



| Flash |

Fake Tether Cryptocurrency Tokens Announced for Sale

F-2024-05-16a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Cryptocurrency, Scams

May 16, 2024

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 09:00 AM (EDT) on May 16, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Flash | Fake Tether Cryptocurrency Tokens Announced for Sale

Key Findings

- Since the beginning of May 2024, two advertisements for the sale of fake Tether ERC20 (also known as USDT) have been offered in deep and dark web (DDW) forums. Such announcements are historically uncommon, though there is a roughly even chance that demand for these services is increasing.
- Threat actors seeking to acquire fake Tether ERC20 coins most likely intend to leverage them in malicious, fraudulent activity such as exchange or investment scams. These are often conducted via the establishment of a webpage imitating a legitimate cryptocurrency or investment platform.
- If threat actors are continually successful in leveraging fake cryptocurrencies for malicious purposes, it is likely that additional purchasing options will become available in DDW forums. This would very likely lead to an increased threat to both individuals and organizations that are either involved in cryptocurrency trading or accept it as tender.

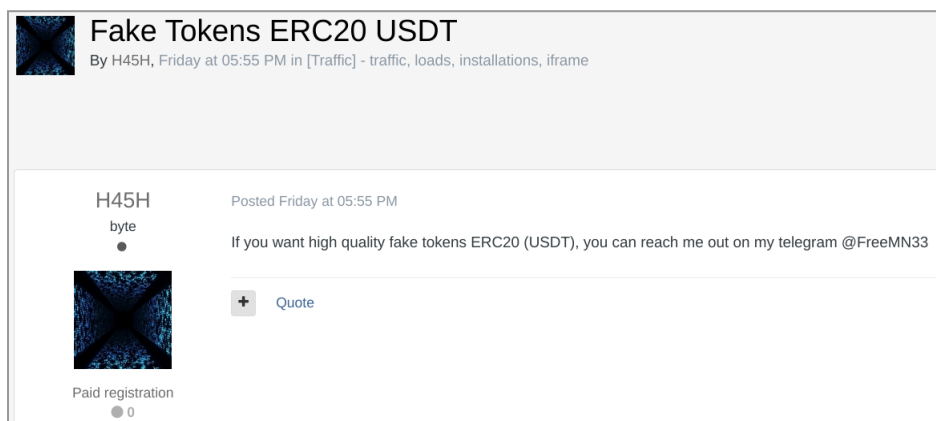
Details

Since the beginning of May 2024, two advertisements for the sale of fake Tether ERC20 have been offered in DDW forums. Such announcements are historically uncommon, though there is a roughly even chance that demand for these services is increasing.

- Tether is a type of Stablecoin—a cryptocurrency with value that is tied to another asset. Tether is tied to the U.S. dollar, which enables a stable value in comparison to other, more volatile cryptocurrencies.

Threat actors seeking to acquire fake Tether ERC20 coins most likely intend to leverage them in malicious, fraudulent activity such as exchange or investment scams, which are often conducted via the establishment of a webpage imitating a legitimate cryptocurrency or investment platform. These will often offer unrealistic exchange rates or returns. The threat actor will then restrict victim withdrawals and steal the invested funds.

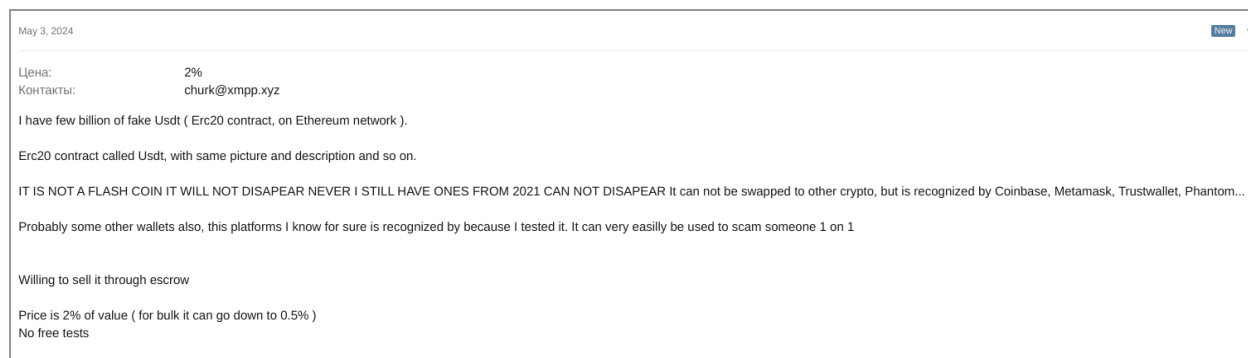
On May 10, 2024, untested actor “H45H” advertised the sale of fake Tether ERC20 tokens on the predominantly-Russian language DDW forum Exploit. The actor gave no further detail and advised interested parties to contact them via their Telegram account.



Exploit post by H45H advertising the sale of fake Tether ERC20

Source: ZeroFox Intelligence

Previously on May 3, 2024, vetted English-speaking threat actor “Churk” announced the sale of fake Tether ERC20 on the Russian-speaking forum xss. Churk claimed to have “a few billion fake USDT” for sale, at a cost of 0.5–2 percent of the Tether value. Churk alleged that the fake cryptocurrency shares common identifiers with its legitimate counterpart, such as pictures and other attributes. This sale is very likely credible, given Churk’s positive reputation within the forum and explicit agreement to use the forum’s escrow service.



Xss post by Churk advertising the sale of fake Tether ERC20

Source: ZeroFox Intelligence

Churk advised that the fake USDT are not a “flash coin”, claiming to still be in possession of fake coins from 2021 that are recognized by the cryptocurrency platforms Coinbase, Metamast, Trustwallet, and Phantom. Churk conceded, however, that the fake USDT cannot be exchanged for other crypto, though they can be used “easily” in unmediated 1:1 exchange scams.

- Flash coin is a term used to describe fake cryptocurrency that disappears before its use, often shortly after arriving in a crypto wallet. They can be in a variety of formats, such as Bitcoin (BTC), Ethereum (ETH), or Ripple (XRP).

On May 13, 2024, positive reputation actor “maximlofl” commented on the thread, warning potential buyers of multiple issues they had experienced after purchasing 2,500 fake tether tokens at a cost of USD 50. Maximlofl alleged that:

- The fake coin does not automatically appear in a crypto wallet, requiring it to be added manually. Maximlofl provided an image which suggests that the fake currency was not recognized.
- The USDT logo does not show on the tokens, resulting in the token appearing inauthentic.



maxim1of1
RAID-массив
Пользователь

Joined: Jul 20, 2022
Messages: 52
Reaction score: 4

Today at 8:41 AM

I paid for 2,500 usdt tokens which cost \$50. (He gave me extra 1,000 tokens 😊)

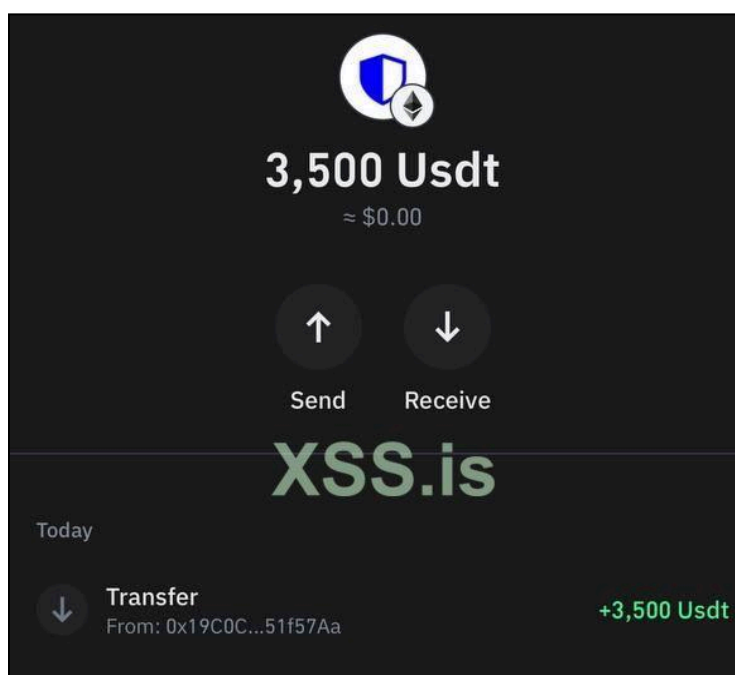
Well, he sent the tokens but there are some issues I want to let everyone know before you purchase

1. The token does not automatically show up in your wallet, you have to add it manually from the contract address
2. No USDT logo showing on the token so it looks fake
3. The value of the token in dollars in the wallet shows \$0.00 as you can see from the screenshot below, but the 3,500 USDT arrived

Just to let everyone know before you make a purchase

Xss post by maxim1of1 warning potential buyers of Churk's services

Source: ZeroFox Intelligence



Xss post by maxim1of1 displaying a crypto wallet balance of USD 0.00

Source: ZeroFox Intelligence

Further discussion followed between several actors as to whether different cryptocurrency platforms would be more suitable for the fake Tether. Churk advised that compatibility issues would be addressed. Another actor, "sed", pointed out that the most important feature of the fake Tether is that it does not disappear.

- Fake exchange and investment scams are conducted via the threat actor setting up a website imitating a legitimate cryptocurrency site, almost certainly

promising unrealistic high returns and rates. These fake exchanges allow victims to deposit funds but then restrict withdrawals, or the threat actors will simply disappear with the invested money.

These two announcements indicate a roughly even chance of an increased interest in fake cryptocurrencies within DDW forums. Cryptocurrencies such as Tether are likely to be continually implicated in this activity, due in part to threat actors' ability to emulate it, its general popularity amongst competitors, and the high degree of anonymity that can be exploited.

If threat actors are continually successful in leveraging fake cryptocurrencies for malicious purposes, it is likely that additional purchasing options will become available in DDW forums. This would very likely lead to an increased threat to both individuals and organizations that are either involved in cryptocurrency trading or accept it as tender.

Recommendations

- Be vigilant of unsolicited communications that offer lucrative cryptocurrency investments or banking opportunities or unusually high returns.
- Always use reputable, well-established cryptocurrency platforms, exchanges, and wallet services. Avoid those that are unfamiliar, especially if they appear to contain design errors that arouse suspicion.
- When visiting cryptocurrency platforms, be sure that the webpage is legitimate before entering sensitive information. Some phishing scams target these web pages specifically, using brand impersonation and web page cloning to target users.
- Be aware of cryptocurrency scams that leverage social engineering hooks, such as the endorsement of a given platform by a celebrity or the promise of a “giveaway” in exchange for a small upfront cost.
- Never share private keys, passwords, or seed phrases with anybody. Legitimate cryptocurrency platforms will never ask a user to divulge sensitive information.
- Use secure hardware wallets for cryptocurrency storage, and avoid leaving funds on exchanges or in online wallets.
- Enable multi-factor authentication (MFA) on all accounts used to access cryptocurrency platforms.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%