Too Good To Be True: Exploring the Ecosystem of Cryptocurrency Giveaway Scams

Xigao Li, Anurag Yepuri, Nick Nikiforakis
PragSec Lab

Stony Brook University
Computer Science

What are Crypto Giveaway Scams?

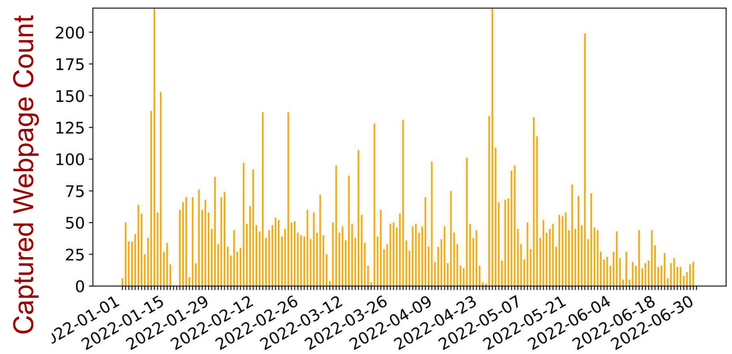
- Attackers set up professional-looking websites, abusing the names and images of celebrities to advertise "giveaway" events.
- Scammers promise to double or triple the funds that users send to a specific wallet address.
- Scammers then drive traffic to these websites through any means possible, e.g. Twitter and YouTube.
- Once users are convinced to send funds to a wallet, they will never get any funds back, and there is no way to reverse the transaction.

How to Capture Scam Websites

We design and build **CryptoScamTracker**, a tool that automatically identifies websites that are likely candidates for cryptocurrency giveaway scams.

- Domain monitoring module of CryptoScamTracker uses Certificate Transparency (CT) logs as input, processing millions of CT announcements each day with a keyword filter.
- Crawl Module collects domains from the monitoring module, schedules crawl jobs for all domains and collects the HTML code and screenshot of the webpage. Results are stored in a database for manual verification.
- Analysis Module analyzes the captured dataset to quantify attacker practices.

Websites captured by CryptoScamTracker



KEY TAKEAWAYS

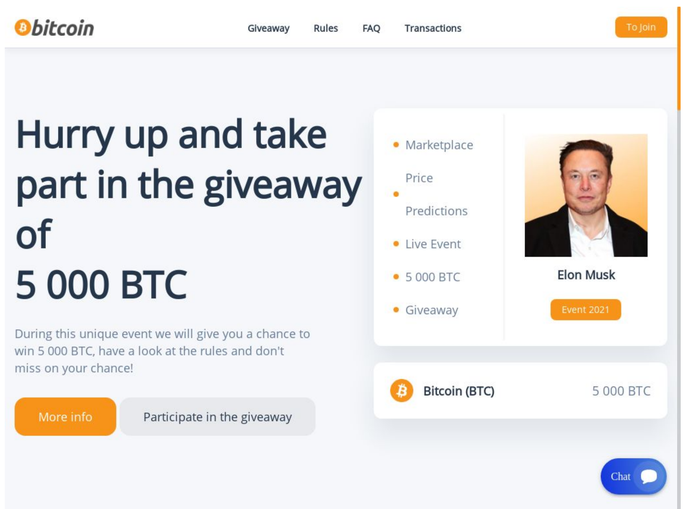
→ $24.9M–$69.9M funds were stolen by Scammers (using the minimum and maximum prices during our study).

→ Blocklists have limited coverage. Only 16.75% domains we captured are marked suspicious/malicious by VirusTotal.

→ Scammers tend to register high-cost traditional gTLDs and prefer unpopular hosting providers (e.g REGRU, DDoS-Guard).

→ Third-party JavaScript libraries such as live-chat services are a possible future way of detecting giveaway scams.

→ Most prolific scammers are responsible for large-scale campaigns operating hundreds of domain names across multiple cryptocurrencies.



Example of cryptocurrency scam web page

What do we know about scammers?

- Our **6-month** study collected **10K** cryptocurrency scam web pages served from **3.8K domains**; on average we capture 56 new web pages per day.
- 50% of scam web pages have a **short lifetime (less than 26 hours)**. The total cost for registering the domains serving these pages is **more than $23,000**.
- 2,312 website screenshots are clustered into **139 clusters with only 5 styles**, indicating they are created from same templates, possibly by automated tools.
- Current crowdsourced database only captures a small minority of CryptoScamTracker-identified domains and wallets (**CryptoScamDB: 0.35% BitcoinAbuse: 14%**)
- The most prolific scammers register hundreds of domains targeting users of all popular cryptocurrencies.