The Far-Reaching Attacks of the Void Balaur Cybermercenary Group

Archived: 2026-04-05 15:02:11 UTC

Void Balaur's Offerings

One of the threat actor's primary services is hacking into the mailboxes of email providers and social media accounts. Void Balaur, in some cases, can even provide complete copies of mailboxes that are stolen without any user interaction for a higher price. The latter is particularly interesting, since it would take unusual circumstances such as an insider threat or the compromise of an email provider's system to be able to offer private data without user interaction.

Starting in 2019, Void Balaur also began selling the sensitive private data of Russian individuals. These included passport and flight information; criminal records; credit history; account balance and statements; and even printouts of SMS messages. Again, it is difficult to determine how exactly the group manages to gather such an extensive array of information, especially with regards to telecom data — but there are several possibilities, such as telecom engineers being hacked, or even the telecom system itself being compromised.

The group uses Russian underground websites to advertise their products and services, especially in forums such as Darkmoney and Probiv. Void Balaur seems to be highly respected in these underground forums, as the feedback for their services is almost unanimously positive, with their customers pointing out the threat actor's ability to deliver the requested information on time, as well as the quality of the data being provided. Previously, the group also peddled its offerings on a website where it advertised services such as hacking into mailboxes, launching distributed denial-of-service (DDoS) attacks, and flooding phone numbers in Commonwealth of Independent States (CIS) countries.

Figure 1. Some of the products being offered by Void Balaur on their website from 2020

Void Balaur also set its sights on cryptocurrency exchanges and their employees, creating numerous phishing sites to lure cryptocurrency exchange users in order to gain access to their wallets. One cryptocurrency exchange in particular — EXMO — has been victimized several times by the group.

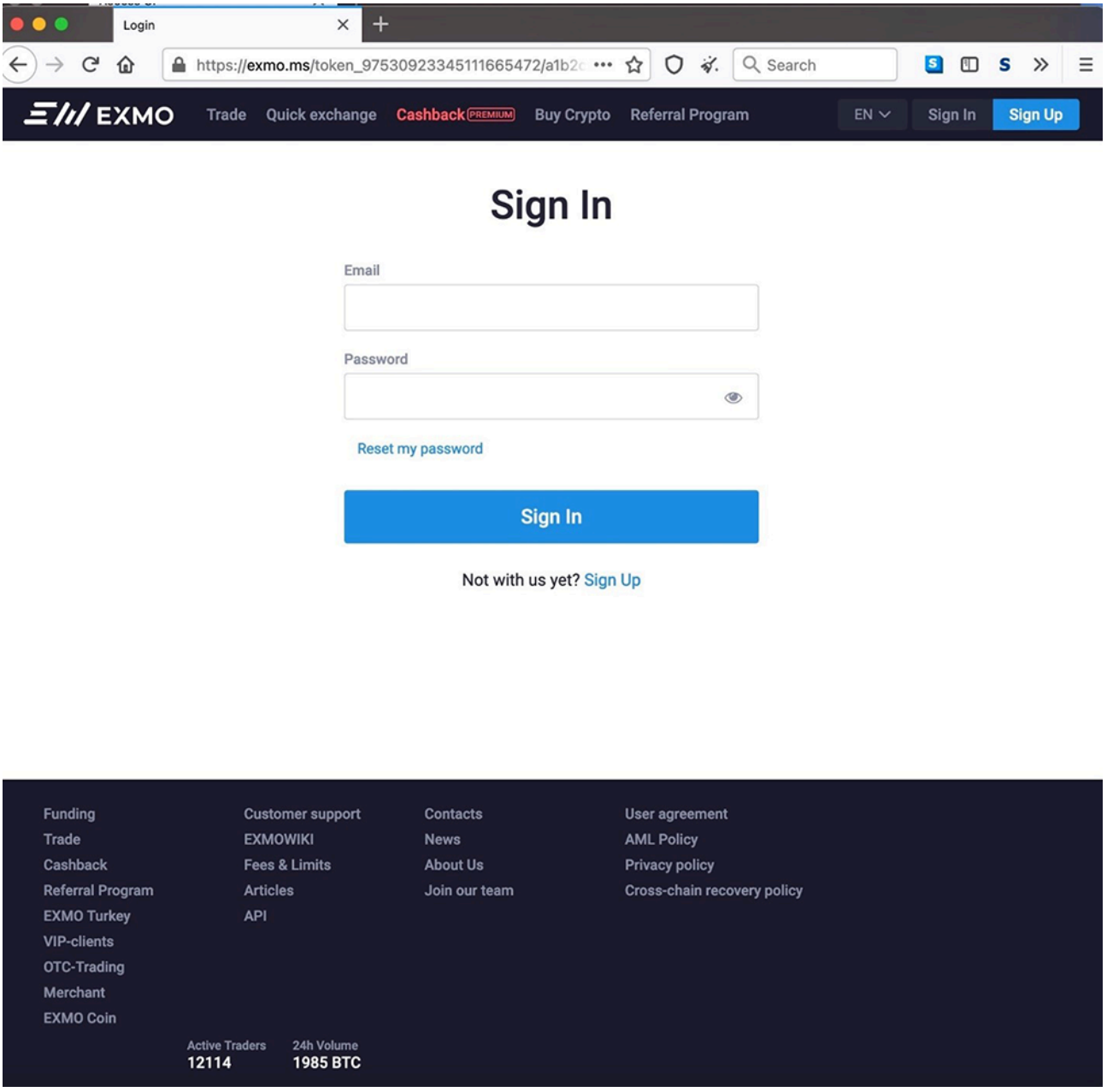

Figure 2. An example of a Void Balaur phishing site that presents itself as a login page for EXMO

An extensive list of victims

We were able to determine the nature of the threat actor's victims with some confidence by correlating indicators such as infrastructure, hostnames, and email addresses to information found in external reports from eQualit.ieopen on a new tab and Amnesty Internationalopen on a new tab.

The reports mentioned attacks on human rights activists, journalists, media websites, and websites that cover political news. Void Balaur is not averse to going after more high-profile targets either, as the group also launched attacks the former head of an intelligence agency, active government ministers, members of the national parliament in an Eastern European country, and even presidential candidates.

It's possible that these were not one-off attacks, but a part of a larger campaign with multiple fronts. In addition, while seemingly financially motivated, many of the threat actor's campaigns could be driven by the desire to cause disruption and strife among their victims.

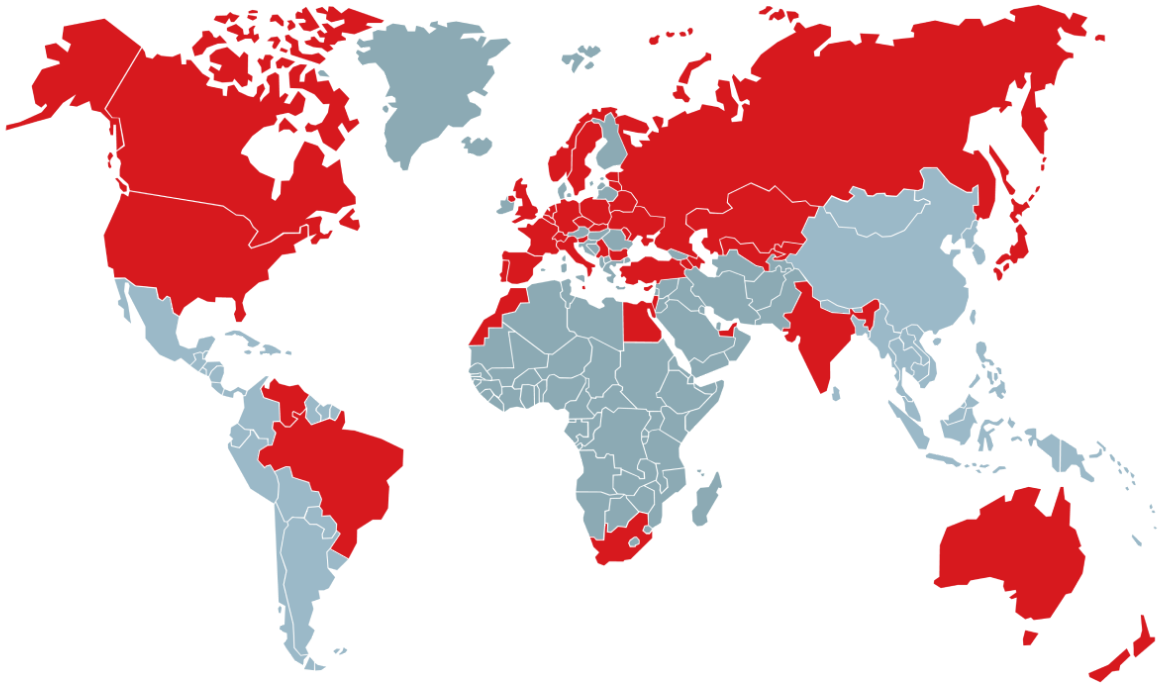

Figure 3. Countries in which Void Balaur email targets were located (companies were targeted via corporate email addresses; individuals were targeted via private email addresses)

Void Balaur's use of malware

Based on the Amnesty International report, Void Balaur has also used seemingly simply — but highly specialized — malware. One of these malwares, called Z*Stealer, is designed to gather credentials from different types of software such as instant messaging apps, email clients, browsers, and Remote Desktop Protocol (RDP) programs. In addition, it is also capable of stealing cryptocurrency wallets.

DroidWatcher is another malware the group uses in its campaigns. Similar to Z*Stealer, it is also meant for information theft, while adding spying and remote tracking capabilities, allowing its users to access sensitive location and communications information.

Defending against cybermercenary attacks

A cybermercenary group like Void Balaur possesses plenty of tools and resources at its disposal for perpetrating attacks against high-profile targets. These security best practices can help mitigate the impact of an attack or even prevent an attack from being successful.

- Choose email providers that prioritize security and have strong security protocols in place.
- Use two-factor authentication (2FA) when accessing email and social media accounts, preferably by using apps or devices specially designed for 2FA.
- Ensure that apps that are used to transmit sensitive information have end-to-end encryption for communications.
- Delete older messages to minimize the chance of sensitive data ending up in the hands of malicious elements. Some mobile apps have a setting that automatically deletes chats after a certain time.
- Employ drive encryption for all machines.
- Turn off both work and personal machines that store important data when not in use
- Consider the use of encryption systems for communication involving sensitive information or dialogue.

Learn more about the cybermercenary known as Void Balaur in our research paper titled Void Balaur: Tracking a Cybermercenary's Activitiesopen on a new tab.

Indicators of compromise related to Void Balaur can be found hereopen on a new tab.

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

We Recommend
