



NFT Drainer Claims to Bypass Cryptocurrency Wallet Update

ZEROFOX INTELLIGENCE

F-2022-09-21a

Classification: TLP:CLEAR

Criticality: Extremely High

Intelligence Requirements: Dark web, PII & Fraud

September 21, 2022



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 11:00 AM (EDT) on September 21, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

NFT Drainer Claims to Bypass Cryptocurrency Wallet Update

Key Findings

- A credible dark web actor is advertising an updated non-fungible token (NFT) drainer aimed at the latest version of MetaMask, indicating a burgeoning market for more sophisticated attack vectors aimed at the NFT user base.
- Threat actors' shift to more sophisticated exploits tracks with the increase in general awareness and popularity of NFTs, which provide a lucrative target base.

Analyst Commentary

A credible dark web actor is advertising an updated NFT¹ drainer aimed at the latest version of MetaMask, indicating a burgeoning market for more sophisticated attack vectors aimed at the NFT user base. In early September 2022, well-regarded threat actor “jezabeth” announced a new NFT drainer capable of draining ERC-20, ERC-1155, ERC-721, and Ethereum (ETH) tokens on popular Russian language dark web forum exploit[.]in; the actor is selling this drainer for 8 ETH, which is valued at about USD 10,790.

- According to the actor, the victim's NFTs are accessed by employing Seaport contract signatures, which drain tokens without the user being prompted to pay transaction fees; the actor emphasizes that this tool bypasses the latest MetaMask update.

¹ An NFT is a non-interchangeable unit of data that is stored on a blockchain and can validate the ownership and uniqueness of digital assets.



jezabeth

byte



Paid registration

 1

18 posts

Joined

02/16/21 (ID: 114178)

Activity

кодинг / coder

Posted September 9

Newest NFT drainer + warning bypass (Seaport / OpenSea API)

This will be the best drainer you could find now.

Drains Tokens: ERC-20 / ERC-1155 / ERC-721 / ETH

NFT's will be drained by using Seaport contract signature. User does not pay for transaction fee. No warnings will be given from MetaMask, it bypasses latest update.

Drainer will first drain the most expensive tokens, then the least expensive tokens. Landingpage is easy to customize

Bypass the last SetApprovalForAll warning of MetaMask.

Can provide video on Telegram, message me for my Telegram.

Price: 8 ETH

Escrow / Middleman accepted, costs for buyer

Source: ZeroFox Intelligence

Crypto and NFT-related scams have risen in line with increased adoption over the last 18 months, as threat actors continue to develop new techniques to exploit the lack of regulation within the space. NFT drainers are one example of such techniques and are widely leveraged by scammers due to their relative ease of acquisition; multiple versions of NFT drainer source code remain readily available on open source repositories such as GitHub, as well as within private messaging channels in Telegram.

NFT drainers are typically designed to replicate existing NFT projects and their respective websites, leveraging malicious smart contracts to steal the contents of a victim's crypto wallet. Threat actors will often deploy drainers by:

- Creating scam projects of their own to build hype and collect prospective investors, culminating in a fake minting² website.
- Hacking Discord channels and Twitter profiles of existing projects to insert malicious "surprise mints" or other enticing links to dupe communities.
- Inserting phishing links on the social media profiles of legitimate projects and notable influencers.

All methods ultimately require user interaction with a malicious smart contract. Often, scammers will also employ the use of social media bots to artificially grow a false account to appear legitimate, as well as to spread phishing messages.

² Minting is the term used to describe the process of creating a new token on the blockchain.



NFT projects and their followers are particularly vulnerable to scams due to the speculative nature of the NFT market and many users seeking potentially-lucrative gains. Hyped projects have often sold out within hours—or in some cases minutes—enabling scammers to capitalize on investors reacting quickly to project launches and follow-up offerings.

To protect users from wallet-draining scams, some cryptocurrency wallets have started to introduce a layer of security asking for access permission instead of automatically granting it in an effort to allow users time to reconsider their options. However, threat actors like “jezabeth” are innovating to counter the defenses of wallets like MetaMask.

Recommendations

Users should always keep up to date with the most current security protocols, including:

- Always check wallet transactions and approvals when interacting with contracts.
- Do not click suspicious or unexpected links sent as direct messages or on social media channels.
- Never share private keys or seed phrases. Ensure these are stored offline and not on devices or cloud storage.
- Use a cold storage hardware wallet to store assets; never keep assets in hot wallets that are used to interact with contracts.
- Avoid purchasing hardware wallets from third-party resellers or pre-owned wallets, as these may have already been compromised.
- Ensure due diligence is carried out on any project before investing; check the profile and background of a project and its founders.



Appendix: 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.