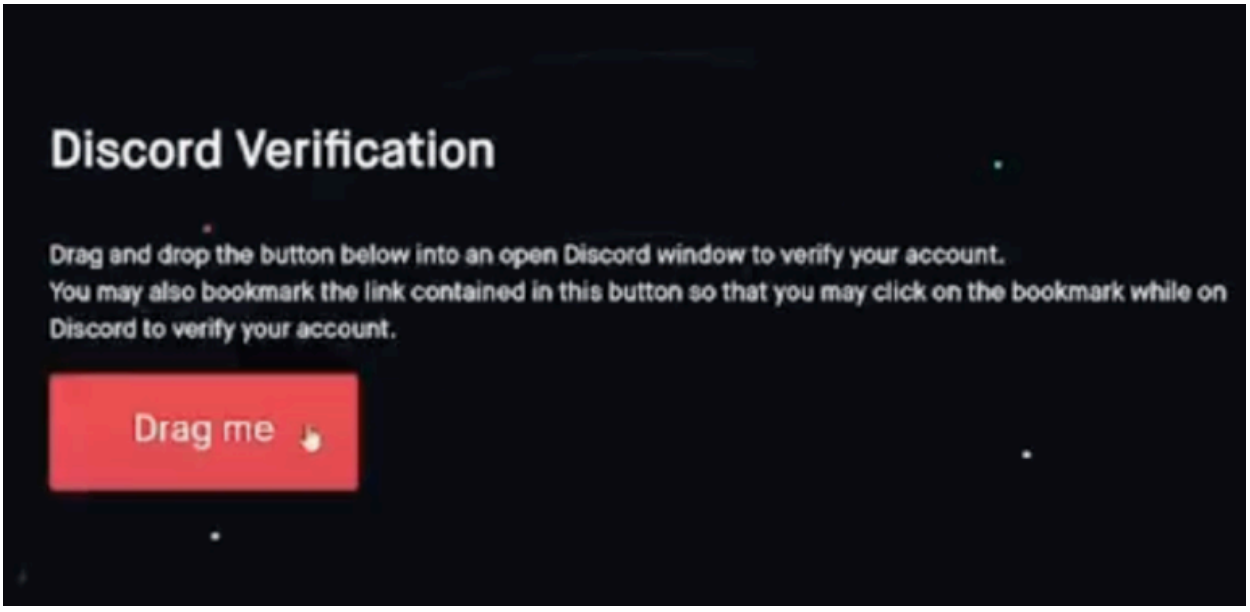
Discord Admins Hacked by Malicious Bookmarks

Published: 2023-05-31 · Archived: 2026-04-02 11:50:59 UTC

A number of **Discord** communities focused on cryptocurrency have been hacked this past month after their administrators were tricked into running malicious Javascript code disguised as a Web browser bookmark.



This attack involves malicious Javascript that is added to one's browser by dragging a component from a web page to one's browser bookmarks.

According to interviews with victims, several of the attacks began with an interview request from someone posing as a reporter for a crypto-focused news outlet online. Those who take the bait are sent a link to a Discord server that appears to be the official Discord of the crypto news site, where they are asked to complete a verification step to validate their identity.

As shown in this Youtube video, the verification process involves dragging a button from the phony crypto news Discord server to the bookmarks bar in one's Web browser. From there, the visitor is instructed to go back to discord.com and then click the new bookmark to complete the verification process.

However, the bookmark is actually a clever snippet of Javascript that quietly grabs the user's Discord token and sends it to the scammer's website. The attacker then loads the stolen token into their own browser session and (usually late at night after the admins are asleep) posts an announcement in the targeted Discord about an exclusive "airdrop," "NFT mint event" or some other potential money making opportunity for the Discord members.

The unsuspecting Discord members click the link provided by the compromised administrator account, and are asked to connect their crypto wallet to the scammer's site, where it asks for unlimited spend approvals on their tokens, and subsequently drains the balance of any valuable accounts.

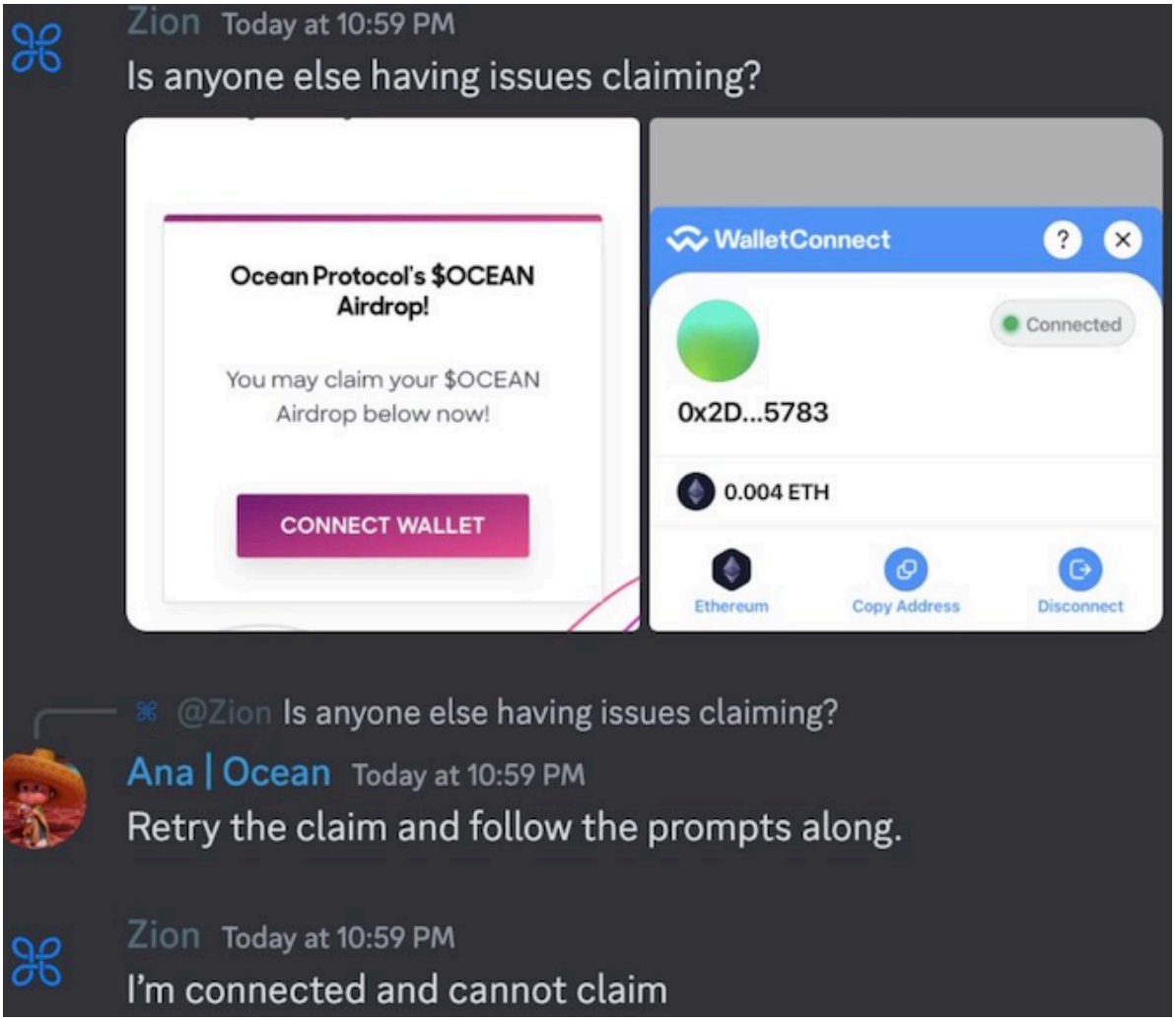
Meanwhile, anyone in the compromised Discord channel who notices the scam and replies is banned, and their messages are deleted by the compromised admin account.

Nicholas Scavuzzo is an associate at Ocean Protocol, which describes itself as an "open-source protocol that aims to allow businesses and individuals to exchange and monetize data and data-based services." On May 22, an administrator for Ocean Protocol's Discord server clicked a link in a direct message from a community member that prompted them to prove their identity by dragging a link to their bookmarks.

Scavuzzo, who is based in Maine, said the attackers waited until around midnight in his timezone time before using the administrator's account to send out an unauthorized message about a new Ocean airdrop.

Scavuzzo said the administrator's account was hijacked even though she had multi-factor authentication turned on.

"A CAPTCHA bot that allows Discord cookies to be accessed by the person hosting the CAPTCHA," was how Scavuzzo described the attack. "I've seen all kinds of crypto scams, but I've never seen one like this."



In this conversation, "Ana | Ocean" is a compromised Discord server administrator account promoting a phony airdrop.

Importantly, the stolen token only works for the attackers as long as its rightful owner doesn't log out and back in, or else change their credentials.

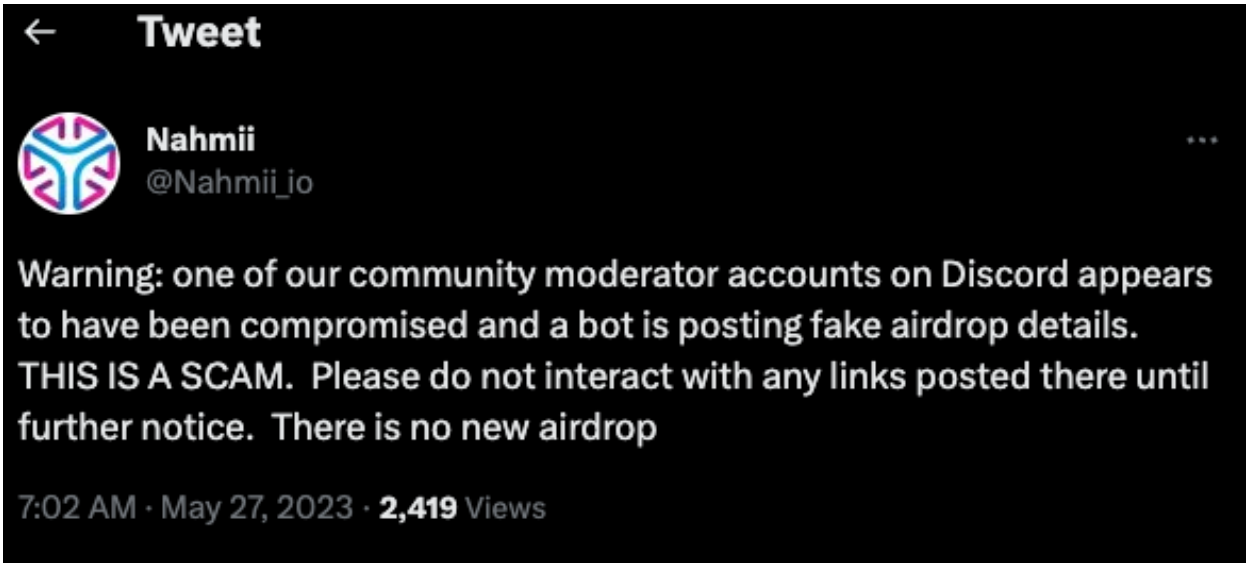
Assuming the administrator can log in, that is. In Ocean's case, one of the first things the intruders did once they swiped the administrator's token was change the server's access controls and remove all core Ocean team members from the server.

Fortunately for Ocean, Scavuzzo was able to reach the operator of the server that hosts the Discord channel, and have the channel's settings reverted back to normal.

"Thankfully, we are a globally distributed team, so we have people awake at all hours," Scavuzzo said, noting that Ocean is not aware of any Discord community members who fell for the phony airdrop offer, which was live for about 30 minutes. "This could have been a lot worse."

On May 26, **Aura Network** reported on Twitter that its Discord server was compromised in a phishing attack that resulted in the deletion of Discord channels and the dissemination of fake Aura Network Airdrop Campaign links.

On May 27, **Nahmii** — a cryptocurrency technology based on the Ethereum blockchain — warned on Twitter that one of its community moderators on Discord was compromised and posting fake airdrop details.



On May 9, **MetrixCoin** reported that its Discord server was hacked, with fake airdrop details pushed to all users.

KrebsOnSecurity recently heard from a trusted source in the cybersecurity industry who dealt firsthand with one of these attacks and asked to remain anonymous.

“I do pro bono Discord security work for a few Discords, and I was approached by one of these fake journalists,” the source said. “I played along and got the link to their Discord, where they were pretending to be journalists from the Cryptonews website using several accounts.”

The source took note of all the Discord IDs of the admins of the fake Cryptonews Discord, so that he could ensure they were blocked from the Discords he helps to secure.

“Since I’ve been doing this for a while now, I’ve built up a substantial database of Discord users and messages, so often I can see these scammers’ history on Discord,” the source said.

In this case, he noticed a user with the “CEO” role in the fake Cryptonews Discord had been seen previously under another username — “**Levatax**.” Searching on that Discord ID and username revealed a young Turkish coder named **Berk Yilmaz** whose Github page linked to the very same Discord ID as the scammer CEO.

Reached via instant message on **Telegram**, Levatax said he’s had no involvement in such schemes, and that he hasn’t been on Discord since his **Microsoft Outlook** account was hacked months ago.

“The interesting thing [is] that I didn’t use Discord since few months or even social media because of the political status of Turkey,” Levatax explained, referring to the recent election in his country. “The only thing I confirm is losing my Outlook account which connected to my Discord, and I’m already in touch with Microsoft to recover it.”

The verification method used in the above scam involves a type of bookmark called a “bookmarklet” that stores Javascript code as a clickable link in the bookmarks bar at the top of one’s browser.

While bookmarklets can be useful and harmless, malicious Javascript that is executed in the browser by the user is especially dangerous. So please avoid adding (or dragging) any bookmarks or bookmarklets to your browser unless it was your idea in the first place.
