

# Raccoon Stealer malware suspends operations due to war in Ukraine

[bleepingcomputer.com/news/security/raccoon-stealer-malware-suspends-operations-due-to-war-in-ukraine/](https://bleepingcomputer.com/news/security/raccoon-stealer-malware-suspends-operations-due-to-war-in-ukraine/)

Lawrence Abrams

By

[Lawrence Abrams](#)

- March 25, 2022
- 02:22 PM
- [0](#)



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.

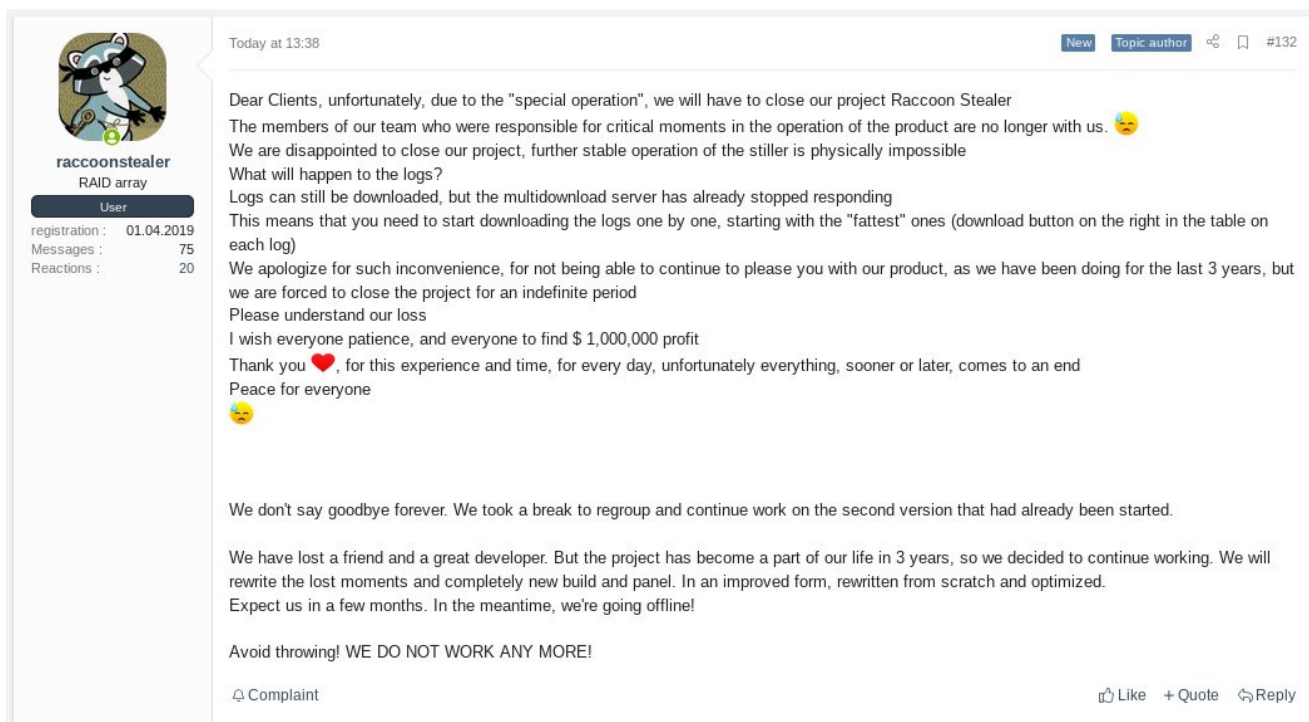
## Raccoon Stealer operation suspended

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."



The screenshot shows a forum post from the user 'raccoonstealer'. The user's profile information includes a registration date of 01.04.2019, 75 messages, and 20 reactions. The post content is as follows:

Today at 13:38

Dear Clients, unfortunately, due to the "special operation", we will have to close our project Raccoon Stealer  
The members of our team who were 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 stiller is physically impossible  
What will happen to the logs?  
Logs can still be downloaded, but the multidownload server has already stopped responding  
This means that you need to start downloading the logs one by one, starting with the "fattest" ones (download button on the right in the table on each log)  
We apologize for such inconvenience, for not being able to continue to please you with our product, as we have been doing for the last 3 years, but we are forced to close the project for an indefinite period  
Please understand our loss  
I wish everyone patience, and everyone to find \$ 1,000,000 profit  
Thank you ❤️, for this experience and time, for every day, unfortunately everything, sooner or later, comes to an end  
Peace for everyone  
😞

We don't say goodbye forever. We took a break to regroup and continue work on the second version that had already been started.

We have lost a friend and a great developer. But the project has become a part of our life in 3 years, so we decided to continue working. We will rewrite the lost moments and completely new build and panel. In an improved form, rewritten from scratch and optimized.  
Expect us in a few months. In the meantime, we're going offline!

Avoid throwing! WE DO NOT WORK ANY MORE!

Complaint Like Quote Reply

## 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.

Yesterday at 14:13 New Topic author #162

**MarsTeam**  
RAID array  
User

registration: 05/21/2021  
Messages: 67  
Reactions: 34  
Deal guarantor: one  
Deposit: 0.009\$

white1 said: ⤴  
does sap work at all? no answer no hello only money takes nothing else

Damldor said: ⤴  
Similarly, not a serious approach to people, gave a crooked new thing and ran away.

Guys, we are sorting out the blockage of messages, we will answer everyone within a day  
A lot of people came from the racoon, we physically do not have time to process all the messages

Complaint Like + Quote Answer

## 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.

### Related Articles:

Ukraine warns of “chemical attack” phishing pushing stealer malware

Eternity malware kit offers stealer, miner, worm, ransomware tools

German automakers targeted in year-long malware campaign

Phishing attacks target countries aiding Ukrainian refugees

## RIG Exploit Kit drops RedLine malware via Internet Explorer bug

### Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.