Analyzing the Impact of the Operation Endgame Takedown on Rhadamanthys & the MaaS Ecosystem

By SpyCloud Labs Research Team

Published: 2025-12-10 · Archived: 2026-04-05 22:50:44 UTC

After a coordinated disruption of the Rhadamanthys Malware-as-a-Service (MaaS) platform by law enforcement and private industry, minor activity from Rhadamanthys and its developer, KingCrete, continues. However, the takedown clearly did major damage to Rhadamanthys' operations, and it looks like most users are moving away from the infostealer in favor of competitors like Vidar infostealer, leaving just a trickle of continued Rhadamanthys activity.

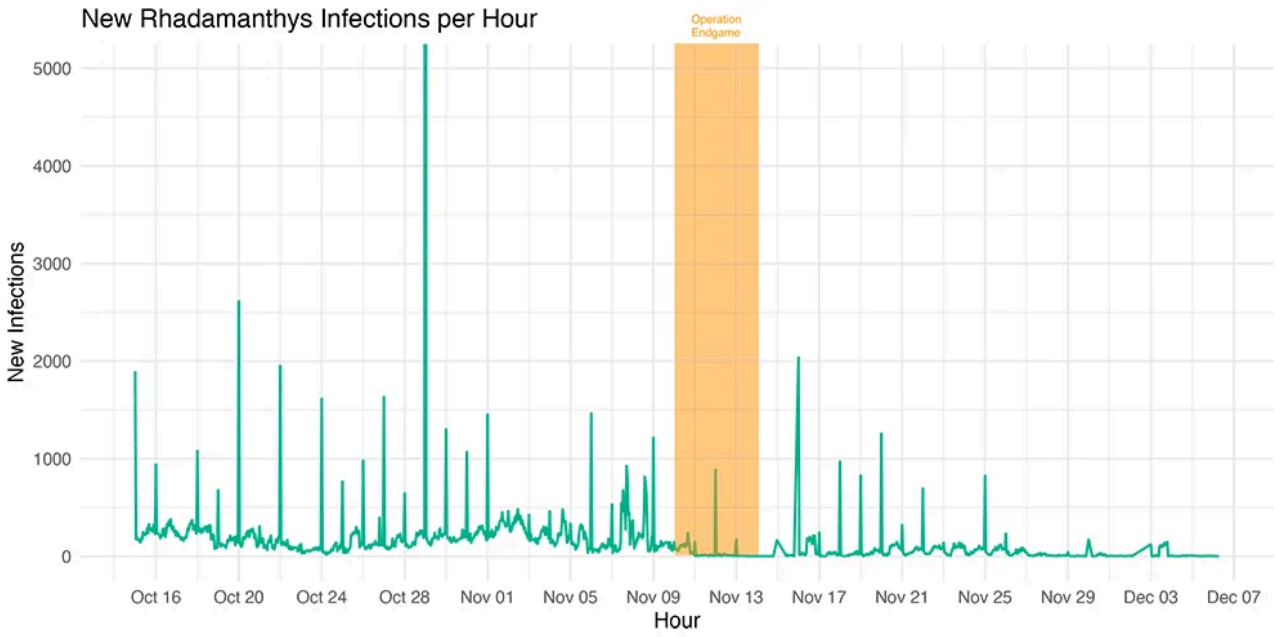
On November 10, Europol led a coordinated law enforcement action to take down the Rhadamanthys infostealer infrastructure as part of Operation Endgame. Our team at SpyCloud Labs supported this phase of Operation Endgame, which included disruptive actions for multiple different malware variants, including the Rhadamanthys infostealer, Trojan VenomRAT, and a relatively unknown proxy bot called Elysium.

The coordinated action against these MaaS variants involved 1,025 server takedowns, 20 domains seized, 11 physical locations searched, and the arrest of the main suspect for VenomRAT in Greece.

Prior to the takedown action, Rhadamanthys was one of the most popular infostealer malware variants on the market and was differentiated from other top infostealers due to the fact that it could infect users in Commonwealth of Independent States (CIS) countries.

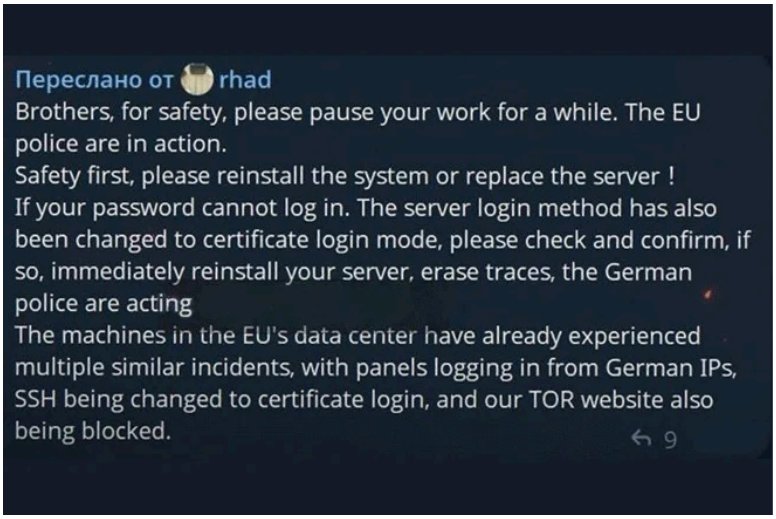
From our perspective one month later, the Rhadamanthys takedown appears to have been a relatively successful operation. Based on our dataset of millions of recaptured Rhadamanthys infostealer logs, we see a clear decline in new infostealer malware infections in the days directly following the takedown.

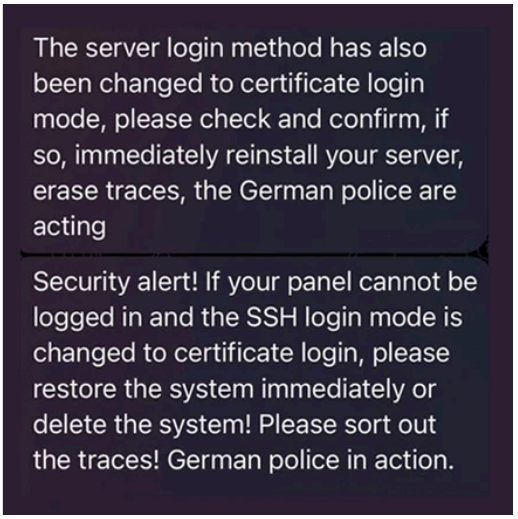
While we saw a small spike in mid-November suggesting there may have been a limited amount of Rhadamanthys activity post-takedown, that activity appears to have dropped down to practically nothing in the last couple of weeks.



New Rhadamanthys logs recaptured by SpyCloud, graphed by malware infection time.

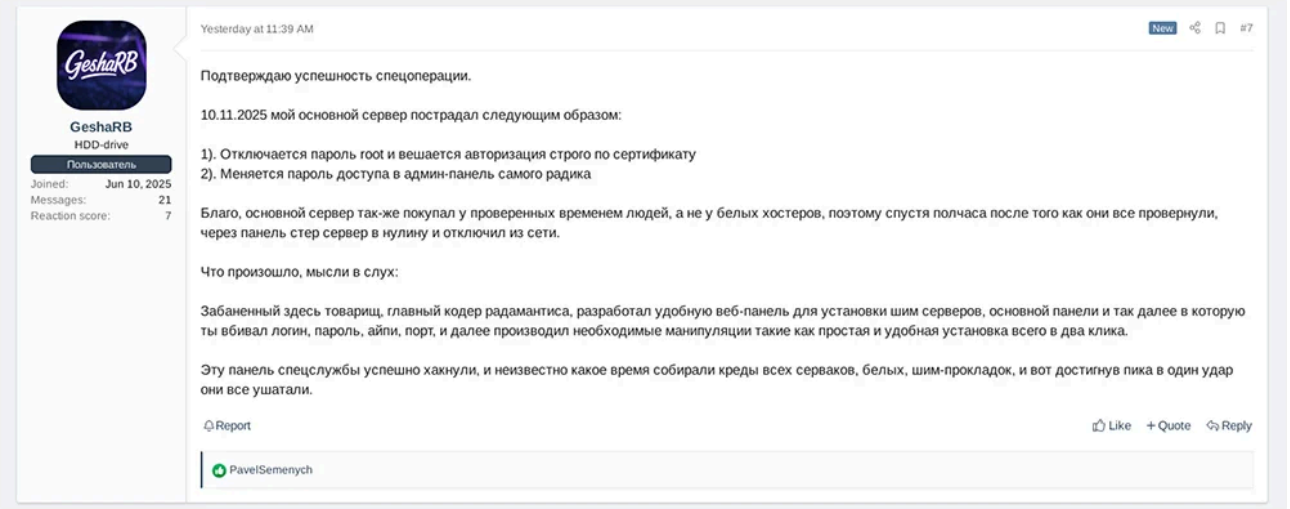
As the takedown was unfolding on November 10, researchers observed cautionary messages sent by the Rhadamanthys developer(s) to their customers. They warned Rhadamanthys users to “pause their work” and “erase traces” as there was an active law enforcement action against the malware.





Screenshots of messages from the Rhadamanthys developers to their customers about the takedown as it was in progress, shared by independent security researcher [g0njxa on X](#).

GeshaRB, an account apparently belonging to a Rhadamanthys customer, also posted a detailed account of the takedown to XSS, describing effects of the operation from their perspective as a Rhadamanthys user.



XSS post describing the Rhadamanthys takedown. This is a response to a thread on the takedown titled "operation endgame отработала по rhadamanthys".

Translation:

I confirm the success of the special operation.

On 11/10/2025 my main server was affected as follows:

1. *The root password is disabled and authorization is strictly by certificate.*
2. *The password for accessing the admin panel of Rhadamanthys itself changed.*

Luckily, I also bought the main server from reliable people, not from white hosting providers, so half an hour after they had done everything, I wiped the server from the control panel and disconnected it from the network.

What happened, thoughts out loud:

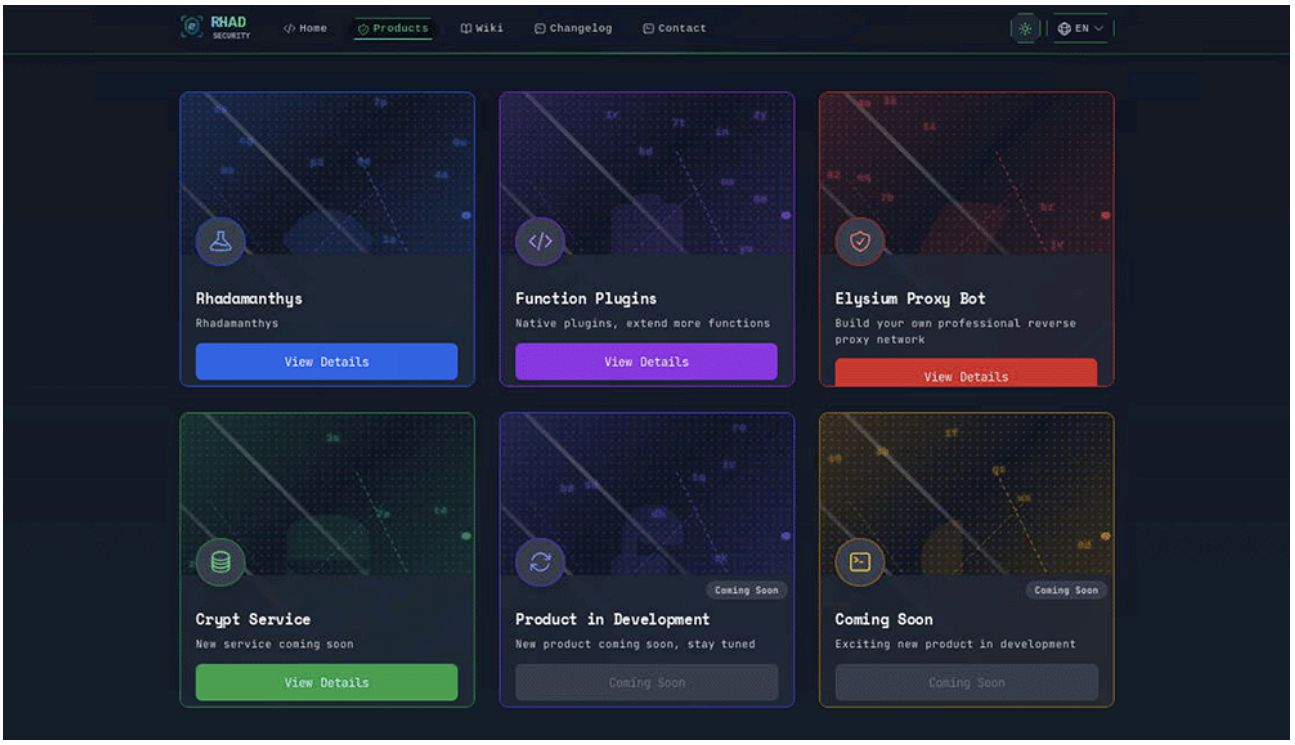
The guy banned here, the main coder of Rhadamanthys, developed a convenient web panel for installing shim servers, the main panel, and so on, into which you entered your login, password, IP, and port, and then performed the necessary manipulations, such as a simple and convenient installation in just two clicks.

The special services successfully hacked this panel, and for an unknown amount of time they collected the credentials of all the servers, white ones, and shims, and then, having reached the peak, in one blow they destroyed everything.

In his post he refers to KingCrete, the Rhadamanthys developer, as "the guy banned here". This is because KingCrete's profiles were previously banned from both the XSS and Exploit criminal hacking forums – both of which cater specifically to Russian-language threat actors – because Rhadamanthys had no built-in protections to stop it from infecting users in CIS countries.

This made Rhadamanthys something of an outlier in the space, as most MaaS is specifically designed to perform location and/or language checks to avoid executing on a device which is located in, or operated by a user from, a CIS country.

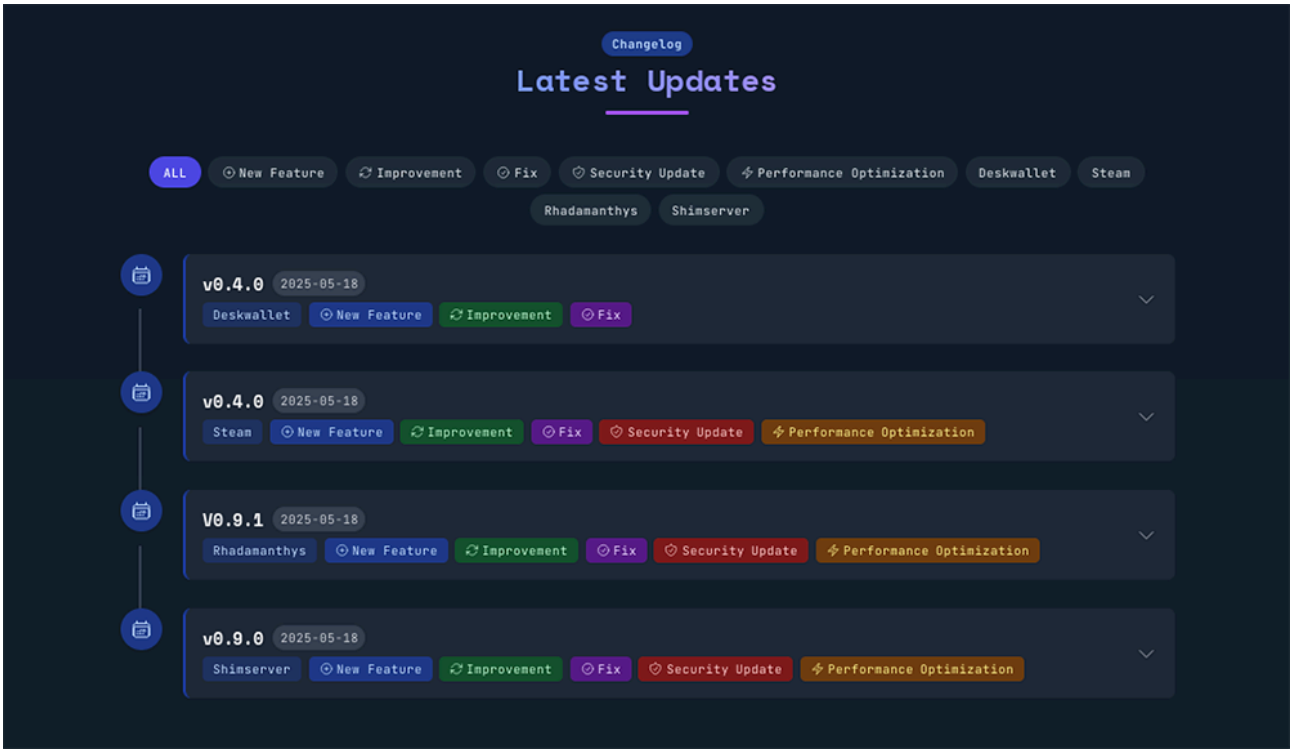
About three weeks after the takedown, KingCrete appears to have started attempting a comeback, creating some new infrastructure including reviving the “RHAD Security” .onion site where he sells Rhadamanthys and other criminal services.



RHAD Security .onion site that appears to be selling Rhadamanthys, Elysium, and a crypter service.

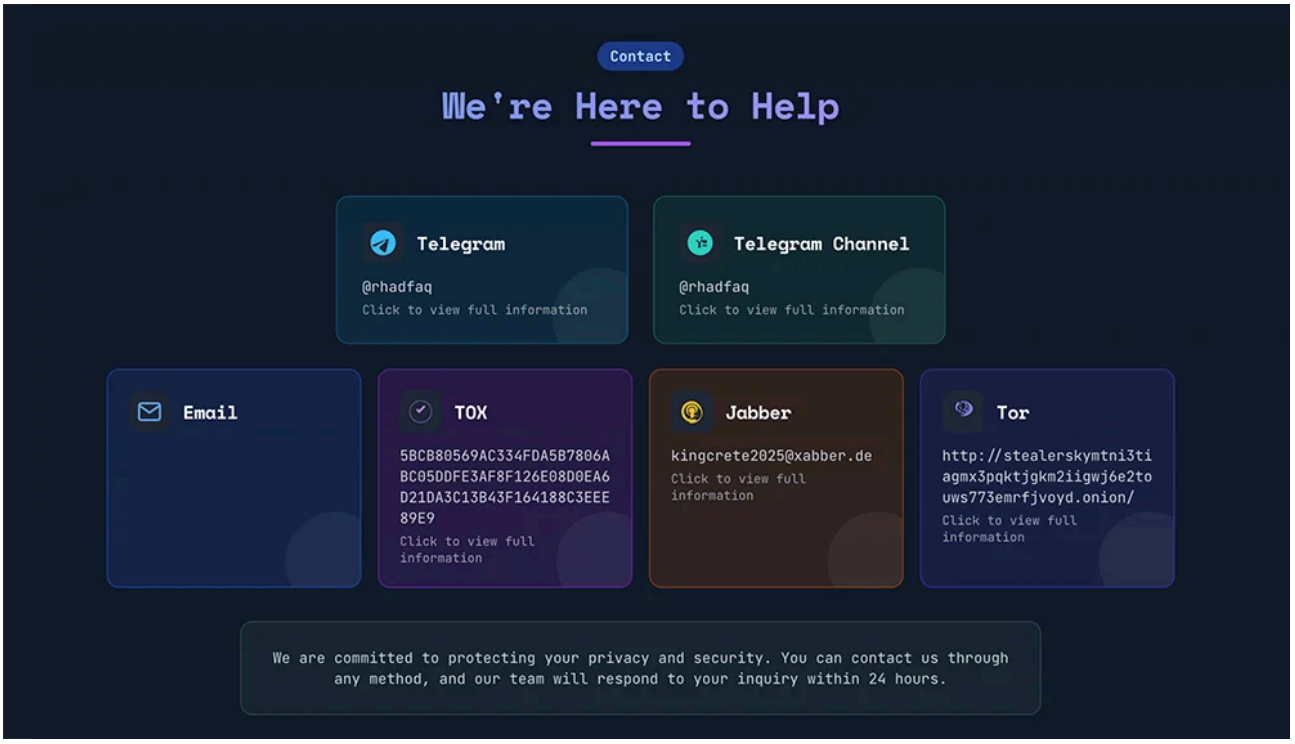
However, it will likely take more than that for him to truly return; a successful takedown is bad for business. In this case, customers lost all of their data – and likely their confidence in KingCrete as well. That trust eroded even further when law enforcement alleged that he had been stealing data from his own customers and keeping the most valuable, easily monetizable information for himself.

According to the changelog on the RHAD Security site, no new updates have been published for Rhadamanthys since May. This might indicate to potential customers that KingCrete hasn’t made any significant changes to his operation since the takedown – potentially leaving the same security gaps open that allowed law enforcement to gain access to the infostealer infrastructure during Operation Endgame.

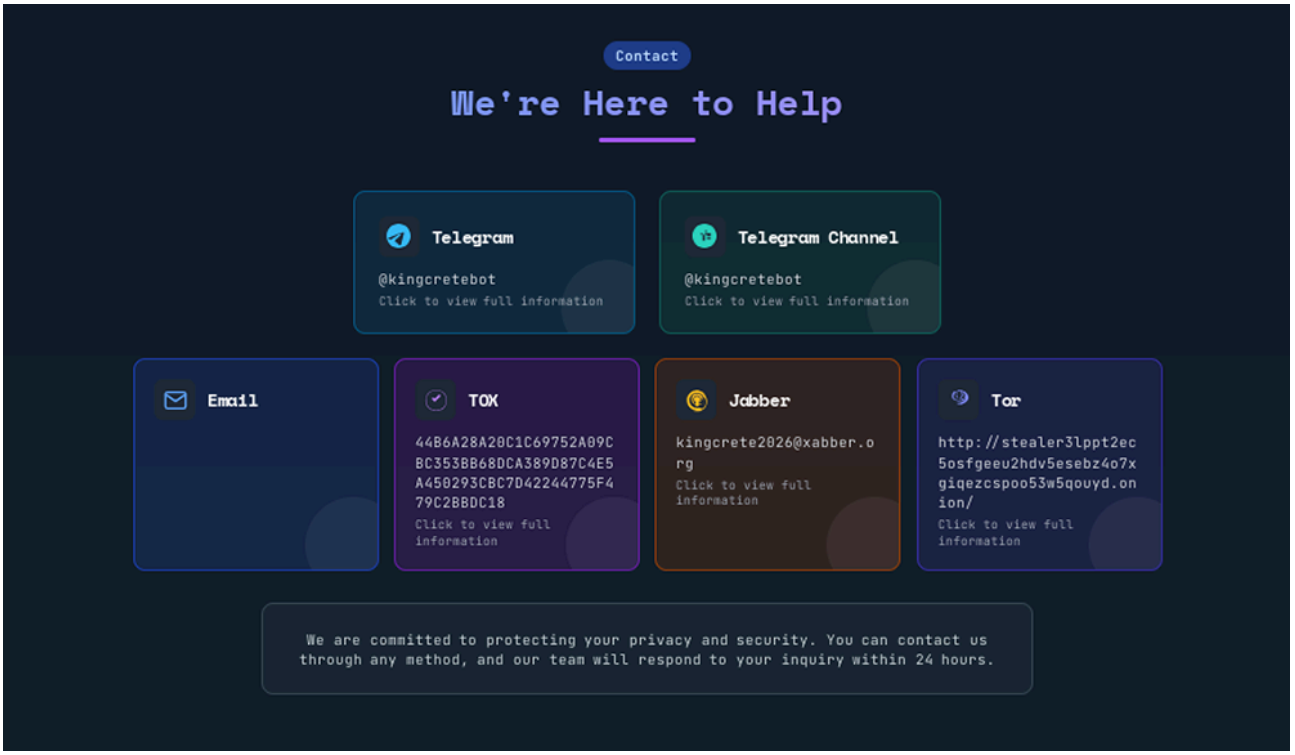


Changelog on the RHAD Security .onion site showing that no new Rhadamanthys updates have been published since May 2025.

Furthermore, criminals have no guarantee that this revived infrastructure is really KingCrete – when cybercriminal infrastructure comes back after a successful law enforcement operation there are often swirling rumors that the revived infrastructure is either a copycat or a law enforcement operated honeypot. This new RHAD Security website is nearly identical to the old site except for one key component – all of the contact information at the bottom has been updated to totally new accounts.



Contact information section of the RHAD Security website captured prior to Operation Endgame.



Contact information section of the RHAD Security website captured in December 2025, after Operation Endgame.

After the takedown of the Redline and META infostealers during Operation Magnus last October, SpyCloud researchers observed an explosion of LummaC2 infections. Our hypothesis was then, and remains, that – following a successful disruption of a MaaS family – a segment of the user base quickly transitions to the next most capable infostealer.

Following the Rhadamanthys takedown, we at SpyCloud Labs debated whether users of Rhadamanthys would move to StealC, Vidar, or back to LummaC2 (unlikely given the apparent disdain of the latter following a significant doxxing campaign against its developers).

Now that we have more data from after the Rhadamanthys takedown, we can see that Vidar seems to be emerging as the preferred MaaS platform of choice. We have observed an already-existing surge of Vidar infections that began around the middle of September continuing to rise following the Rhadamanthys disruption.

New infections per day for the five top malware variants throughout 2025, to date.

While it is clear that the disruption of Rhadamanthys did not unilaterally destroy the entire ecosystem – and to be clear, no one thought it would – it *is* apparent that the takedown, helped by the prior self-immolation of LummaC2, has had a distinct impact on the total number of new infostealer infections.

SpyCloud recaptures malware-stolen data and enables your team to remediate exposures before cybercriminals can launch follow-on attacks.

Source: https://spycloud.com/blog/impact-operation-endgame-takedown-on-rhadamanthys-stealer/