

What are “drainer smart contracts” and why is the FBI warning of them?



Getty Images

reader comments

125 with

The FBI is advising potential NFT buyers to be on the lookout for malicious websites that use “drainer smart contracts” to surreptitiously loot cryptocurrency wallets.

The websites present themselves as outlets for legitimate NFT projects that provide new offerings. They’re promoted by

compromised social media accounts belonging to known NFT developers or accounts made to look like such accounts. Posts frequently try to create a sense of urgency by using phrases such as “limited supply” or by referring to the promotion as a “surprise” or the result of a previously unannounced token minting.

“The spoofed websites invite victims to connect their cryptocurrency wallets and purchase the NFT,” FBI officials wrote in a Friday advisory. “The victims unknowingly connect their cryptocurrency wallets to a drainer smart contract, resulting in the transfer of cryptocurrency and NFTs to wallets operated by criminals.”

From there, the scammers often launder the stolen assets through a series of cryptocurrency exchanges or other services that mix them with assets of others, in an attempt to obfuscate the path and final destination of the stolen NFTs. Smart contracts are a type of computer coding that executes an agreement or transaction, usually involving the transfer of digital assets. Crooks often use smart contracts that contain bugs or loopholes that transfer millions of dollars in assets from one or more parties entering into the agreement.

NFT is short for non-fungible token. It most frequently refers to visual art in digital form such as images, but can at least theoretically encompass anything in digital form including music, video game items, or domain names. While the image or other media can be copied, a non-fungible—meaning unique or irreplaceable—token embedded in the media can’t be duplicated. The token is supposed to serve as proof that the holder is the rightful owner of the art. Some NFTs have sold for millions of dollars.

Advertisement

Scammers are exploiting this market to steal cryptocurrency from people. In the schemes the FBI warns of, the scammers often pose as NFT developers who are promoting new releases.

Friday's advisory recommends NFT consumers take the following precautions:

- If a well-known NFT project announces a surprise NFT opportunity, research if the developer has revealed surprise opportunities in the past or if they have made statements that they will never offer surprise mints. Many criminal actors prey on the sense of urgency victims feel whenever a surprise opportunity is announced.
- Check to ensure the social media account advertising the opportunity is the legitimate account of the development team, and not a cloned account made to look like the real thing. Any discrepancies in spelling, account history, screen name, followers, or creation date indicate the account proclaiming the opportunity is fake.
- When accessing websites that request you connect your cryptocurrency wallet, look to see if the website is real and not a clone of the legitimate website. Indicators of this would be a misspelled web domain name, a URL with additional or unnecessary characters, or links on the webpage that either do not work or reroutes users back to the main page.
- Vet any opportunity that offers NFTs as a reward especially if it feels too good to be true.

The advisory went on to invite victims of such scams or people suspecting fraud to report them to the FBI's Internet Crime Complaint Center. FBI officials advise that people include any links, social media or cryptocurrency accounts, or domains used in the scam and use the keyword "NFTHack."

<https://arstechnica.com/?p=1959148>