

Scammers make off with \$1.6 million in crypto

[i blog.group-ib.com/fake-crypto-giveaway](https://blog.group-ib.com/fake-crypto-giveaway)



08.04.2022

Fake giveaways hit bitcoiners again. Now on YouTube



Yaroslav Kargalev

Deputy Head of CERT-GIB Team



Daniil Glukhov

Junior Analyst, DRP Team

A few years ago, the cryptocurrency world shook under an onslaught of scammers who wanted to cash in on the outage of the popular messenger Telegram. Within a few hours, 5 crypto wallets advertised through a fake Twitter account supposedly belonging to Pavel

Durov received 148.364636 ETH, which is equivalent to about \$60,000 at the exchange rate on the reporting date.

Everything happened very fast. Just hours after Telegram first started experiencing technical issues on March 29, 2018, two identical tweets posted by the scammers posing as the founder of Telegram, Pavel Durov, appeared on a discussion thread in his official Twitter account. The tweets referred to a special promotion as part of an "apology campaign" to compensate users for the messenger's outage, thereby luring many of Durov's subscribers to a fake account.

In a shockingly similar case, last March, a man in Britain lost half a million dollars. This time scammers impersonated Elon Musk posting in a thread in his official Twitter account.

These all are typical example of a scam called a **Fake Crypto Giveaway**. This is how it usually plays out: fake Twitter accounts supposedly belonging to celebrities (crypto enthusiasts in most cases) promise users to double their cryptocurrency payments sent to the wallets, in reality controlled by the scammers. However, the platform keeps improving its mechanisms to better detect and block rogue schemes. It forces scammers to look for alternative ways to monetize their fraudulent operations.

As such, the scammers started using fake crypto-celebrity streams on YouTube. Similarly to the examples featuring fake Pavel Durov and Elon Musk accounts, YouTube stream viewers are encouraged to transfer cryptocurrency to scammers' wallets, with a promise of receiving double the amount in return. All the streams promote a link to a fake website designed to show visitors the mechanism behind a fake giveaway.

The scheme described in this research allowed crypto scammers to attract 165,000 viewers to their fake YouTube streams. The analysis of crypto wallets, controlled by the scammers, showed that they walked away with more than \$1,680,000, receiving 281 transactions within three days of monitoring. Below we describe how it all happened...

The wrong Vitalik

Between February 16 and 18, 2022, **Group-IB Digital Risk Protection** (DRP) experts detected 36 fraudulent YouTube streams promising profitable cryptocurrency investments. Those were the videos of famous crypto enthusiasts cut from legitimate streams and edited to create the fake ones. In one case, in order to attract viewers to a fake giveaway and make them believe that the stream was legitimate, fraudsters used a very well-known name in the crypto world: Vitalik Buterin, the creator of Ethereum.

ETHEREUM

Giveaway Rules Bonus Transactions

Official Ethereum Event 2022

We believe that Ethereum Coin will be worth 10,000\$ per coin. To speed up the process of cryptocurrency mass adoption, We decided to run 50,000 ETH giveaway.

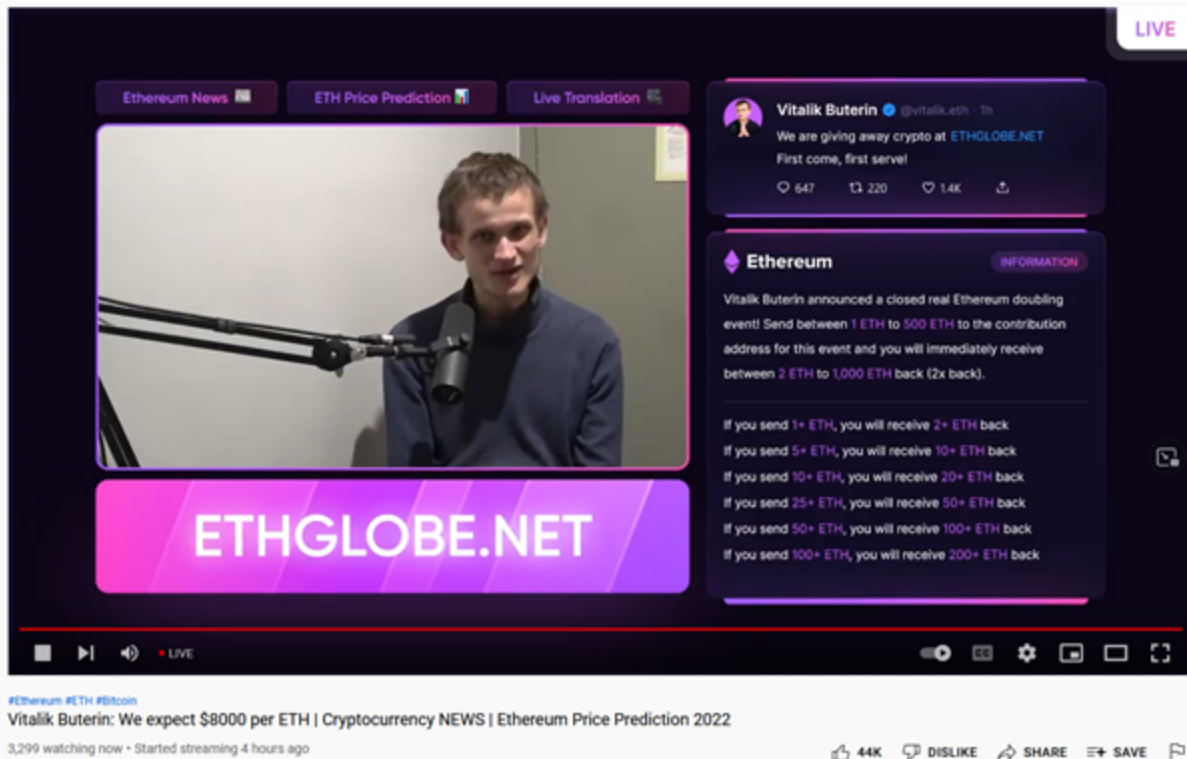
To participate you just need to send from 1 ETH to 500+ ETH to the contribution address and we will immediately send you back 2 ETH to 1,000 ETH (x2 back) to the address you sent it from.

MORE INFO

The tactic is not new, but apparently is still having a moment. Other famous names, that the scammers exploited as part of the latest wave, were **Elon Musk**, **Brad Garlinghouse**, **Michael J. Saylor**, **Changpeng Zhao**, and **Cathie Wood**.

During fake YouTube streams, crypto celebrities discuss current cryptocurrency trading volumes, show graphs indicating the growth of various metrics, and repeatedly refer to enormous profits. On average, such fake streams attracted between **3,000** and **18,000** viewers. The victims are encouraged to visit a website that contains all the information required to make a transaction and that explains why a transfer should be made immediately.

A stream featuring a fake footage of Vitalik Buterin attracted more than **165,000** viewers who were promised that their crypto savings would be doubled in real time if they transferred tokens to a crypto wallet, which in reality was controlled by the fraudsters. Some of them could be bots to make people believe that the stream was legitimate. But it is still quite a big number.



YouTube channels that run thematic streams usually have names associated with the key speaker of a specific stream. For example, if a stream features Vitalik Buterin, most likely the channel name would include Ethereum. In order to attract traffic, fraudsters use popular tags and keywords related to crypto enthusiasts and cryptocurrencies.

All these channels have supposedly been either hacked or purchased on the underground market. It is more than likely that they once belonged to individuals who used them on a regular basis. This can be derived from the date that the channel was registered, from the videos and playlists published on the channel that do not match the topic of the fraudulent stream, and from the large number of views. Some channels contain nothing but the fraudulent stream, however.

Most streams lasted more than three hours, but some were cut off abruptly. Sometimes the channel owner shut them down, while in other cases the channels were closed down for violating terms and conditions of use. Once a stream goes down, it usually becomes inaccessible.

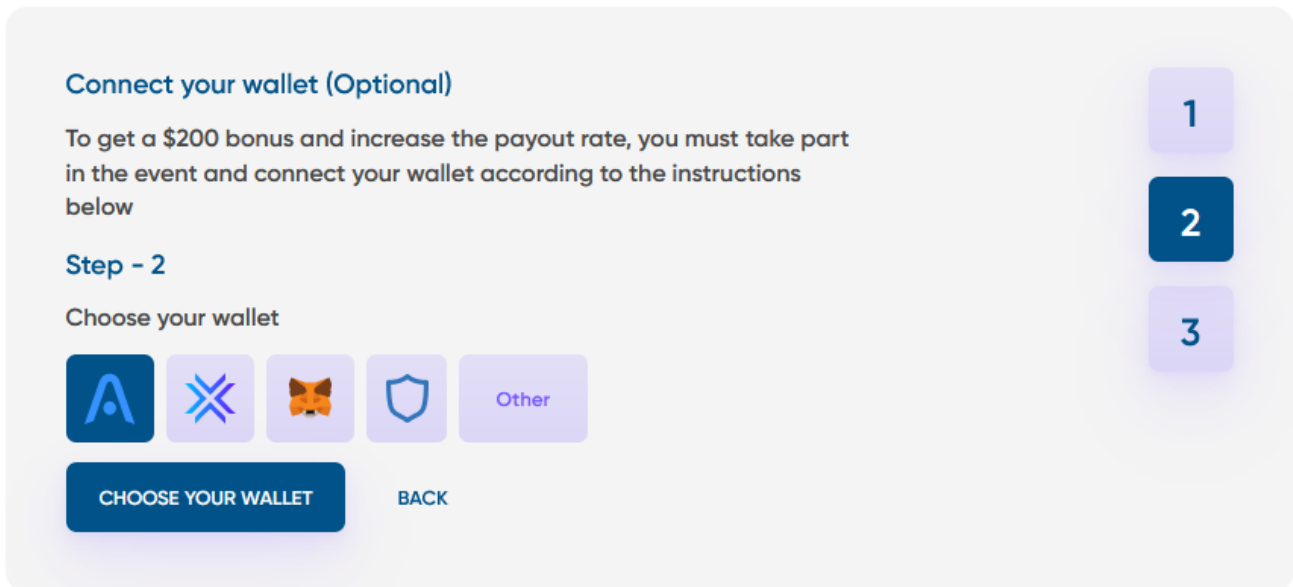
Hot and empty

In most cases, streams mainly discussed cryptocurrencies such as **Bitcoin**, **Ethereum**, and **Ripple**, while **Cardano**, **Dogecoin**, and **Shiba Inu** trailed behind with fewer mentions. QR codes with links to crypto wallets were sometimes displayed over the stream.

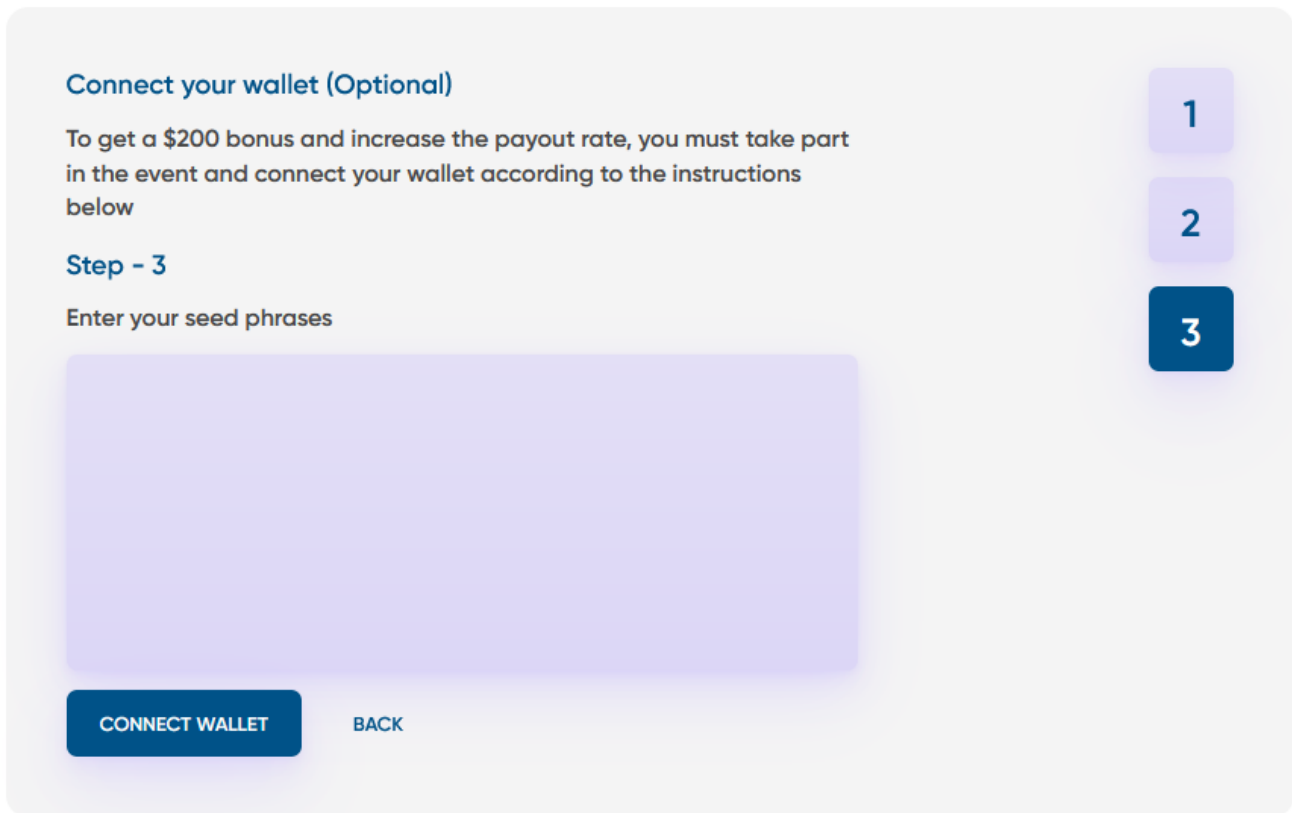
Research into the fraudulent scheme revealed that addresses of crypto wallets mentioned on fake websites were sometimes changed or updated. Several domain names often displayed

one and the same crypto wallet address. In total, Group-IB experts detected more than 30 crypto wallets used for the scheme, with a total remaining balance of **\$933,963**. The most popular cryptocurrency used by fraudsters as part of the scheme is **Ethereum**. Within three days of monitoring, (from February 16 to 18, 2022) all detected crypto wallets, controlled by the scammers, received 281 transactions in total, amounting to more than \$1,680,000.

When analyzing fraudulent websites promoted during the fake streams, Group-IB's Computer Emergency Response Team (CERT-GIB) detected an unusual technique. Depending on the cryptocurrency and type of crypto wallets, scammers asked visitors to their fake giveaway website to enter seed phrases to connect their wallets.



Scammers explained the request by a made-up promotion where participants who connected their wallets would receive an additional bonus and increased payout.



Once a victim shares their seed phrase, **fraudsters gain control over their wallet and withdraw all funds from it**. The exact number of victims and total amount of stolen funds remains unknown, but clearly some victims could not resist taking the bait.


Scammers' infrastructure

While analyzing the streams that promoted the latest wave of fake giveaways promoted, CERT-GIB experts initially retrieved the links to **29** websites with guidelines on how to double the investments. As a rule, 3 to 4 streams run simultaneously, and they all lead viewers to the same domain. The domain names contain keywords from streams and names of crypto projects.

Regardless of the cryptocurrency used, all such websites were designed based on the same pattern: scammer impersonate a well-known crypto enthusiast, project, or the entire crypto industry, announce the giveaway conditions, and publish the following: short FAQs, the address of a crypto wallet where participants are supposed to transfer their coins, and a section with fake examples of successful giveaway transactions. Their goal is to make visitors believe they can get rich.


For example

Send 1+ ETH, to receive 2+ ETH back.
 Send 10+ ETH, to receive 20+ ETH back.
 Send 50+ ETH, to receive 100+ ETH back.
 Send 250+ ETH, to receive 500+ ETH back.
 Send 500+ ETH, to receive 1,000+ ETH back.



Extra bonuses

25+ ETH = 5% Bonus
 100+ ETH = 10% Bonus
 250+ ETH = 20% Bonus
 500+ ETH = 30% Bonus
 1000+ ETH = 40% Bonus



About


During this unique event we will give you a chance to win 50,000 ETH, have a look at the rules and don't miss on your chance! You can only participate once!

[Rules](#) →


Rules

To participate you just need to send from 1 ETH to 500 ETH to the contribution address and we will immediately send you back 2 ETH to 1,000 ETH (x2) to the address you sent it from.


[About](#) →




To make a transaction, you can use any wallet or exchange to participate!



Once we receive your transaction, the outgoing transaction is processed to your address.



Once we receive your transaction, we will immediately send the requested amount back to you.

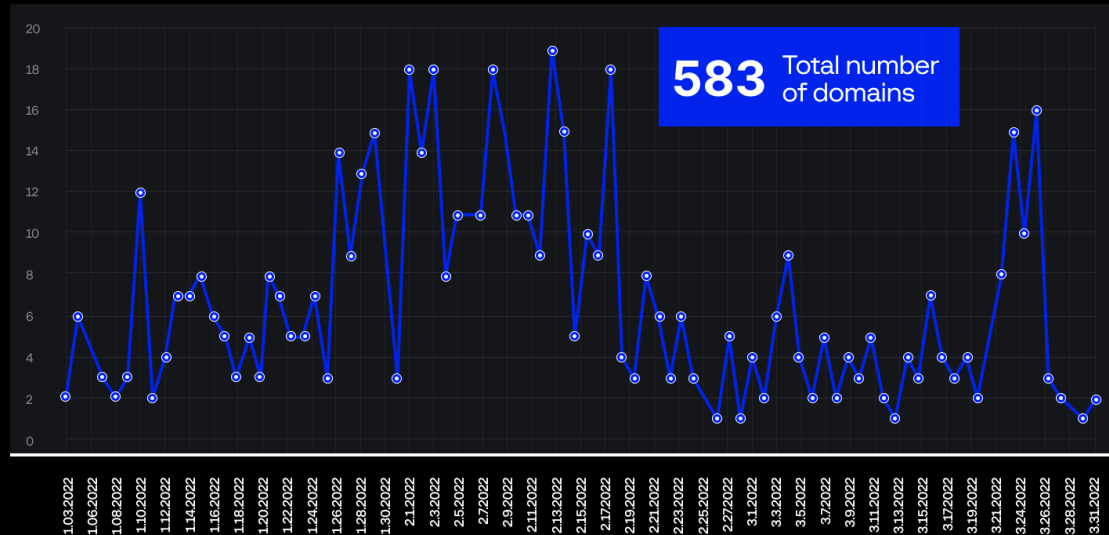


Every address that is sent too late, gets their ETH immediately sent back.

Most of the time, fraudsters use one-page template-based websites with an eye-catching design and high-quality crypto-themed images. The website design is the main factor that helps fraudsters deceive visitors and make them transfer cryptocurrency to the designated wallets.

A deeper analysis of the scammer's domain infrastructure revealed that those 29 websites were part of a massive network of **583** interconnected resources all set up in the first quarter of 2022. Notably, there were three times as many domains registered for this scheme in less than three months of 2022 compared to the whole of last year.

Fake Crypto Giveaway Domain Registration in Q1 2022



Group-IB, 2022

Below is a snapshot of interconnected network nodes used as part of a single cryptocurrency scam campaign. It shows that separate web resources are connected based on various network indicators.

Despite that giveaway schemes have existed for a long time and are based on straightforward deception techniques, they remain effective. The fact that they work could be rooted in an influx of inexperienced cryptocurrency users who have not encountered this kind of fraud yet, which are the kind of potential victims that fraudsters target the most.

And you can also buy NFTs...

Research into a fraud scheme involving cryptocurrency streams revealed another YouTube-related scheme targeting NFT (Non-Fungible Token) investors.



The NFT scheme is based on the same pattern. Scammers use original footage with crypto gurus, such as Gary Vaynerchuk aka Gary V, who discuss purchasing NTF images whose price could increase 10-fold over time. The stream description contains a link to a scam website where visitors are promised one NFT in exchange for sharing the data of their crypto wallet (password and key, required to restore access to the account).

Identify and mitigate digital risks to your brand

with Group-IB Digital Risk Protection

Request Demo

Recommendations

How to protect your cryptocurrency assets and not fall victim to crypto scammers.

Verify all information using official sources only

For example, go to the crypto project's official website. If you cannot find any information about the promotion taking place, you are likely being deceived regardless of the actions that you are being asked to take.

Do not share your seed phrase with third parties

Seed phrases must be kept secret and stored securely. To do so, use password management tools. To minimize the risk of leakage, prioritize desktop solutions over cloud-based ones. Remember: the person who owns the seed phrase owns the wallet.

Keep up with the latest news on relevant topics

Learn from other people's experiences. Often, someone else will have already encountered a similar situation. Be especially vigilant about free giveaways. Do not share confidential data on rogue websites. Become familiar with information security recommendations and follow them.