Ermac malware: the other side of the code

By Ben Wagner

Published: 2024-01-29 · Archived: 2026-04-06 02:50:55 UTC

Authors

Ben Wagner

Mobile Security Researcher

IBM Security

When the Cerberus code was leaked in late 2020, IBM Trusteer researchers projected that a new Cerberus mutation was just a matter of time. Multiple actors used the leaked Cerberus code but without significant changes to the malware. However, the MalwareHunterTeam discovered a new variant of Cerberus — known as Ermac (also known as Hook) — in late September of 2022.

To better understand the new version of Cerberus, we can attempt to shed light on the behind-the-scenes operations of the actor maintaining Ermac. While a new version of the malware has been released, we will focus on the original version.

Gaining insight into the backstage operations of the malware is not simply a case of reverse engineering malware samples that were released into the wild. Once that reverse engineering was complete, however, unique and interesting aspects of the inner workings of the malware were revealed.

As a Cerberus descendent, Ermac shares the same source code and fraud capabilities, including stealing a user's bank credentials and second-factor authentication (2FA) messages that are delivered to the user via SMS or notification.

Here is an example of the shared preferences file created by Cerberus and Ermac. We can easily see that Ermac malware has the same elements as Cerberus, and there are also new entries representing new capabilities in Ermac.

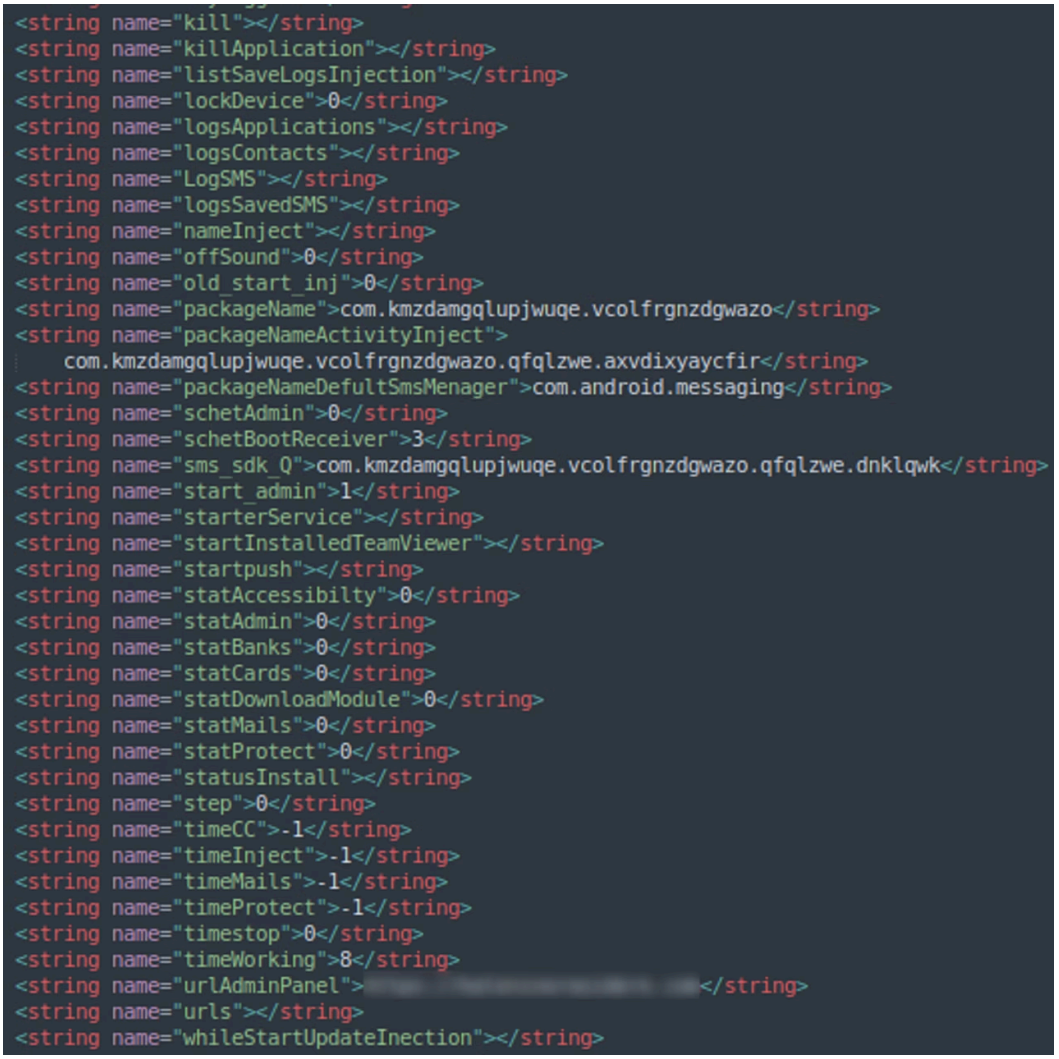

Figure 1: Cerberus shared preference.

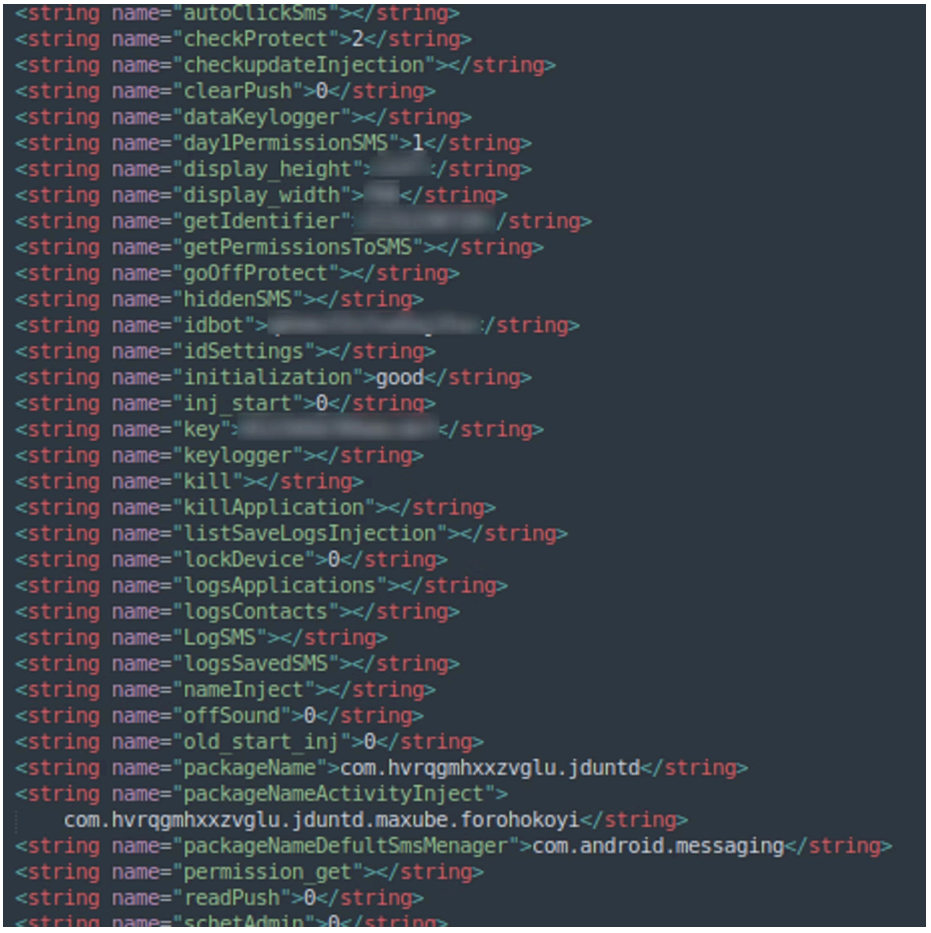

Figure 2: Ermac shared preference.

The capabilities of Ermac were already discussed in depth. However, it is worth mentioning that Ermac malware contains than Cerberus. The Ermac packer is open source and can be found online.

This is yet more evidence that Ermac could be a new operator and that the threat actor is actively maintaining the leaked Cerberus code and constantly evolving Ermac's code base.

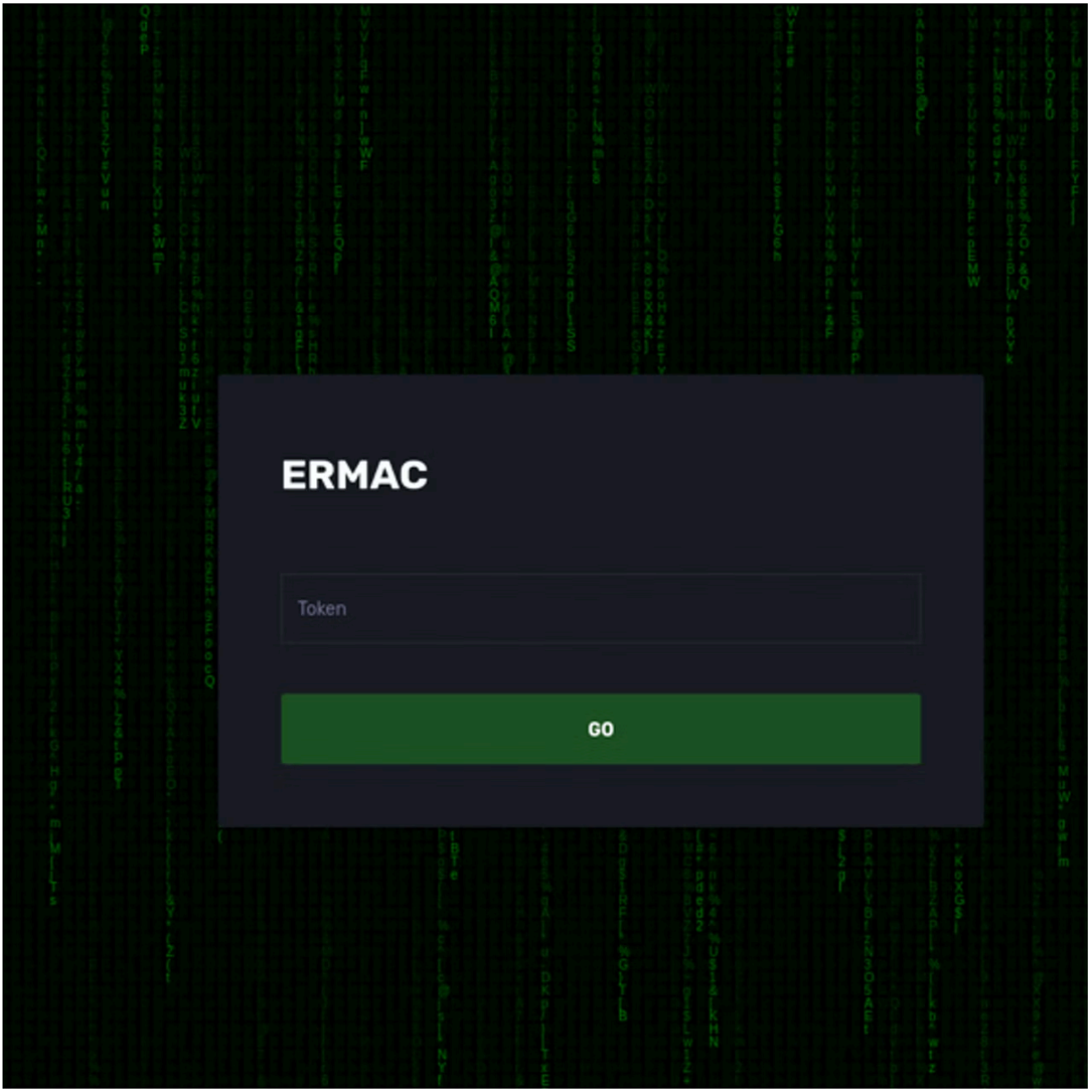

Figure 3: This is the first page presented once connecting to the Ermac command and control server.

A deep dive into the Ermac command and control server (C&C) user interface (UI) reveals the differences between Cerberus and Ermac and provides a unique glimpse into the Ermac functionality, monetization scheme and features under development. IBM Trusteer researchers have discovered two new beta capabilities in the Ermac malware: ransomware and a virtual private network (VPN) connection.

These images taken from the C&C demonstrate Ermac's different capabilities.

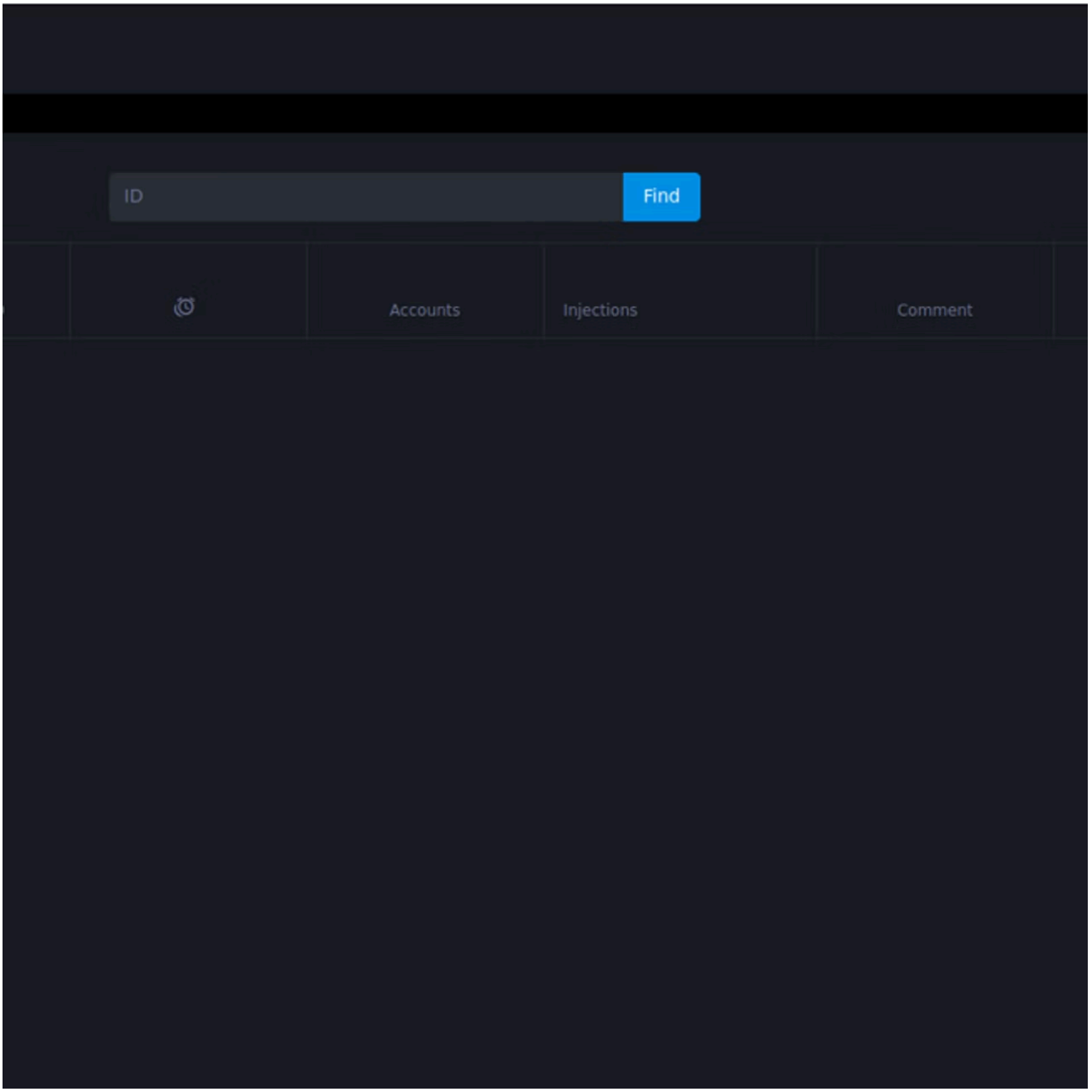

Figure 4: ERMAC C&C bot management page.

The data that the C&C manages is organized in a structured table with multiple columns.

The first column shows the ID that is generated for each bot. We can also see the different actions and device modes: for example, if the user is currently watching the screen, whether different models are loaded and so on.

The next column stores information about the victim's device and operating system version.

Column three stores different tags regarding the bot's status; for example, "favorite," "blacklist" and "trash."

The next column is called GEO and stores information about the country and device location of the bot.

Next, there is information regarding the malware installation date and time and the last time the bot was successfully connected to the C&C.

The “injection” column contains the different applications on which the malware can perform overlay attacks.

The “action” column lists the different actions the C&C operator can command the bot to perform on the victim’s device. These actions include open inject, forward calls, clear application data and more (see Figures 8-13).

The logs column contains the raw data exfiltrated from the victim’s device, including the contact list, 2FA, list of installed applications, application notifications, keystrokes log and more.

Figure 5: Ermac capabilities.

One of the most interesting screens is the “Auto command,” which is still in beta mode. On the screen, we can see capabilities like sending SMS, opening inject (overlay screen), grabbing the contacts list and the killbot, which is an Ermac self-destruct switch. We can also see unique commands such as “Clear app data” and “Get Accounts.”

Visibility to the C&C exposes new commands still under development: “beta Ransomware” and “beta Set bot VPN.”

Figure 6: Ermac events.

Here, we can see Ermac events. All activities of the bots can be seen in this figure.

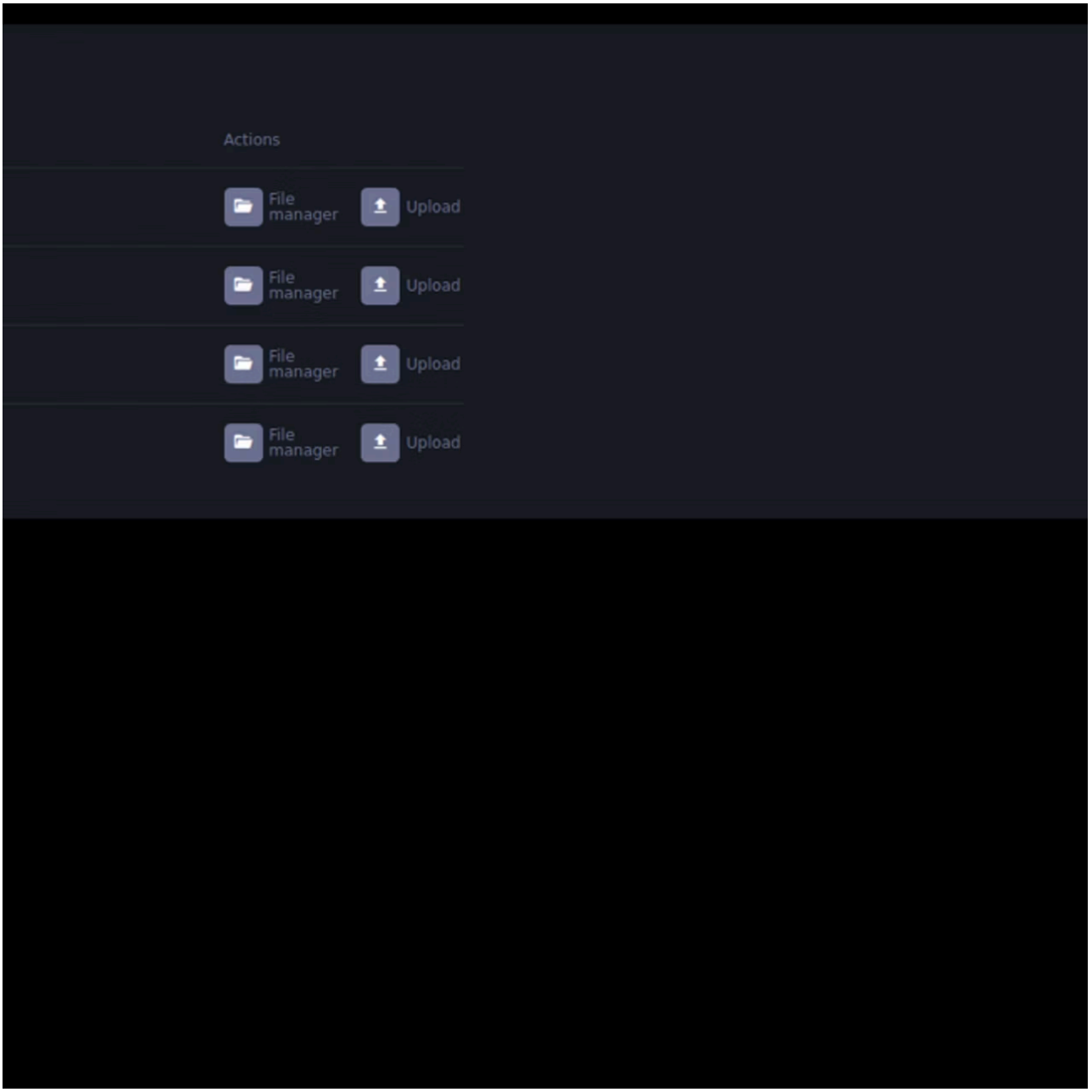

Figure 7: Devices list screen (in development).

Another capability that is still under development is the ability to upload or download files from the bot itself. In production, this allows the bot operator to have more control over the victim's machine and opens the door to new attack tactics.

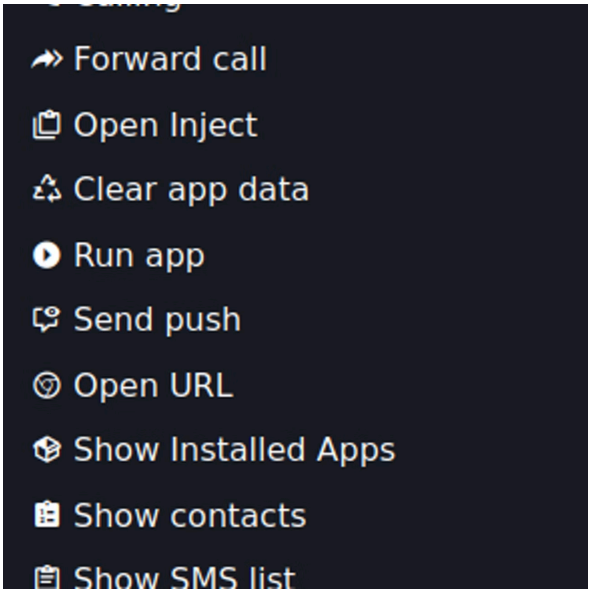

Figure 8: Bot commands.

The malware operator can choose any of the infected devices, initiate a call from that device and even pick which SIM to use for the call. The “lock screen” checkbox can be turned on or off. While on, Ermac shows the victim a fake screen during the entire duration of the call, thus hiding the ongoing call from the victim while preventing any other use of the device.

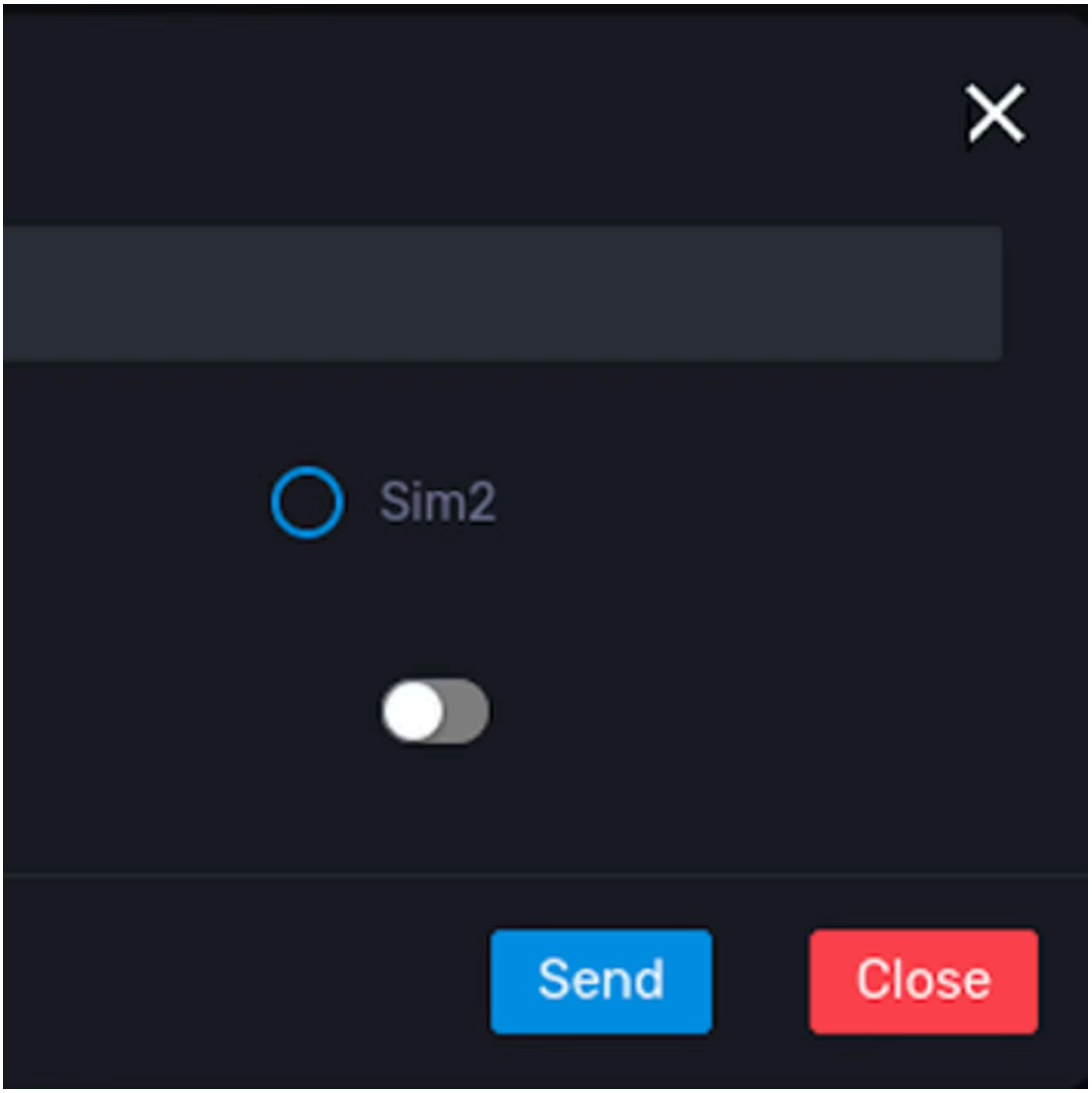

Figure 9: Calling command.

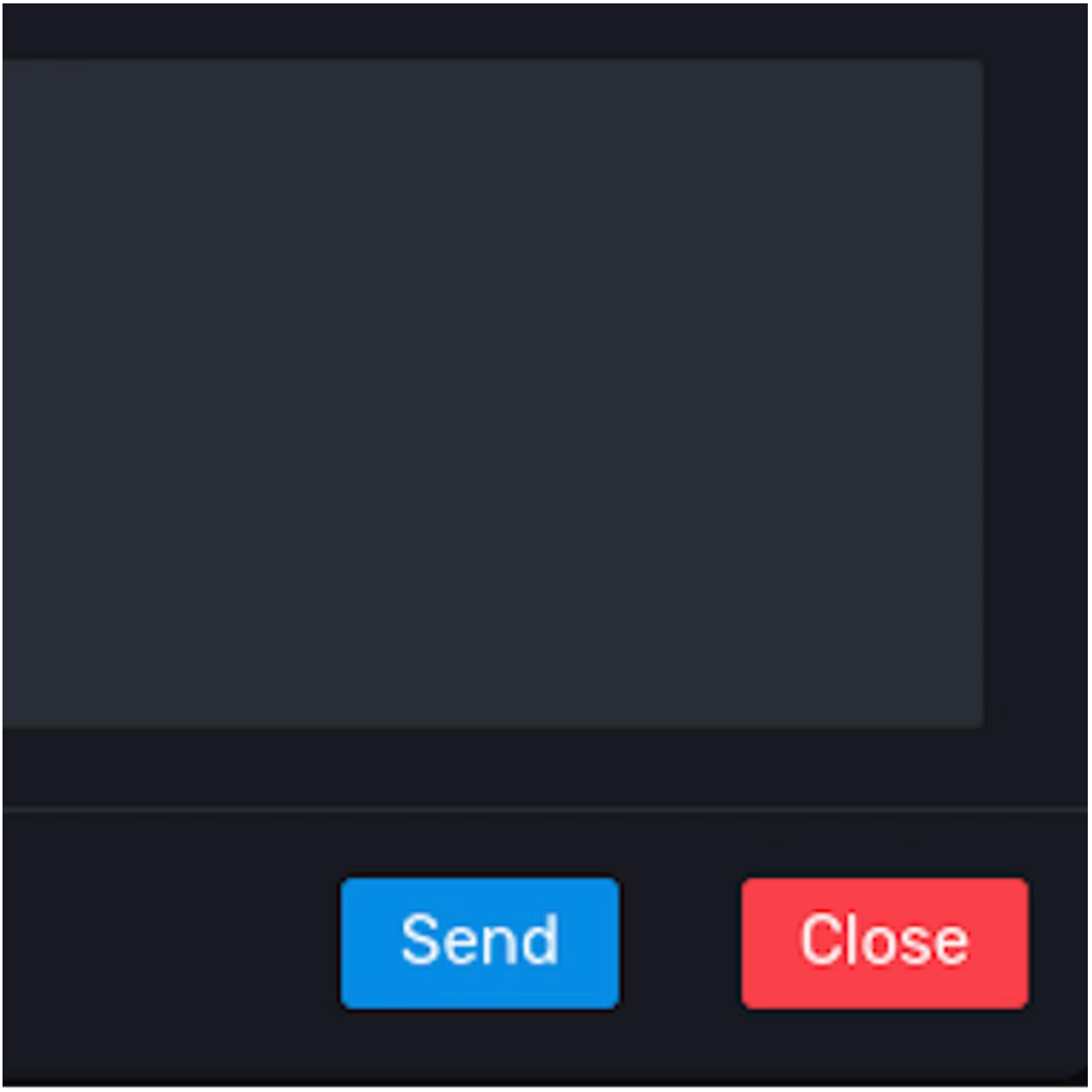

Figure 10: SMS command.

The clear cache command can be used to clear all the data of an app. When the malware clears the data, it also clears the cache.

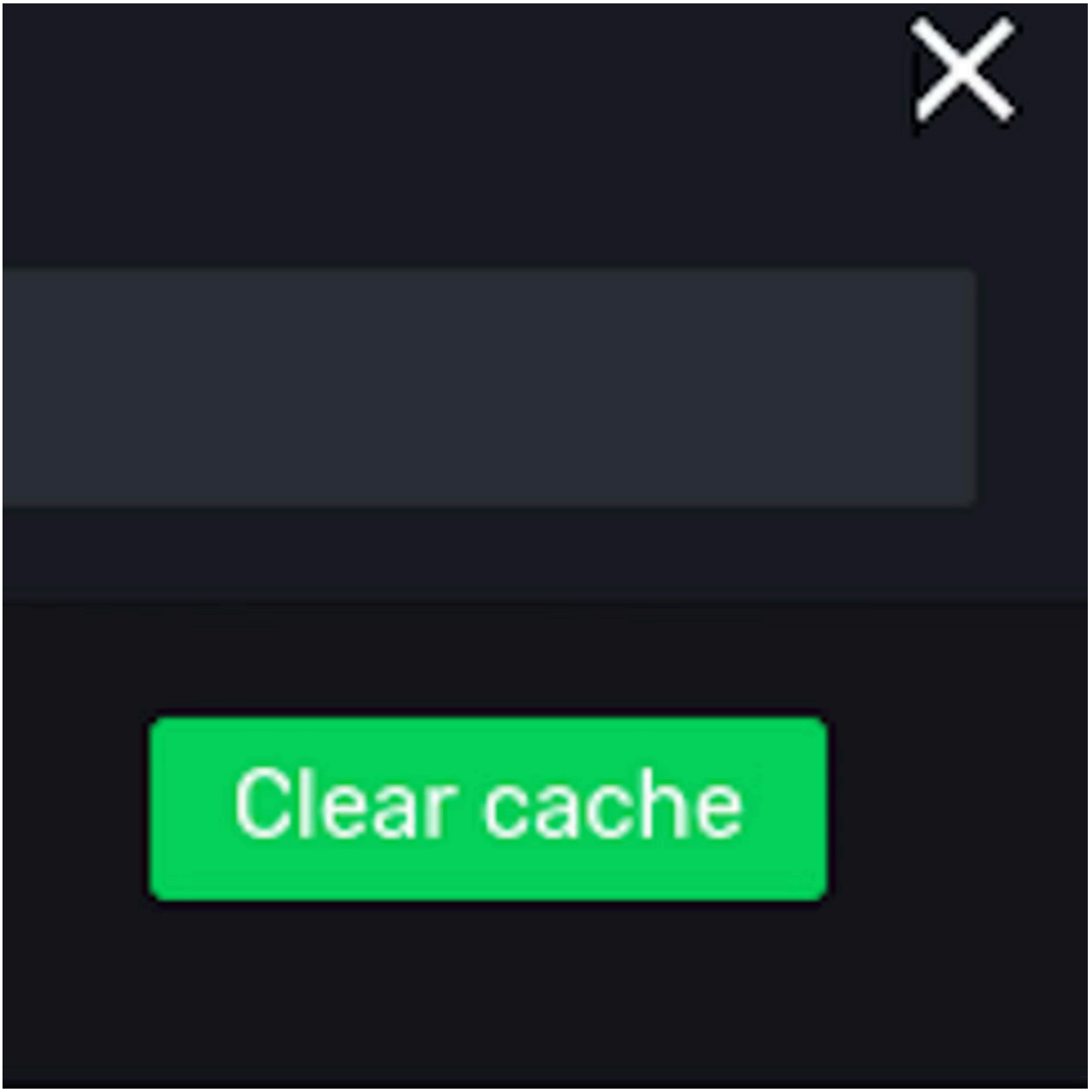

Figure 11: Clear Cache command.

The fraudster can lure victims to open their bank application by sending a push notification with a text from the "bank."

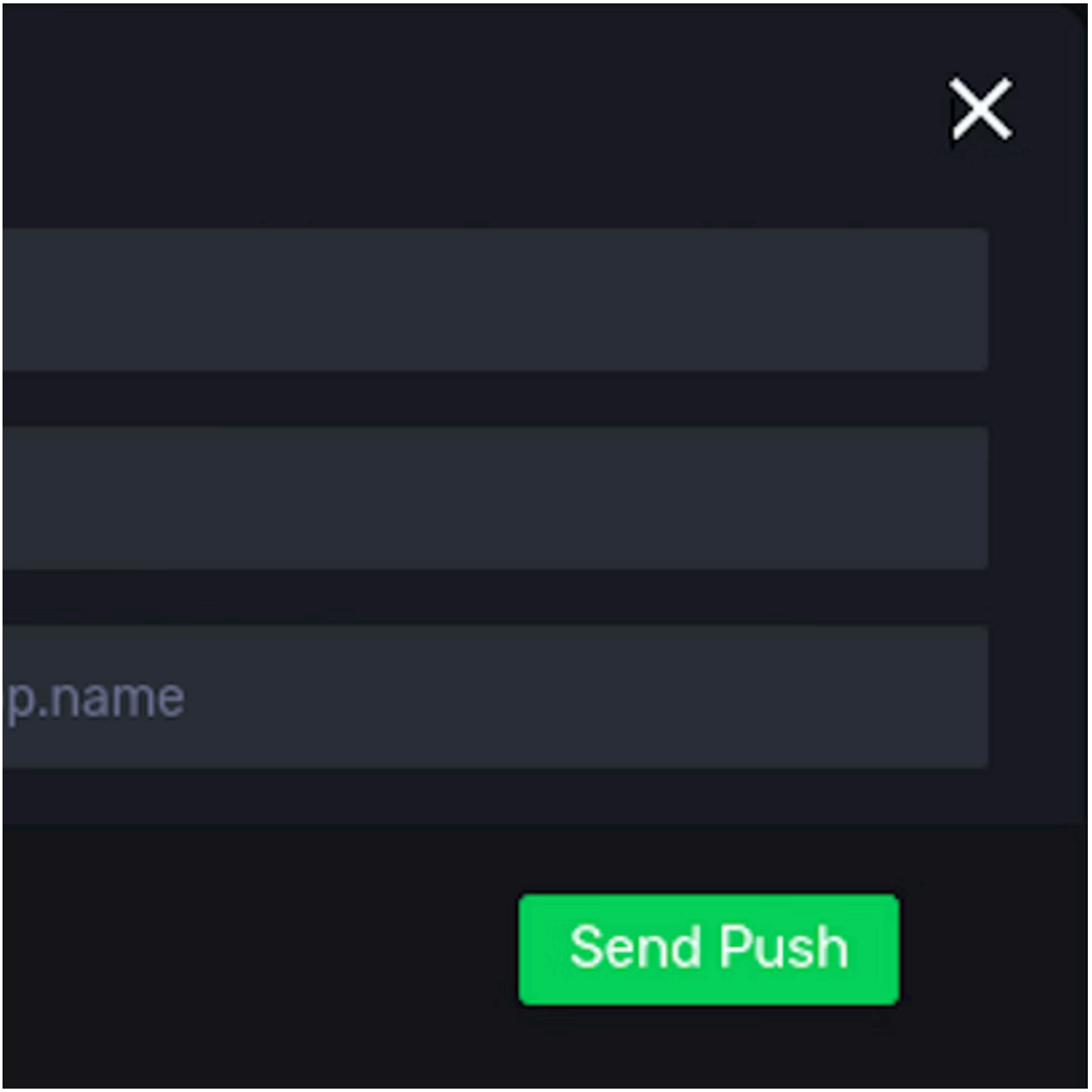

Figure 12: Send Push command.

The fraudsters can steal the seed phrase from the user's device used for the crypto wallet and later use it to log in to the victim's account without having to prove their identity.

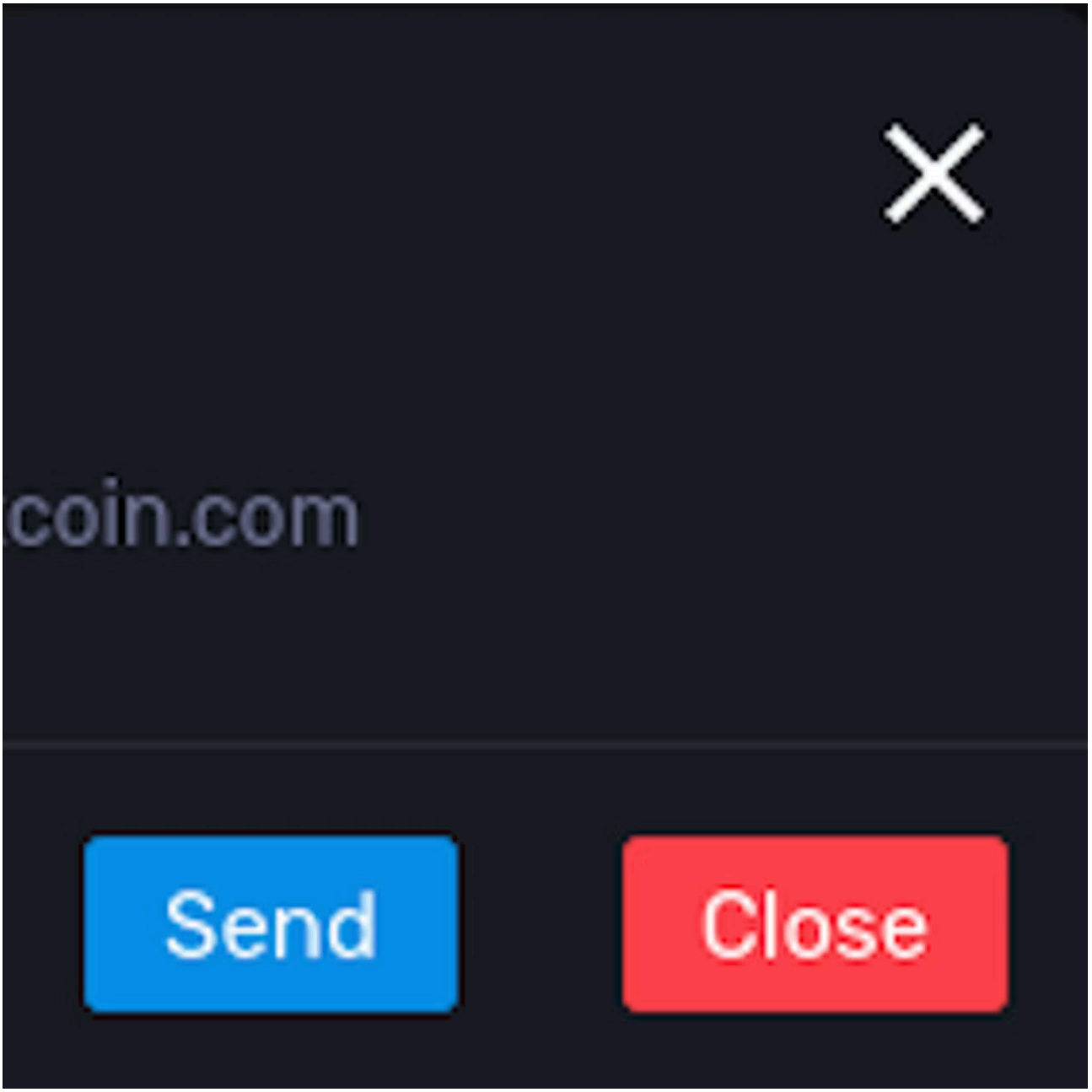

Figure 13: Get Seed Phrase command.

In the C&C user management panel, we can see all the users and roles that exist in the system. This demonstrates that Ermac is built to be operated in a fraud-as-a-service (FaaS) model. The Ermac operator, “root,” can create a new user and password from this screen that can later be used by a fraudster client to manage their bots by logging into the C&C using this new user.

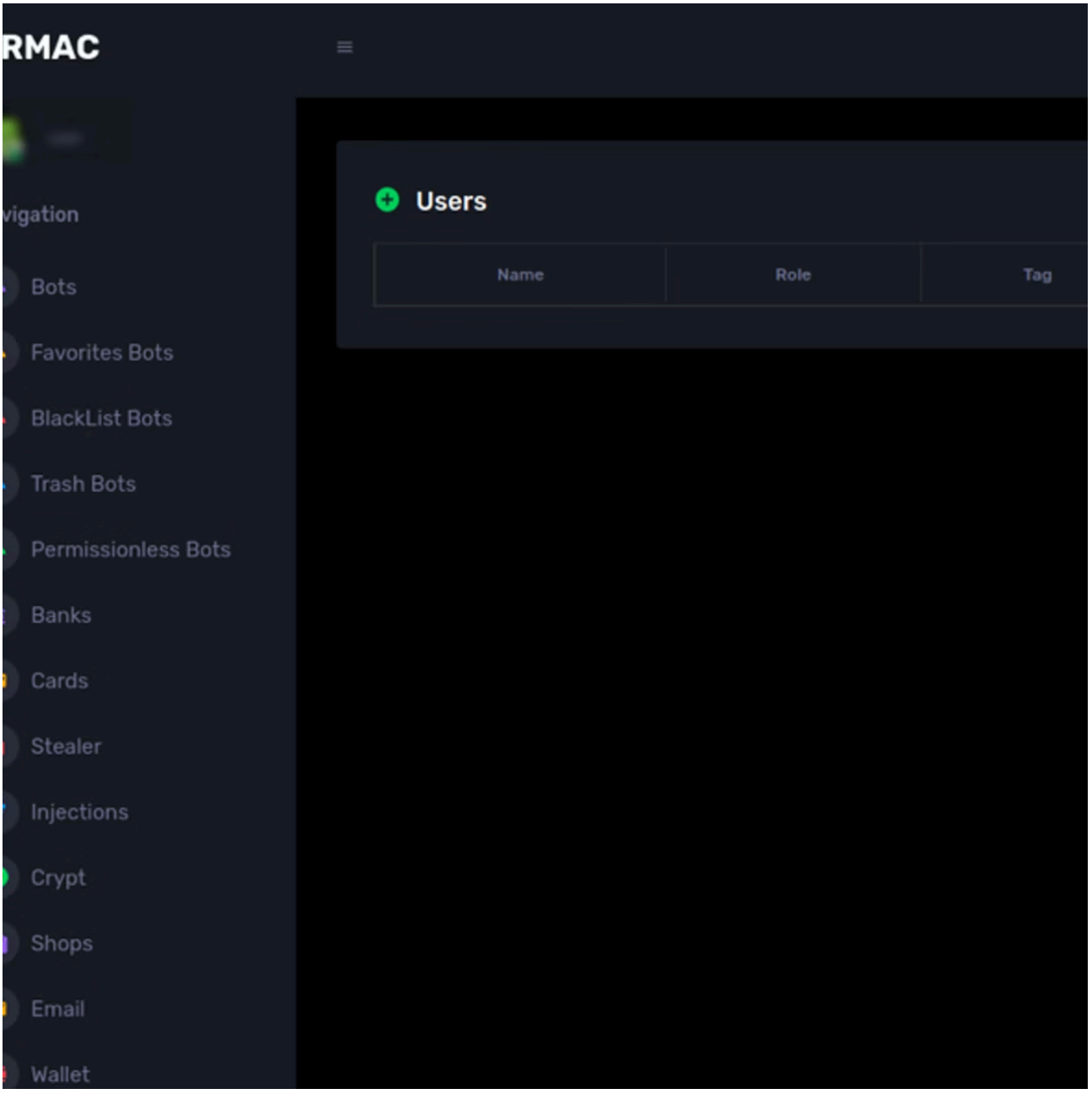

Figure 14: C&C user management panel.

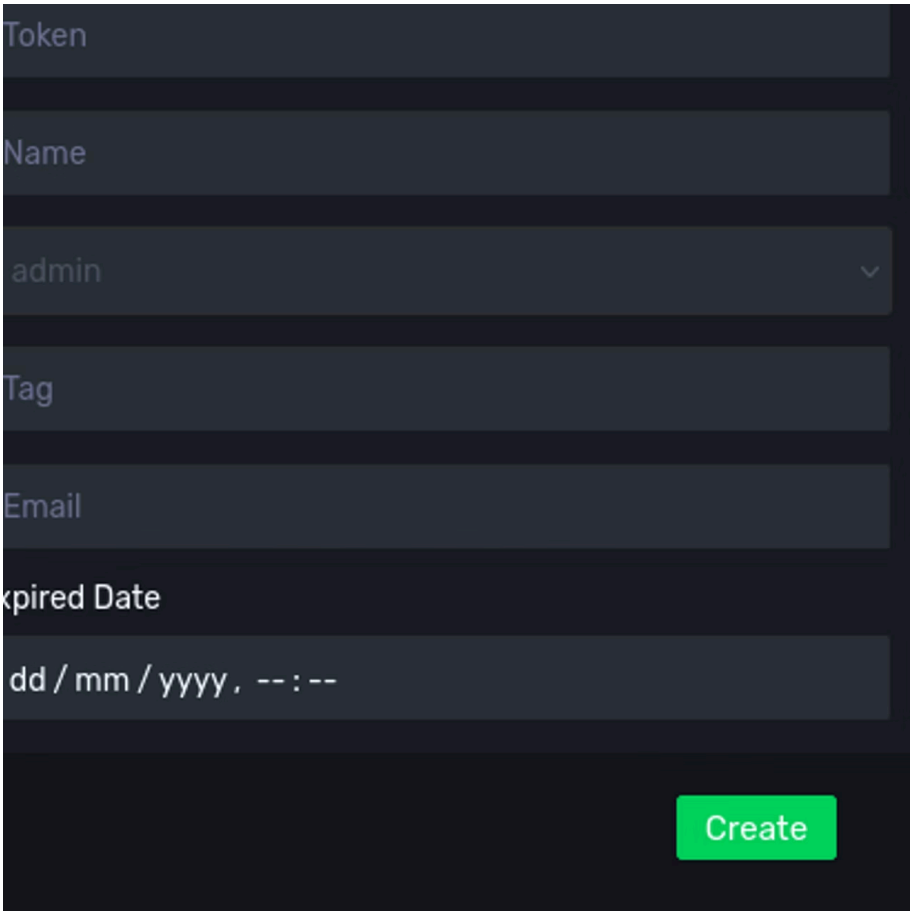

Figure 15: C&C user management panel "Create New User" screen.

When the admin creates a new user, they can pick a token (password) for the user to log in with and can assign a role to the user.

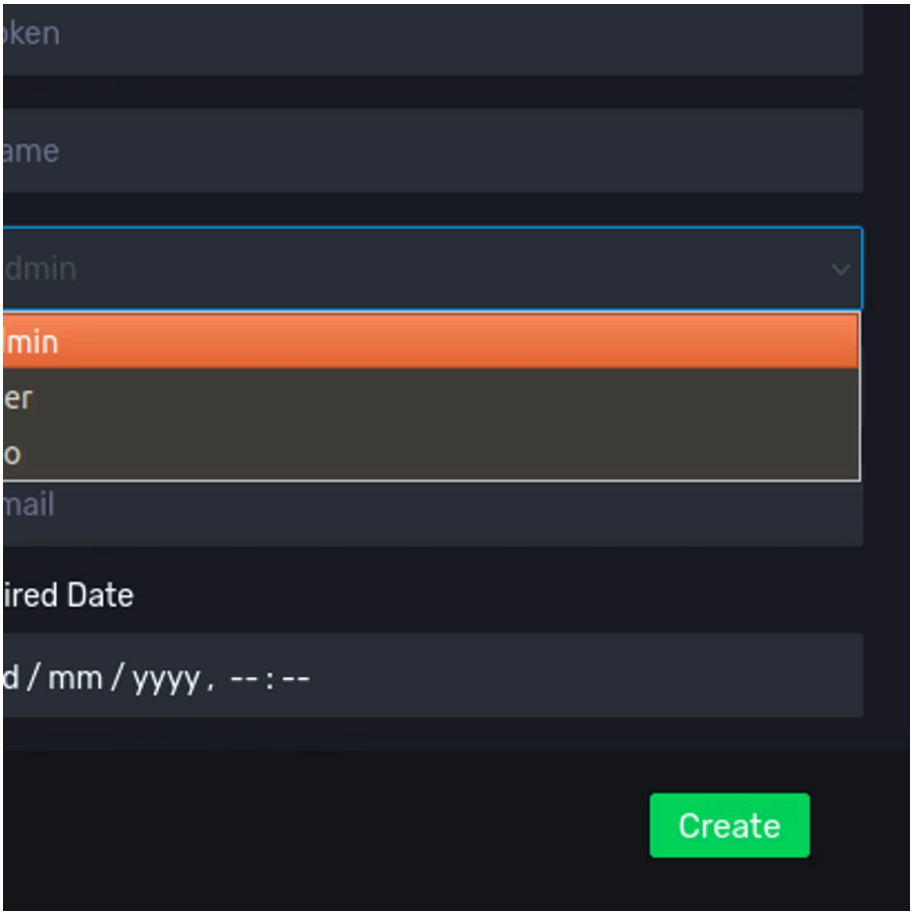

Figure 16: C&C user management panel "Create New User" screen defines a role.

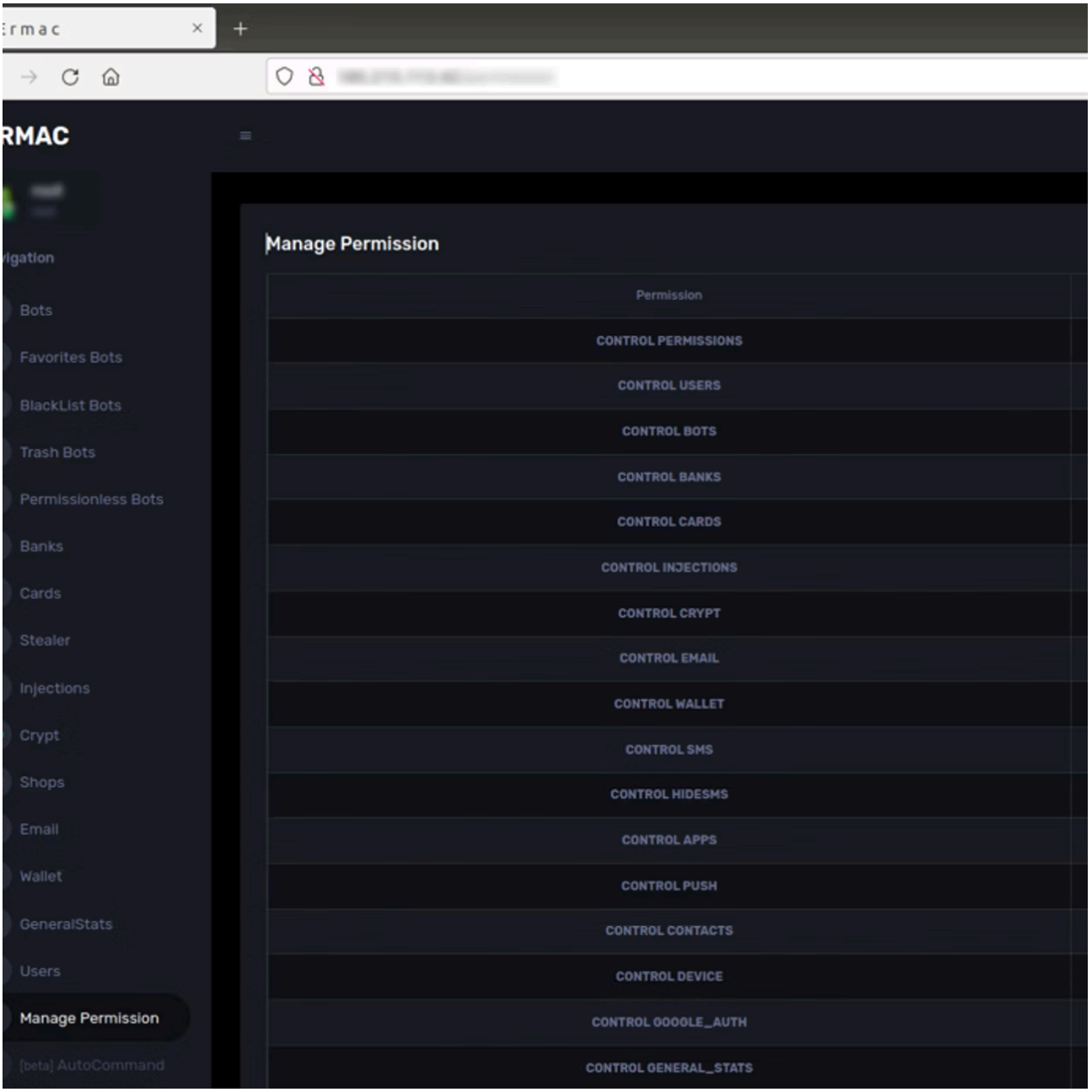

Figure 17: Permissions screen.

Each role has its own permission profile that is managed on the permissions screen.

Although Ermac's risk is very similar to Cerberus, Ermac has some new capabilities that have not been seen before. This is one of the more sophisticated Cerberus mutants because of the new capabilities that it offers, such as "ransomware" and "set bot VPN."

We expect to see more mutations with new capabilities using Cerberus's leaked code. It is interesting and rare to have a look from "the other side" of malware, as we have done in this article, to see the C&C and how fraudsters manage and control bots all over the world.

IBM Trusteer researchers will continue to monitor changes in the malware and keep you updated.

The author would like to thank Nethanella Messer and James Kilner for their contribution to this article.
