

Forum:[Hack Forums](#)

Thread: [Crypto Phishing Alert Stay Safe!](#)

Astroming - April 13, 2025, 6:24 pm

A recent phishing scam led to a major loss of approximately \$760K in wstETH, stETH, and pufETH due to malicious approvals.

? Key Wallets Involved

? Victim's Wallet: 0x5789A38a3FAcfaa86ED950e88D79a9A2F6140052 – \$760K stolen

? Hacker's Wallet: 0xA212763d2BdDb0BD704f1df9Ab9F3A6b64ACa633 – Holding stolen funds

? Drainer Wallet: 0xFC4EAA4ac84D00f1C5854113581F881b42b4A745 – Linked to multiple scams

? What's Happening?

Unlike other scams where funds are quickly laundered, the hacker's wallet still holds the stolen assets with no sign of movement.

? Hacker's Wallet Created: June 11, 2024

? Initial Balance: \$850K (and rising)

The drainer wallet, known for its fraudulent activities, was created on July 22, 2024, and now holds over \$3.1M, taking a 10-11% cut from stolen funds.

? How This Scam Works

Scammers use phishing websites to trick victims into signing malicious transactions, redirecting funds through a well-known "Scam-as-a-Service" system: Exogator Drainer.

? Exogator Drainer Facts

Active Since: September 2022

Estimated Total Stolen: Over \$70M

How It Works:

? 20% of stolen funds go to Exogator Drainer

? 80% goes to the scammer

New Variant: A "Lite" version may now take only 10% in fees instead of 20%.

? How Victims Get Tricked

1 Fake websites with malicious smart contracts

2 Victims unknowingly approve a fraudulent transaction

3 Funds are split between the scammer & Exogator Drainer

4 Stolen assets are linked to a malicious smart contract

(0x0000db5c8B030ae20308ac975896e79741e70000)

? The Scale of the Scam

? Over \$100M stolen from thousands of victims

? More than 16,000 wallets affected

? Scammers remain anonymous

Mewtwo - April 14, 2025, 3:01 am

Believe it or not, these phishing attacks do happen quite often. Crypto websites get breached and the public isn't known about it. Then there's an email sent to you regarding that crypto site, or any other site, like for example: phishing FTX reimbursement:

First, they get a compromised SMTP /website bug that has a reputable email trust, that allows them to send any type of email from there. Then they have a website that looks exactly like FTX reimbursement, but ask for your email/password login, seed phrases, or any other personal information. People fall for this. These are the big red flags that should always be taken.

Toscan - April 14, 2025, 10:30 am

Email spoofing is so easy I don't ever trust any links for emails or even people in general

Phishing scams are EVERYWHERE. It's so common these days I don't really use my email. Although to avoid these scams ALWAYS check the URL and verify it is legitimate. DOUBLE CHECK the link or even TRIPLE CHECK the link you're on.

Email's are not safe, it doesn't matter if the e-mail seems legit because they can spoof "fake" their sending email address and name, and even the hyperlinks they send to you will actually say the link is legit. Always right click these links and paste them into the address bar, and once you navigate to the link make sure the link is safe once you're there. Now ONLY if the link is correctly spelled and is indeed the right safe URL. It will be safe. Phishing attacks only work if you give them your details and submit them, or if you click any weird pop ups url on their site that can lead to hijacking your PC.

SIM-5613027 - April 20, 2025, 4:54 pm

(Apr 13, 2025 06:24 PM)Astroming Wrote: [\[CITE\]](#) A recent phishing scam led to a major loss of approximately \$760K in wstETH, stETH, and pufETH due to malicious approvals.

? Key Wallets Involved

? Victim's Wallet: 0x5789A38a3FAcfaa86ED950e88D79a9A2F6140052 – \$760K stolen

? Hacker's Wallet: 0xA212763d2BdDb0BD704f1df9Ab9F3A6b64ACa633 – Holding stolen funds

? Drainer Wallet: 0xFC4EAA4ac84D00f1C5854113581F881b42b4A745 – Linked to multiple scams

? What's Happening?

Unlike other scams where funds are quickly laundered, the hacker's wallet still holds the stolen assets with no sign of movement.

? Hacker's Wallet Created: June 11, 2024

? Initial Balance: \$850K (and rising)

The drainer wallet, known for its fraudulent activities, was created on July 22, 2024, and now holds over \$3.1M, taking a 10-11% cut from stolen funds.

? How This Scam Works

Scammers use phishing websites to trick victims into signing malicious transactions, redirecting funds through a well-known "Scam-as-a-Service" system: Exogator Drainer.

? Exogator Drainer Facts

Active Since: September 2022

Estimated Total Stolen: Over \$70M

How It Works:

- ? 20% of stolen funds go to Exogator Drainer
- ? 80% goes to the scammer

New Variant: A "Lite" version may now take only 10% in fees instead of 20%.

? How Victims Get Tricked

- 1 Fake websites with malicious smart contracts
- 2 Victims unknowingly approve a fraudulent transaction
- 3 Funds are split between the scammer & Exogator Drainer
- 4 Stolen assets are linked to a malicious smart contract
(0x0000db5c8B030ae20308ac975896e79741e70000)

? The Scale of the Scam

- ? Over \$100M stolen from thousands of victims
- ? More than 16,000 wallets affected
- ? Scammers remain anonymous

Well, just dont approve a permit and a random contract as the spender. Nowadays anyway blockaid stops most drainer attacks. For example inferno drainer went from making easily \$40m monthly to only \$2m last month. (according to realscamsniffer) they have drained in total over \$500m.... crazy amount overall.