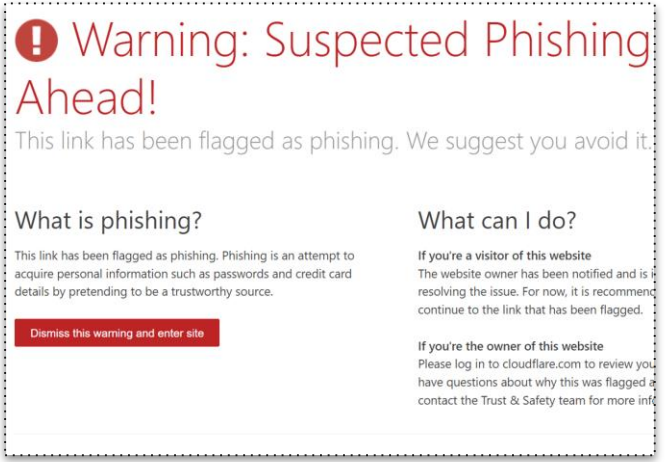
Style #	Style Detail	Clusters	Screenshots
1	Scam web page with celebrity portrait	44	907
2	Scam web page without celebrity portrait	22	430
3	Media article style	8	178
4	"Fork" style with two or more cryptocurrency	14	202
5	QR Code visible in first page style	2	26



Scam websites are created via automated tools.

Anti-scam techniques

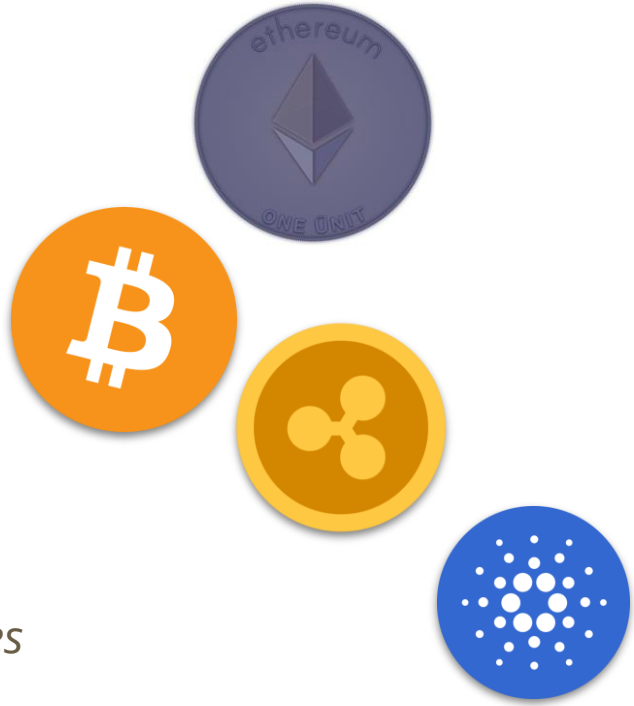
- Online crowd-sourcing databases: only capture a small percentage of domains and wallets in our dataset (CryptoScamDB: 0.35%, BitcoinAbuse: 14%)
- Domain blocklists: Only 16.75% domains we captured are marked suspicious/malicious by VirusTotal.
- Hosting provider regulations: Scammers evade regulations by using unpopular hosting providers (e.g REGRU, DDoS-Guard).



Existing detection systems have limited applicability to giveaway scams.

Targeted Cryptocurrency

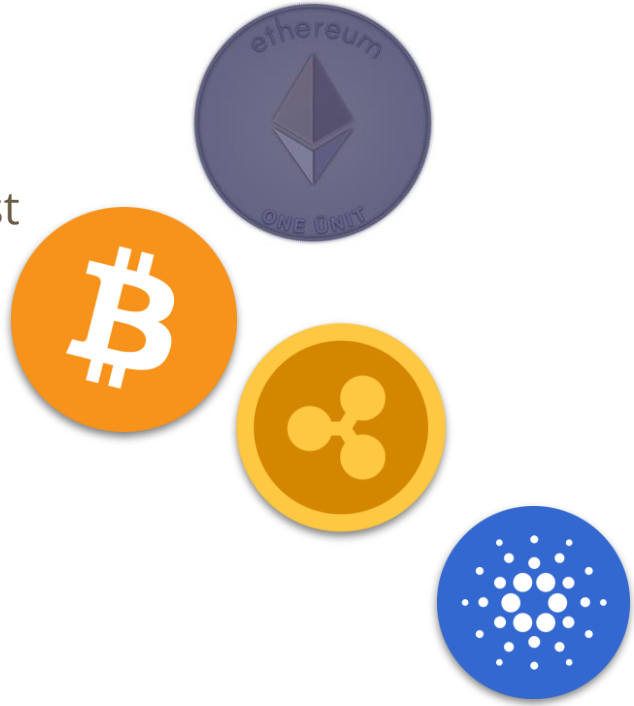
- Total of 13 cryptocurrencies are targeted
- Most favored cryptocurrencies:
    - Ethereum (ETH) - 6,777 scams
    - Bitcoin (BTC) - 5,980 scams
    - Ripple (XRP) - 1,303 scams
    - Cardano (ADA) - 818 scam



Top 4 cryptocurrencies attracted 90% of the scam websites in our dataset.

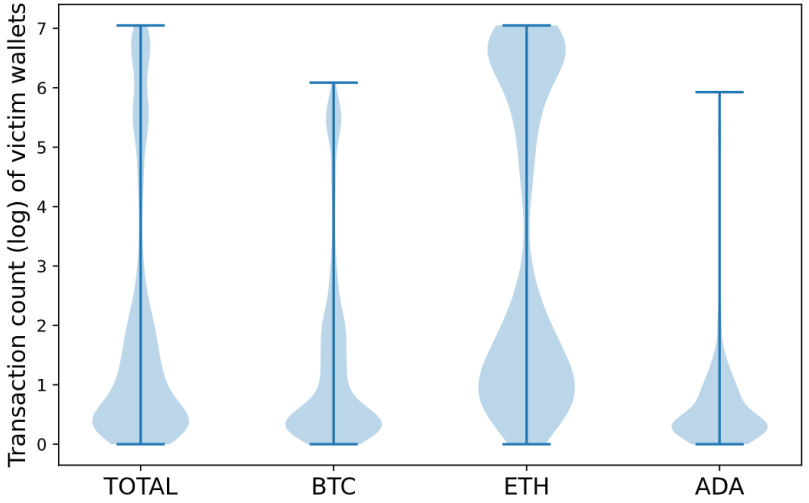
Funds Stolen

- Scammers' wallets are accessible on their respective blockchains, allowing us to track all past transactions.
- $24.9M–$69.9M funds were stolen by scammers
  (using the minimum and maximum cryptocurrency prices during our study)
- Total Stolen Cryptocurrency:
  - BTC: 940.07
  - ETH: 4,330.26
  - ADA: 2,141,876.52
  - XRP: 5,799,593.93



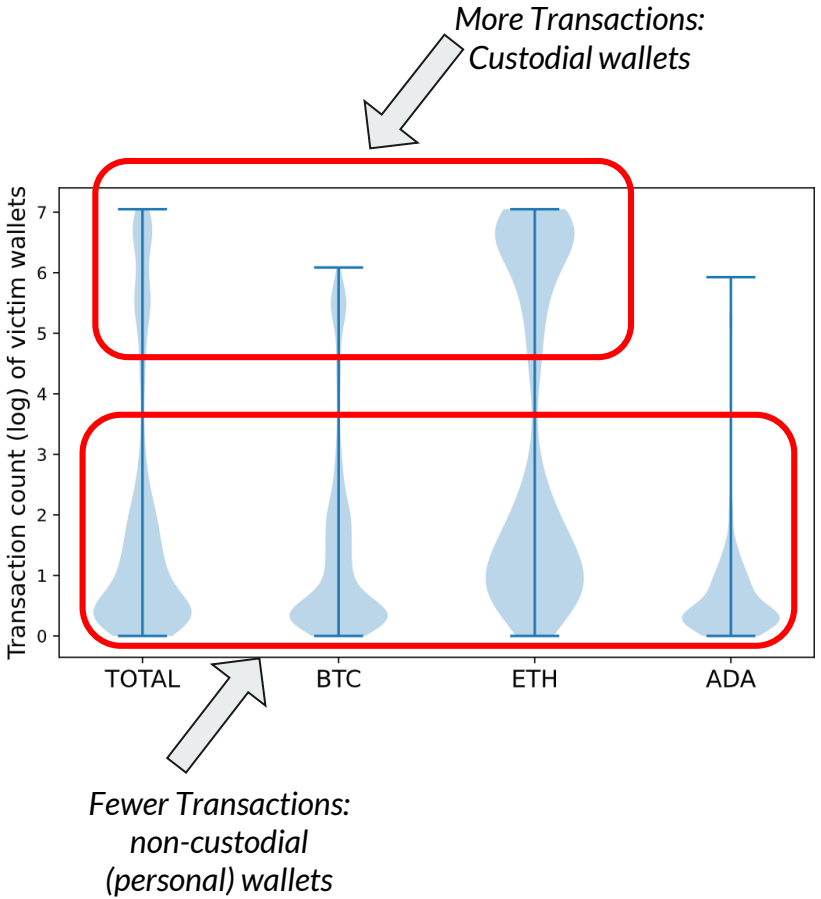
Exploring Victims

- 15,108 victims of scam were identified.



Exploring Victims

- 15,108 victims of scam were identified.
- Majority of victims use personal (Non-Custodial) wallets
  - Exchange-level blocklists will protect a limited number of users
  - Need to push defenses to the client software
- ETH victims use more Custodial wallet, i.e. online exchange platforms like Coinbase



Double and Nothing:

Understanding and Detecting Cryptocurrency Giveaway Scams

Xigao Li, Anurag Yepuri, Nick Nikiforakis

- CryptoScamTracker is effective in capturing cryptocurrency scam websites
- 10K scam web pages served from 3.8K domains are captured in our study
- $24.9M–$69.9M funds were stolen by Scammers
- Websites screenshots are similar, indicating they are deployed using automated tools
- Limited coverage by existing crowdsourced and automated defense systems
- Third-party JavaScript libraries may be a future way of detecting scams

Our dataset is available at: *https://double-and-nothing.github.io/*

Stony Brook University

PragSec Lab

Double and Nothing:

Understanding and Detecting Cryptocurrency Giveaway Scams

Xigao Li, Anurag Yepuri, Nick Nikiforakis

NDSS 2023

https://double-and-nothing.github.io/