Russia-linked Vermin hackers target Ukrainian military in new espionage campaign

By Daryna Antoniuk

Published: 2024-06-07 · Archived: 2026-04-02 12:01:32 UTC

A pro-Russian hacker group known as Vermin has resurfaced after two years of inactivity to target Ukraine's military in a new espionage operation, according to a recent report.

The group is reportedly controlled by the law enforcement of the so-called Luhansk People's Republic (LPR), an unrecognized quasi-state located in eastern Ukraine which was annexed by Russia in 2022. Vermin hackers are believed to be acting on behalf of the Kremlin.

In their latest campaign, analyzed by Ukraine's computer emergency response team (CERT-UA), the group targeted Ukraine's military with the goal of stealing sensitive information from devices.

To conduct this operation, Vermin used a previously known malware called Spectr and legitimate file-syncing software called SyncThing. The hackers delivered the tools to victims' computers through phishing emails containing malicious archives protected by passwords.

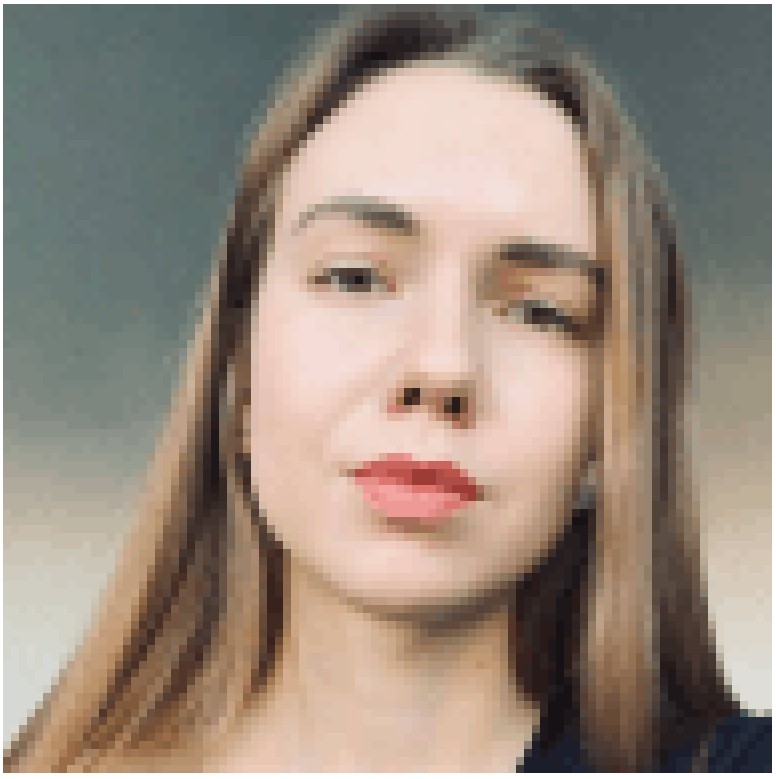
Spectr is a flexible and adaptable malware that can take screenshots of a victim's screen every 10 seconds, copy files with certain extensions, and steal authentication data from messengers, including Telegram, Signal, and Skype. It can also steal information from internet browsers like Firefox, Edge and Chrome, including authentication and session data, as well as browsing history.

In March 2022, CERT-UA warned that Vermin had used Spectr to target Ukrainian government infrastructure.

SyncThing was used in the new campaign to exfiltrate stolen documents, files, passwords, and other information from victims' computers to Vermin's servers, researchers said. The hackers often deploy legitimate tools during their attacks to avoid detection.

Earlier this week, cybersecurity firm Cyble reported that Ukraine's Ministry of Defence and a military base were attacked by Belarusian state-sponsored hackers known as Ghostwriter.

On Tuesday, CERT-UA warned about cyberattacks against Ukrainian military personnel and defense services using DarkCrystal malware, which could allow attackers to gain remote access to a victim's device.



Daryna Antoniuk

is a reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been published at Sifted, The Kyiv Independent and The Kyiv Post.
