Lumma Infostealer – Down but Not Out?

By rohann@checkpoint.com

Published: 2025-05-29 · Archived: 2026-04-23 02:11:20 UTC

Key Findings:

- The takedown achieved a significant disruption to Lumma infostealers' infrastructure, but likely didn't permanently affect most of its Russia-hosted infrastructure.
- Lumma's developers are undertaking significant efforts to reinstate the activity and to conduct business as usual.
- There seems to be a significant reputational damage to the Lumma infostealer, and the key factor for the infostealer to resume regular activity will be the reputational factors (rather than the technological).

On May 21, 2025, Europol, FBI, and Microsoft, in collaboration with other public and private sector partners, announced an operation to dismantle the activity of the Lumma infostealer. The malware, considered to be one of the most prolific infostealers, is distributed through a malware-as-a-service model. In addition to its use by common cyber criminals for stealing credentials, Lumma was observed to be part of the arsenal of several prominent threat actor groups, including Scattered Spider, Angry Likho, and CoralRaider.

The Takedown on the Dark Web

According to the reports, the takedown operation began on May 15. On that day, Lumma customers flooded dark web forums that advertise the stealer, complaining they were unable to access the malware's command and control (C2) servers and management dashboards.

Figure 1 – Threat actor complaints about server access.

The Lumma developer publicly responded on Friday, May 23. He confirmed that almost 2,500 of Lumma's domains were confiscated/taken down by law enforcement agencies.

According to Lumma's developer, the agencies were not able to seize Lumma's main server due to its geographic location. However, they successfully infiltrated it by exploiting an unknown vulnerability in Integrated Dell Remote Access Controller (iDRAC). This allowed them to wipe the server and its backups. While the developer did not log his customers' IP addresses, the law enforcement agencies created a phishing login page to the harvest credentials and digital footprints of Lumma customers. They also planted a JavaScript snippet that tried to access the customers' web cameras.

Figure 2 – The developer’s response to the operation.

Figure 3 – JavaScript script planted on the Lumma dashboard server.

The Future of Lumma

On cyber crime forums, opinions regarding the future of the Lumma infostealer are mixed. Some believe the damage done by the operation will lead to the shutdown of Lumma services or at least make them go private, i.e. ending public advertisement, and returning to word-of-mouth for marketing and vetting customers. Others believe that the takedown operation won’t have any long-lasting effect.

Figure 4 – Threat actors respond to the Lumma servers shutdown.

Lumma's developers already claim to be operational once more. Several cyber criminals published their Telegram conversations in which the developer claimed that no one related to Lumma was arrested and that "everything has been restored, and we are working normally."

Figure 5 – Threat actors sharing chats with the Lumma developer.

Figure 5.2 – Threat actors sharing chats with the Lumma developer.

In addition, a closer look at the malware's infrastructure reveals that the C2 servers registered in Russia were not disabled.

Figure 6 – Online Russian-language Lumma panels after the operation.

Figure 6.2 – Online Russian-language Lumma panels after the operation.

In another sign that the Lumma infostealer is down but not out, information stolen from compromised computers continues to appear on the online market. For example, two days after the operation, an automated Telegram bot that sells stolen credentials obtained by Lumma offered 95 logs from 41 countries for sale. As of May 29, the same bot contains 406 logs, showing a steady increase.

Figure 7 – Stolen logs for sale.

In addition, a centralized shop for the Russian market that sells infostealer logs online contains data from Lumma-infected computers after the takedown operation date.

Figure 8 – Lumma logs for sale on the Russian Market.

As seen in Operation Cronos, which took down LockBit ransomware, law enforcement battling cyber crime often utilize psychological pressure against threat actors to sow distrust among them. The authorities compromised LockBit's leak site and planted a countdown timer teasing disclosing the identity of LockBit's leader.

In the operation against Lumma, law enforcement published messages on Lumma's main Telegram channel, claiming that the admins and affiliates were already sharing information with them. The JavaScript snippet that was planted in the hijacked panels, which allegedly took photos with users' webcams, can also be viewed as a psychological trick. After close inspection of the JavaScript code, threat actors claim that the code is very basic and would not execute properly.

Figure 9 – FBI message shared in the Lumma Telegram group.

Figure 10 – Threat actors responding to claims that admins shared information about Lumma.

Figure 11 – Threat actors discussing the JavaScript snippet.

Summary

Despite the successful takedown operation against the Lumma infostealer, Check Point Research observed significant efforts by the Lumma developer to fully reinstate its infostealer activities and conduct business as usual. Beyond the damage to Lumma's technical capabilities, the real question is how much damage was sustained in terms of Lumma's brand and reputation. Law enforcement agencies' attempts to sow distrust among Lumma's affiliates and customers may not be as easily overcome, as was observed in previous cases.

Source: https://blog.checkpoint.com/security/lumma-infostealer-down-but-not-out/