Raccoon Stealer malware suspends operations due to war in Ukraine

By Lawrence Abrams

Published: 2022-03-25 · Archived: 2026-04-05 14:17:30 UTC

The cybercrime group behind the development of the Raccoon Stealer password-stealing malware has suspended its operation after claiming that one of its developers died in the invasion of Ukraine.

Raccoon Stealer is an information-stealing trojan distributed under the MaaS (malware-as-a-service) model for $75/week or $200/month. Threat actors who subscribe to the operation will get access to an admin panel that lets them customize the malware, retrieve stolen data (aka logs), and create new malware builds.

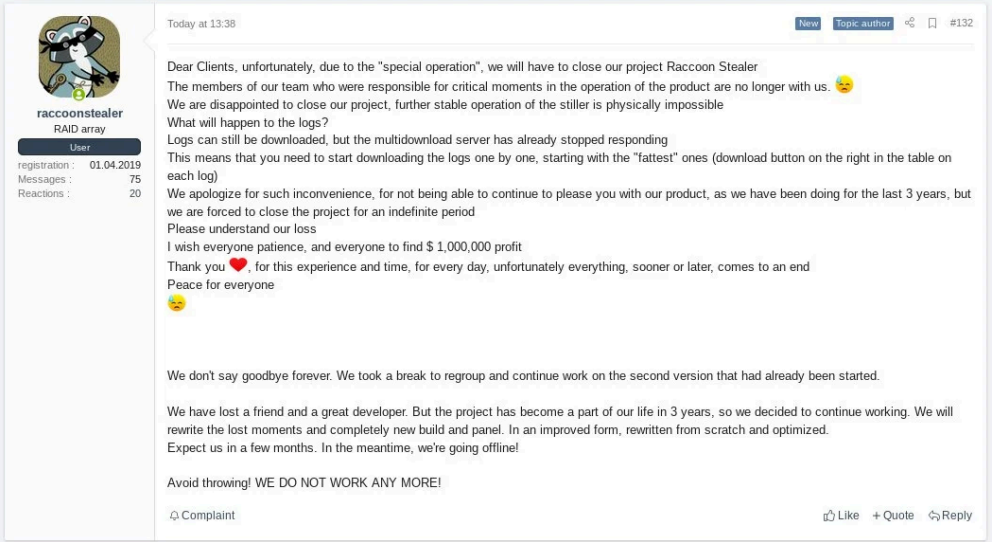
The malware is very popular among threat actors as it can steal a wide variety of information from infected devices, including stored browser credentials, browser information, cryptocurrency wallets, credit cards, email data, and other data from numerous applications.


DIE LINKE.
0:00

Raccoon Stealer operation suspended

As first spotted by security researcher 3xp0rt, the threat actors behind the Raccoon Stealer posted today to Russian-speaking hacking forums that they are suspending their operation after one of their core developers was killed in the invasion of Ukraine.

> "Dear Clients, unfortunately, due to the "special operation", we will have to close our project Raccoon Stealer.
>
> The members of our team who are responsible for critical moments in the operation of the product are no longer with us.
>
> We are disappointed to close our project, further stable operation of the stealer is physically impossible."

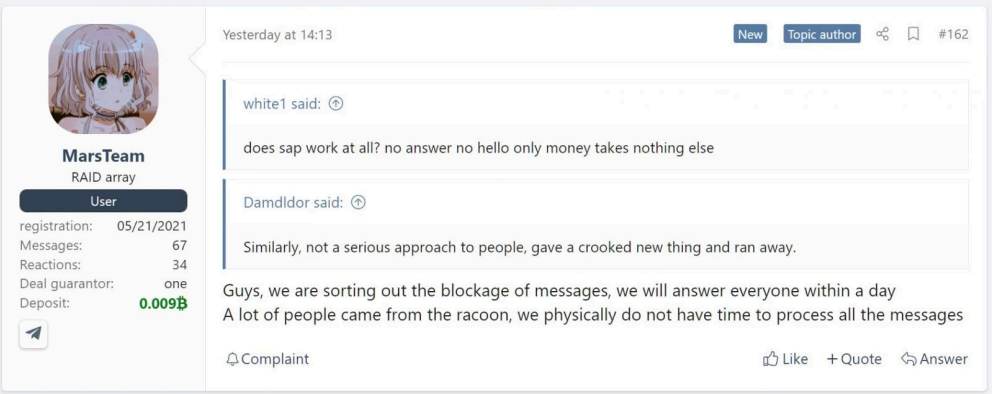


Raccoon Stealer operation suspending operations
Source: 3xp0rt

However, it does not appear that they will be gone forever, as they state that they plan to rebuild the lost components and relaunch in a few months.

With the closure of Raccoon Stealer, 3xp0rt told BleepingComputer that threat actors are now moving to the Mars Stealer operation, which offers a similar service as Raccoon.

According to a post on the Russian-speaking XSS hacking forum, the 'MarsTeam' has been overwhelmed with requests since Raccoon announced they are shutting down, making it difficult to respond to everyone.



Threat actors switching to Mars Stealer

3xp0rt says that we should expect a surge of Mars Stealer campaigns shortly, as threat actors move to the service, which operates similarly to Raccoon.

Ukraine has an active cybercrime community

The invasion of Ukraine has had a significant impact on cybercrime and the hacking underground, with many threat actors residing in the country and publicly taking sides in the war.

A representative of the now-defunct Maze ransomware operation recently released the master decryption keys for past victims on BleepingComputer's forums.

In a conversation with the Maze representative who leaked the keys, BleepingComputer was also told that he is Ukrainian and was arrested by the Ukrainian police.

The recent 'Conti Leaks' of internal chats, source code, and the doxing of TrickBot and Conti ransomware members was directly caused by the criminal operations taking sides with Russia and upsetting Ukrainian threat actors and researchers.

Law enforcement has also been very active over the past year, arresting numerous threat actors [1, 2, 3, 4, 5, 6] residing in Ukraine.
