Recorded Future®

By Insikt Group®

New “Crypto Drainer” Phishing Pages Siphon Cryptocurrency in Seconds

CTA-2023-0202

Executive Summary

A Nigerian prince needs your help. Or a coworker texts you, urgently demanding that you send gift cards. Words like “fraud” and “phishing” often evoke simple scams that only fool the foolish. In reality, threat actors develop refined tactics, techniques, and procedures (TTPs) to target users who believe themselves too clever to be fooled.

“Crypto drainers” are malicious scripts that function like e-skimmers and are deployed with phishing techniques to steal victims’ crypto assets. The phishing pages that are deployed with crypto drainers often imitate popular crypto services and use common third-party applications and extensions (such as MetaMask) that are not unusual for the legitimate services that these phishing pages imitate.

We discovered a ready-to-go crypto drainer phishing page advertised by a threat actor on a top-tier dark web forum. This phishing page purports to mint non-fungible tokens (NFTs) and uses third-party services that are commonly used in the crypto sphere. After analyzing this crypto drainer, we concluded that it can be effectively used to steal crypto assets from compromised crypto wallets. Once crypto wallets are compromised, no safeguards exist to prevent the theft of crypto assets. Since their first appearance in 2022, crypto drainer phishing pages have surged in popularity, and crypto drainer phishing pages will likely remain relevant, effective, and widely used in 2023.

Key Judgments

- Crypto drainers are used on phishing pages that imitate popular crypto services to steal crypto assets from unsuspecting victims. They exploit legitimate extensions and applications that are frequently used with the crypto services that the phishing pages imitate.
- We analyzed a ready-to-go crypto drainer phishing page advertised by a threat actor on a top-tier dark web forum. This phishing page entices victims into connecting their wallets with an offer to mint NFTs. As soon as victims attempt to mint NFTs, the crypto drainer siphons available cryptocurrency and desired NFTs to the attacker’s wallet.
- Crypto drainer projects are surging in popularity, and a growing number of ready-to-go crypto drainer phishing packages could allow threat actors to execute them quickly and at scale.

Background

Though blockchain technology is designed from the ground up with security in mind, openings nevertheless exist for threat actors to defraud victims of their crypto assets. “Crypto drainers” are malicious files that function similarly to e-skimmers by automatically executing transfers of crypto assets.

Crypto drainers are commonly deployed on phishing pages that imitate popular crypto services. Examples of the crypto services that a crypto drainer phishing page might imitate include cryptocurrency exchanges or non-fungible token (NFT) platforms. Importantly, crypto drainer phishing

pages often use third-party services or extensions (such as MetaMask) that are commonly used with the crypto services they imitate. The use of legitimate services on crypto drainer phishing pages may increase the likelihood that the phishing page will pass an otherwise savvy user's "scam litmus test".

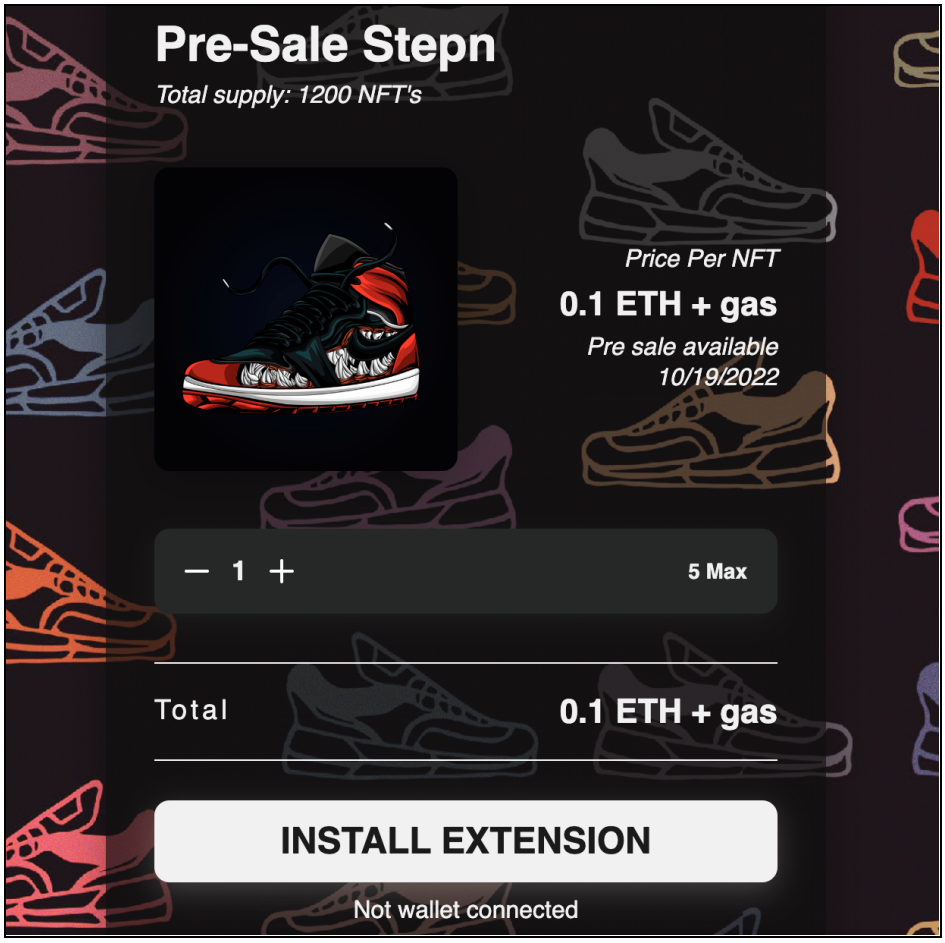


Figure 1: *Recorded Future analyzed a crypto drainer phishing page that entices victims to connect their wallets with the promise of minting NFTs (Source: Recorded Future)*

Threat Analysis

Designing crypto drainers requires coding skills that phishing specialists may lack. As a result, many cybercriminals develop crypto drainers to sell or rent out as components in ready-to-go phishing packages; this is likely part of a greater trend toward phishing-as-a-service (PhaaS). Threat actors who purchase these packages can swiftly enact crypto drainer phishing operations at scale.

Step-by-Step Tutorial

On September 14, 2022, a threat actor on a top-tier dark web forum posted an archive file that included a template for a phishing page and a crypto drainer. This particular crypto drainer is designed to siphon Ether (ETH, Ethereum's native cryptocurrency) and Ethereum-based NFTs from victims' wallets.

Ethereum is a widely used blockchain, so attacks that target Ethereum-based crypto assets may present a wider threat to crypto holders than attacks that target assets on other blockchains.

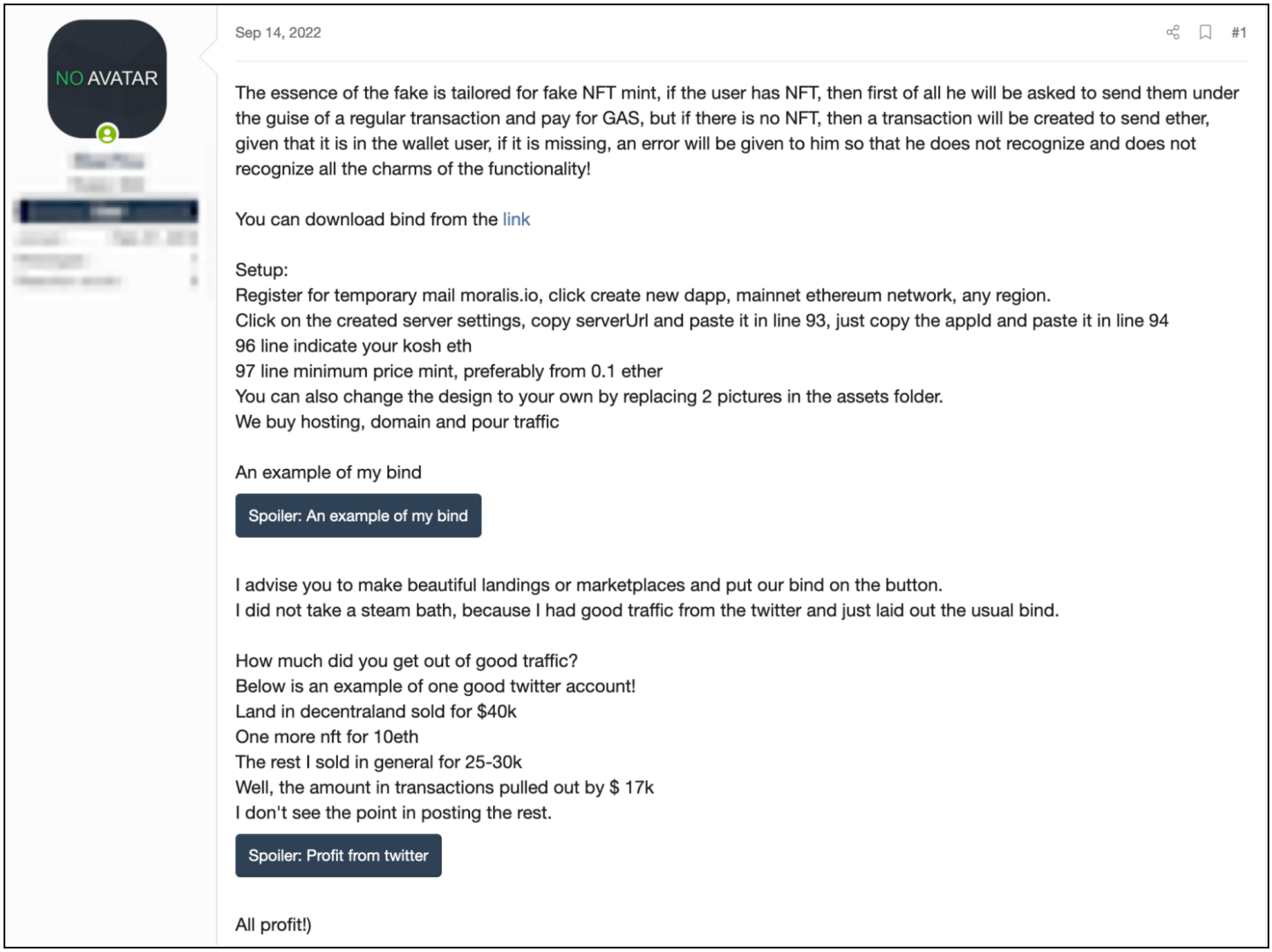


***Figure 2**: In a forum post, a threat actor made their crypto drainer available for download — image text machine-translated from Russian via Google Translate (Source: Top-tier dark web forum)*

The threat actor's crypto drainer must be deployed alongside the legitimate services Moralis and MetaMask to conduct a phishing scam. Moralis provides the framework that the crypto drainer builds upon in order to siphon crypto assets from victims' crypto wallets, and MetaMask allows victims to interact with the crypto drainer.

The scam's order of operations is generally simple:

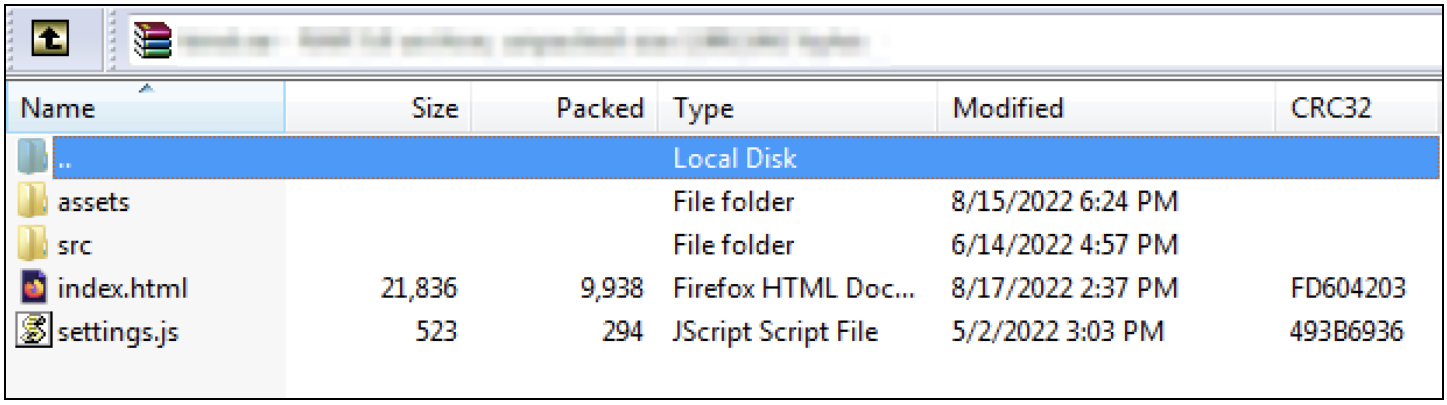
- First, the cybercriminal configures and deploys their phishing page, which entices their victim into connecting their crypto wallet.

- Then, malicious JavaScript code in the crypto drainer exploits the new connection to create and approve a transaction on behalf of the victim.
- Finally, the crypto drainer checks the victim's crypto wallet for desired NFTs before stored crypto assets are swiftly transferred to the attacker's wallet.

In the same post, the threat actor boasted of using their crypto drainer to accumulate around $95,000 in stolen cryptocurrency and NFTs.

Functionality and First Steps

In their original forum post, the threat actor provided an archive file that contained files necessary to configure their crypto drainer phishing page.

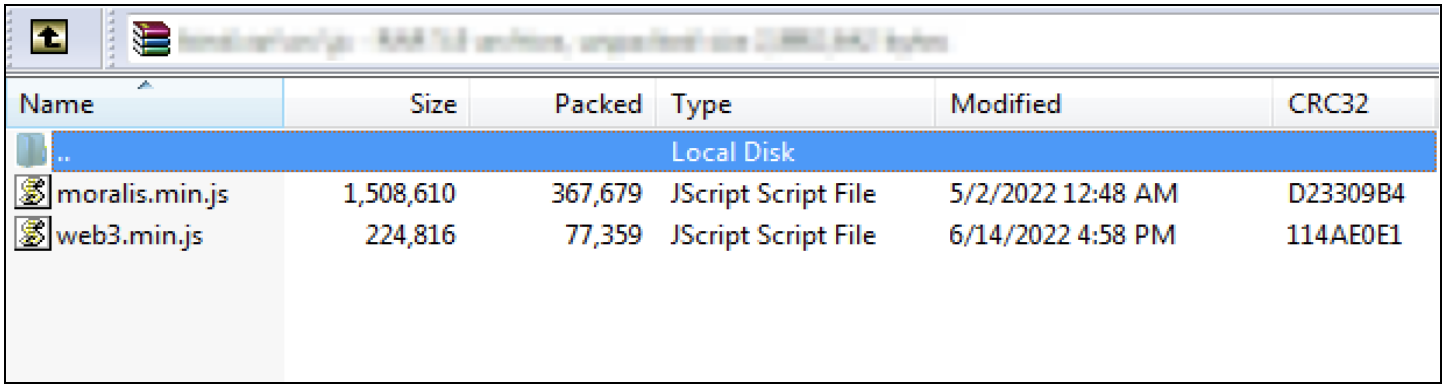


Name	Size	Packed	Type	Modified	CRC32
..			Local Disk		
assets			File folder	8/15/2022 6:24 PM	
src			File folder	6/14/2022 4:57 PM	
index.html	21,836	9,938	Firefox HTML Doc...	8/17/2022 2:37 PM	FD604203
settings.js	523	294	JScript Script File	5/2/2022 3:03 PM	493B6936

Figure 3: *The threat actor's archive file contains the code necessary to deploy the crypto drainer (Source: Recorded Future)*

The core of the crypto drainer script is located in one of the archive file's subdirectories. The malicious JavaScript file "web3.min.js" executes the crypto drainer's functions. This file's code is obfuscated, and its encrypted values are stored in arrays and accessed via calls to multiple decryption functions.

Another file located within the archive file, "moralis.min.js", is the application programming interface (API) client of Moralis. Moralis offers APIs that integrate blockchain technology into websites. "moralis.min.js" integrates Moralis's back-end code into the crypto drainer's phishing page, essentially allowing the crypto drainer to function with Moralis.



Name	Size	Packed	Type	Modified	CRC32
..			Local Disk		
moralis.min.js	1,508,610	367,679	JScript Script File	5/2/2022 12:48 AM	D23309B4
web3.min.js	224,816	77,359	JScript Script File	6/14/2022 4:58 PM	114AE0E1

Figure 4: *The core of the crypto drainer script is located in one of the archive file's subdirectories (Source: Recorded Future)*

Before deploying this phishing page, a threat actor must register an account with Moralis. This can be done using a temporary email address. After registration, the actor must create a new decentralized application (dApp) through Moralis using a configuration specified in the original forum post.

Arming the Phishing Page

Within the archive file, the threat actor must interact with 2 more files. One contains the phishing page to be used (Figure 1). In the second file, this phishing page's default design can be altered by specifying certain images and social media links to be used, depending on what kind of crypto service the threat actor wishes to imitate.

Next, the threat actor must configure their phishing page to connect with Moralis. The threat actor must also specify how their attack will be conducted by inputting:

- An address for the Ethereum wallet where the actor wishes to receive stolen crypto assets
- A list of desired NFTs the crypto drainer will scan for before exfiltrating them to the attacker's Ethereum wallet

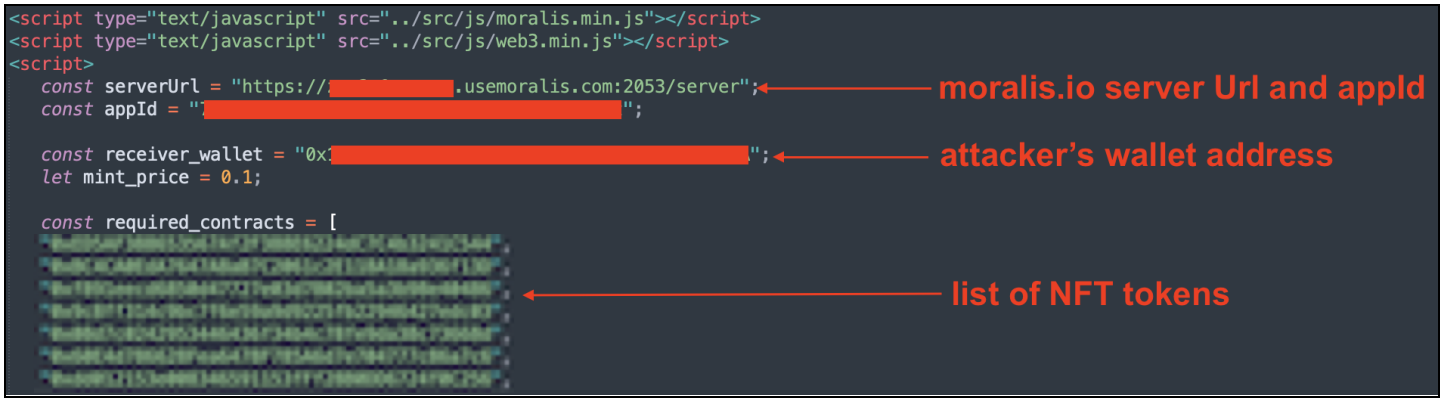


Figure 5: *Threat actors must connect their phishing page to Moralis and specify how their attack will be conducted (Source: Recorded Future)*

Deploying the Phishing Page

A variety of lures exist for crypto drainer phishing pages. This particular crypto drainer phishing page entices victims to connect their crypto wallets with the promise of minting NFTs. "Minting" secures digital assets on the blockchain, thereby creating NFTs, and typically requires that users pay cryptocurrency transaction fees called "gas fees".

Once the victim is browsing the crypto drainer phishing page, regular pop-up messages claim other wallets are currently minting NFTs. This psychological pressure induces the victim to connect their wallet to mint NFTs.

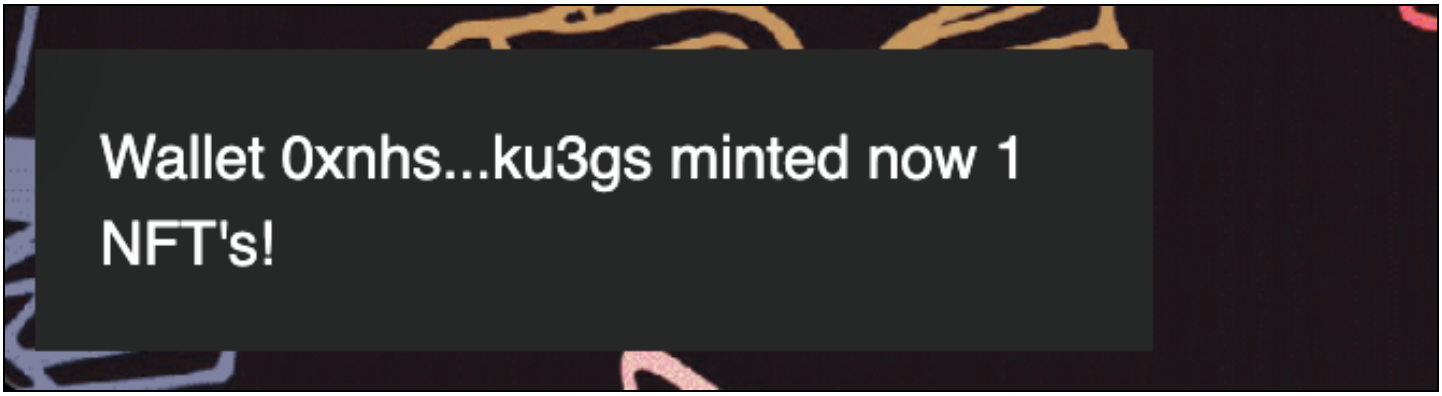


Figure 6: *The crypto drainer phishing page creates a sense of urgency by falsely claiming that other wallets are minting NFTs (Source: Recorded Future)*

Meanwhile, the crypto drainer's script checks whether or not the MetaMask extension is installed on the victim's web browser. MetaMask is used to access Ethereum-enabled dApps by injecting the Ethereum Web3 API into every website's JavaScript context. Put simply, MetaMask functions as a user's crypto wallet, thereby allowing victims to transact with crypto assets via their browser. If the MetaMask extension is not installed, the phishing page prompts the victim to install it.

Once MetaMask has been installed, the phishing page prompts the victim to connect their Ethereum wallet to begin minting NFTs. If the victim agrees, the crypto drainer's script exploits the Moralis API to intercept the victim's wallet address. This, in turn, will allow the crypto drainer to create and sign a new transaction on behalf of their victim.

At this stage, the crypto drainer performs blockchain verification to validate the imminent fraudulent transaction, then checks the NFTs in the victim's crypto wallet against the list of desired NFTs specified earlier by the threat actor. On the phishing page, the option "Mint Now" prompts the victim to pay a gas fee in order to mint their NFT. Once the victim presses the "Mint Now" button, the crypto drainer attempts to steal cryptocurrency from the victim's crypto wallet.

```
async function getTransfer() {
    if (!eth_network) {
        return
    }
    alertify.warning('Creating a transaction...')
    var lightton = await getContracts()
    if (lighton == null) {
        console.log(
            '[Moralis] Client ' + client_address + " don't have NFT's. Transfer ETH..."
        )
        stop = await transferEth()
        if (stop) {
            return
        }
    } else {
        console.log(
            '[Moralis] Client ' + client_address + " have NFT's. Transfer..."
        )
        await transferNft(lightton)
        return
    }
    await getTransfer()
    return
}
```

Figure 7: *"getTransfer()" executes the crypto drainer's core function: stealing crypto assets from victims' wallets (Source: Recorded Future)*

At this point, the crypto drainer exfiltrates all available ETH cryptocurrency and transfers any NFTs specified by the attacker from the victim's wallet to the attacker's wallet. If there are no NFTs or ETH in the victim's wallet, an error message is displayed. This error message is likely meant to remove any suspicion the user may have, reducing the likelihood that they will disconnect their wallet from the phishing page.

However, if the malicious script is completely unable to connect to Moralis's API server, the phishing page is replaced with an image of a dog and the text: "Sebek was here". This peculiar message is likely a vestigial feature from the script's development and may have served as a signal to the script's developer that their crypto drainer required debugging.

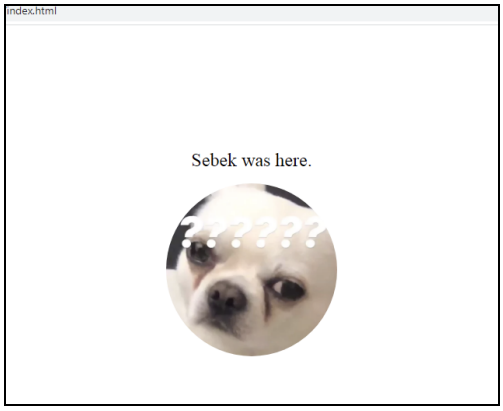


Figure 8: *If the crypto drainer is unable to connect to Moralis, it replaces the phishing page with a peculiar image and text that may have once been used for debugging (Source: Recorded Future)*

"Taking a Cut"

Remarkably, the threat actor who posted this crypto drainer phishing template did not charge other threat actors who wished to make use of their tool. Unremarkably, this was no act of charity — the crypto drainer was likely designed to defraud other cybercriminals of a portion of their illicit earnings.

On October 6, 2022, another threat actor on the same thread warned that this crypto drainer template establishes a WebSocket connection to the URL "hxxps://api[.]rarecity[.]art:2053". This WebSocket connection is used to surreptitiously transmit several values, including the field "change". Before operation, the crypto drainer checks the field "change". If it is set to 1, the crypto drainer script uses a different Moralis app ID, server URL, and API key to transfer crypto assets from the phishing victim's wallet to a third crypto wallet rather than to the wallet of the attacker who deployed the crypto drainer.

This feature was not described in the original advertisement.

Figure 9: *Another threat actor warned their peers of a secret WebSocket connection established by the advertised crypto drainer script — image text machine-translated from Russian via Google Translate (Source: top-tier dark web forum)*

Analysts Confirm Crypto Drainer Template Sees Use among Threat Actors

We were able to confirm that this crypto drainer phishing page template can be used to effectively steal crypto assets from unsuspecting victims after identifying an Ethereum wallet that likely belongs to the threat actor. The Ethereum wallet address[1] is transmitted over the WebSocket connection revealed in the warning provided to other threat actors on the original post. Given that the threat actor who advertised this phishing template likely designed it, it is probable that this wallet address belongs to them.

Over the course of 10 days, the identified Ethereum wallet received 0.8 ETH, worth approximately $1,073 USD as of January 11, 2023. It is highly likely this ETH was obtained via the "back door" described in the warning on the original advertisement, which suggests that other threat actors were able to use the crypto drainer phishing page template to effectively siphon NFTs and cryptocurrency from victims' compromised wallets.

[1] 0×2ed40808C75379AD6114807cbb044cB619c0D214

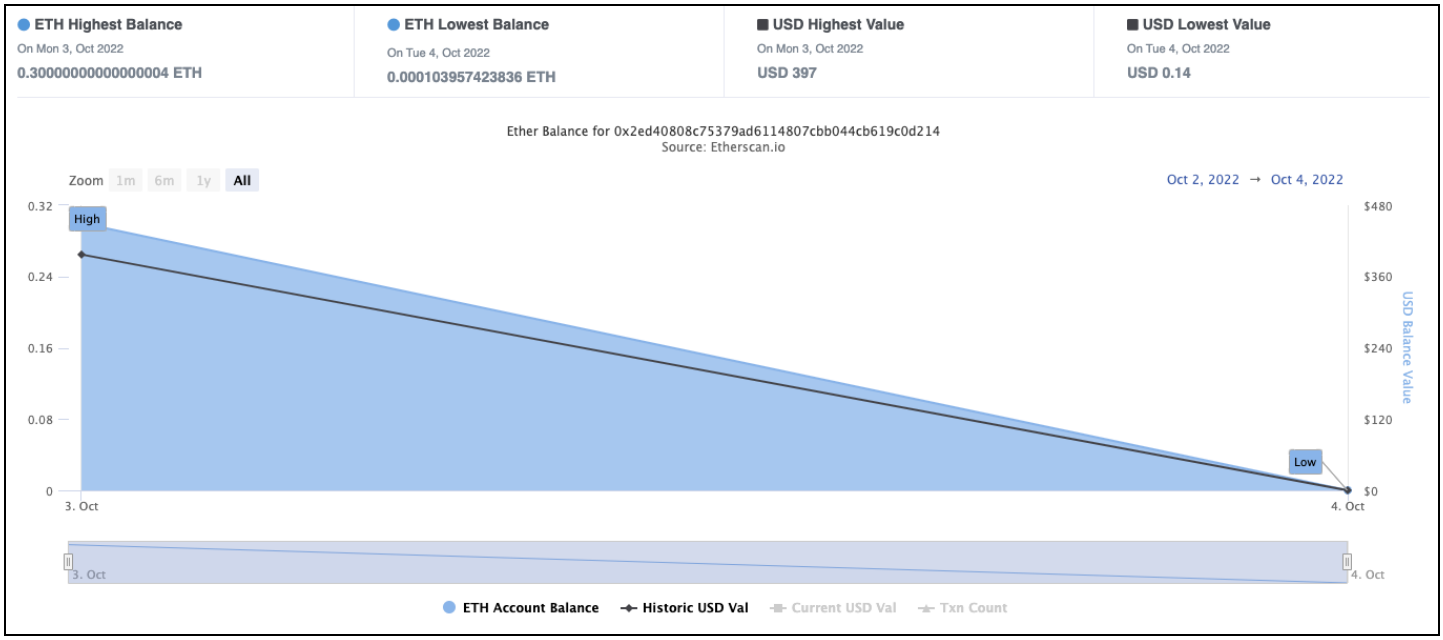


Figure 10: *The transaction history of the identified wallet suggests that the crypto drainer scam is effective (Source: Etherscan)*

During the course of our research, we also identified 9 phishing pages that had deployed this crypto drainer template and Ethereum wallet addresses belonging to the attackers who configured them. As described earlier in this report, these websites masqueraded as legitimate crypto services to siphon crypto assets from victims' wallets. All enumerated Ethereum wallets demonstrated spurts of activity over a short period of time, which is consistent with criminal TTPs. Additionally, on the block explorer Etherscan, blockchain security analysts flagged 3 of the Ethereum wallet addresses as being associated with phishing scams.

Phishing Page Domains	Ethereum Wallets
hxxp://walkn[.]tech/	0xeb80F56B6D3ad95Fac474dd228A4f83e169f102E
hxxps://coffeejunkiemint[.]com/	0×8fa11AF869eB8F5E6c69836DCe19c7d540FF7c77
hxxp://projectseed[.]tech/	0×8fa11AF869eB8F5E6c69836DCe19c7d540FF7c77
hxxps://tudnft[.]space/	0×2D550E85aa24BcD73C758ef949734dc30b33658b
hxxps://step[.]arthub[.]cc/	0×1604e141a254537BAC7b996accC3dCD173249aeA
hxxps://thebubbleworlds[.]com/	0×8fa11AF869eB8F5E6c69836DCe19c7d540FF7c77
hxxps://trolltownnft[.]com/	0×72C777C170497dB3741AD61f4aDD24eE7393D540
hxxps://nftmint[.]space/	0×2D550E85aa24BcD73C758ef949734dc30b33658b
hxxps://nfttud[.]com/	0×2D550E85aa24BcD73C758ef949734dc30b33658b

Table 1: *We identified 9 phishing pages and Ethereum wallets associated with this crypto drainer template*

In addition to these phishing domains and attacker wallets, we identified 92 crypto drainer phishing page domains and attacker wallets that were unrelated to this phishing template.

Sources Indicate Surging Interest

Threat actors have rapidly identified crypto drainers and phishing techniques as a powerful combination of TTPs to steal crypto assets. Since their first appearance in 2022, we have recorded 1,066 mentions of “crypto drainer” or “NFT drainer” on the dark web.

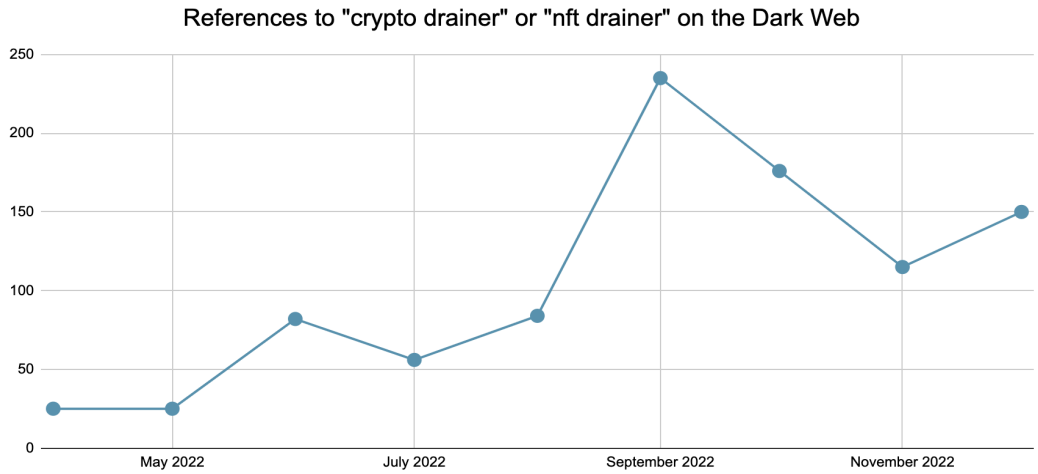


***Figure 11**: From April to December 2022, interest in crypto drainers demonstrated significant growth (Source: Recorded Future)*

Following their first appearance last year, crypto drainers exploded in popularity. A Telegram channel focused on crypto drainers was created in March 2022. Since then, more than 15,000 users have subscribed to the channel, with several posts garnering over 20,000 unique views.

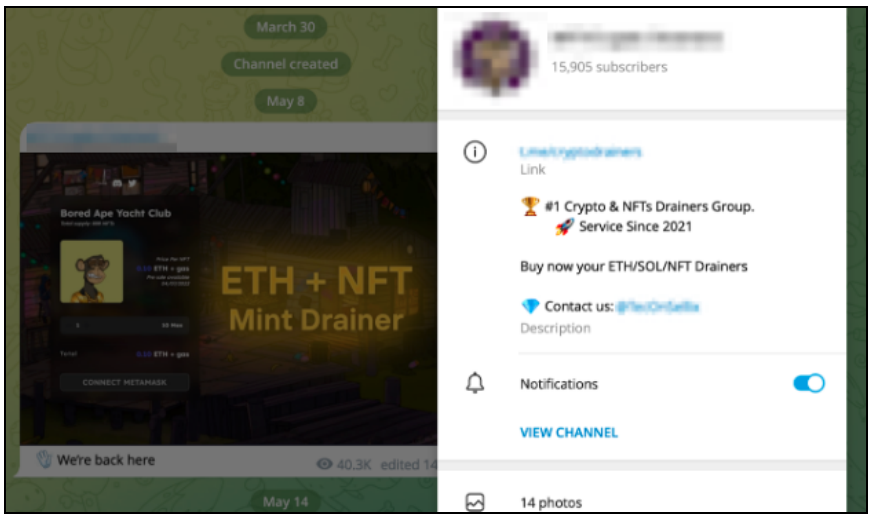


***Figure 12:** A Telegram channel focused on crypto drainers has exploded in popularity since its creation in March 2022 (Source: Telegram)*

Thanks to their widespread development and ease of use, it is likely crypto drainers will only continue to grow in popularity. A particularly troubling sign is that one popular coding repository contains 225 repositories for crypto drainer projects, with over 16 million "commits" (that is, altered and saved versions of the original project). Taken with the 101 phishing domains and attacker wallets that we identified, these findings suggest that crypto drainers are already seeing widespread use among threat actors.

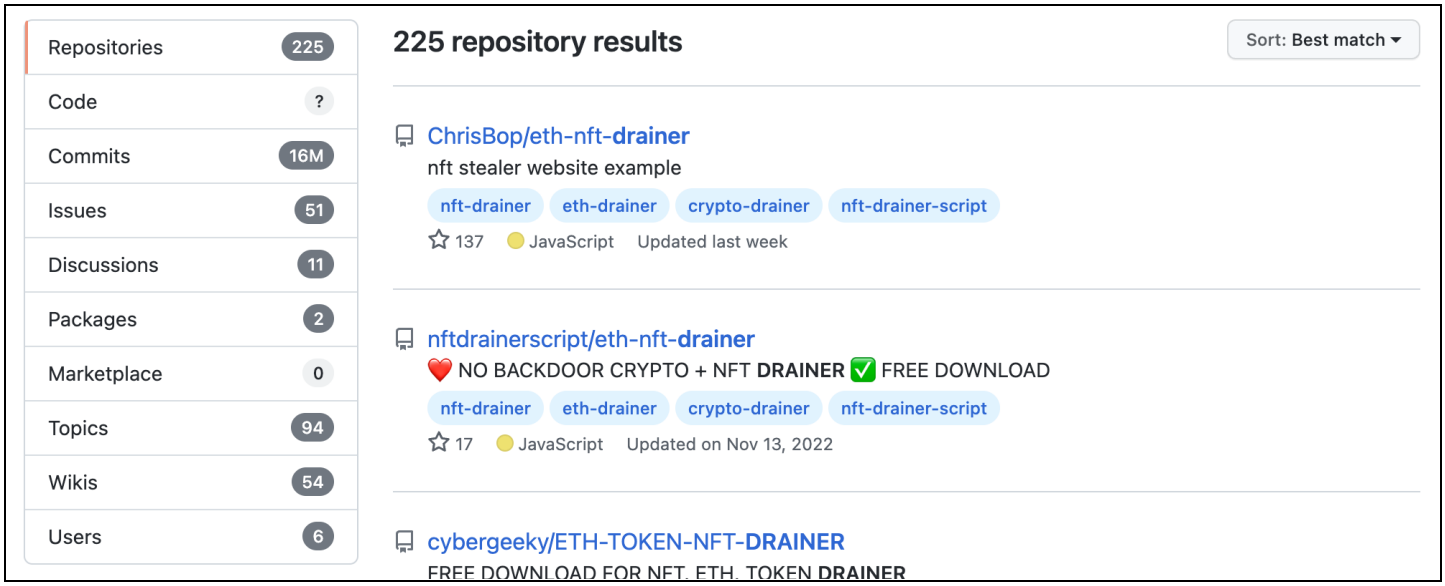


Figure 13: *Crypto drainer projects saved to code repositories see wide distribution (Source: a popular source code repository)*

Mitigations

- Exercise the utmost caution when conducting crypto transactions. Crypto assets are protected by none of the institutional safeguards that mitigate "traditional" fraud.
- Use hardware wallets. Hardware wallets can vastly improve your security posture compared to "hot wallets" like Metamask, which are always connected to the Internet. For hard wallets that are connected to Metamask, all transactions must be approved via the hard wallet, which provides an additional security layer.
- Only use trustworthy dApps and verify smart contract addresses to confirm their authenticity and integrity. True NFT minting interactions rely on smart contracts that may be part of a larger dApp. Contract addresses can be verified using MetaMask, block explorers like Etherscan, or sometimes directly within the dApp.
- Double-check the web addresses of official websites to avoid imitations. Some crypto drainer phishing pages may rely on typosquatting to victimize unsuspecting users.
- Question offers that are too good to be true. Crypto drainer phishing pages attract victims with advantageous cryptocurrency exchange rates or cheap gas fees for NFT minting interactions.
- Resist pressure tactics. Scams often induce a sense of urgency to pressure victims into impulsive actions, and crypto drainer phishing scams are no exception.

Outlook

Crypto drainer phishing pages target crypto users who make use of popular crypto services. These phishing pages frequently use legitimate applications and browser extensions. The use of these legitimate services not only facilitates crypto drainer phishing attacks but also increases the likelihood that these phishing pages will pass an otherwise savvy user's "scam litmus test". Once crypto wallets have been compromised, no safeguards exist to prevent the illicit transfer of assets to attackers' wallets.

We analyzed one crypto drainer phishing page template in detail and concluded that it can be effectively used to steal crypto assets from unsuspecting victims. Furthermore, we identified 9 phishing pages that made use of this template, 92 phishing pages that made use of other templates, and the crypto wallet addresses of the attackers who configured these phishing pages. Taken together with crypto drainers' explosive popularity and the growing presence of ready-to-go crypto drainer phishing packages across the web, our findings demonstrate that crypto drainer phishing scams are relevant, likely effective, and growing in use throughout the cybercriminal community.