Russia-backed hacker group Gamaredon attacking Ukraine with info-stealing malware

By Daryna Antoniuk

Published: 2023-02-06 · Archived: 2026-04-05 20:24:07 UTC

The Russian-sponsored hacker group known as Gamaredon continues to attack Ukrainian organizations and remains one of the “key cyber threats” for Ukraine’s cyberspace, according to a report the Ukrainian government published Wednesday.

Ukraine claims that Gamaredon operates from the city of Sevastopol in Russia-occupied Crimea, but acts on orders from the FSB Center for Information Security in Moscow. The group began operations in June 2013, just months before Russia forcibly annexed the Crimean Peninsula from Ukraine.

In its recent campaigns against Ukraine, Gamaredon used variants of PowerShell info-stealer malware known as GammaLoad and GammaSteel.

These are custom-made information stealer implants that can exfiltrate files of specific extensions, steal user credentials and take screenshots of the victim’s computer, according to Ukraine’s State Cyber Protection Centre.

The two malware variants are not new and have been used previously by Gamaredon hackers to target Ukraine’s security and government services.

To gain initial access to the victim’s network, hackers use phishing emails. These emails contain malicious LNK files distributed in RAR archives. Only users with Ukrainian IP addresses can open these files.

Hackers send the phishing emails from domains associated with legitimate organizations, such as the Security Service of Ukraine, according to the report.

Gamaredon's most popular targets include government organizations, critical infrastructure facilities, and Ukraine’s defense, security, and law enforcement agencies. The names of the enclosed malicious files are usually associated with the war in Ukraine.

Gamaredon's recent activity is characterized by the multi-stage deployment of malware payloads used to maintain persistence. These payloads represent similar variants of the same malware, each designed to behave in much the same way as the others.

According to the report, Gamaredon hackers have evolved throughout the war, improving their tactics and redeveloping used malware variants to stay undetected.

Ukraine’s computer emergency response team, CERT-UA, told The Record that Gamaredon is responsible for the largest number of cyberattacks on Ukraine. “Not a week goes by that we didn’t detect some new mass phishing email campaign with Gamaredon malware,” a CERT-UA spokesperson said.

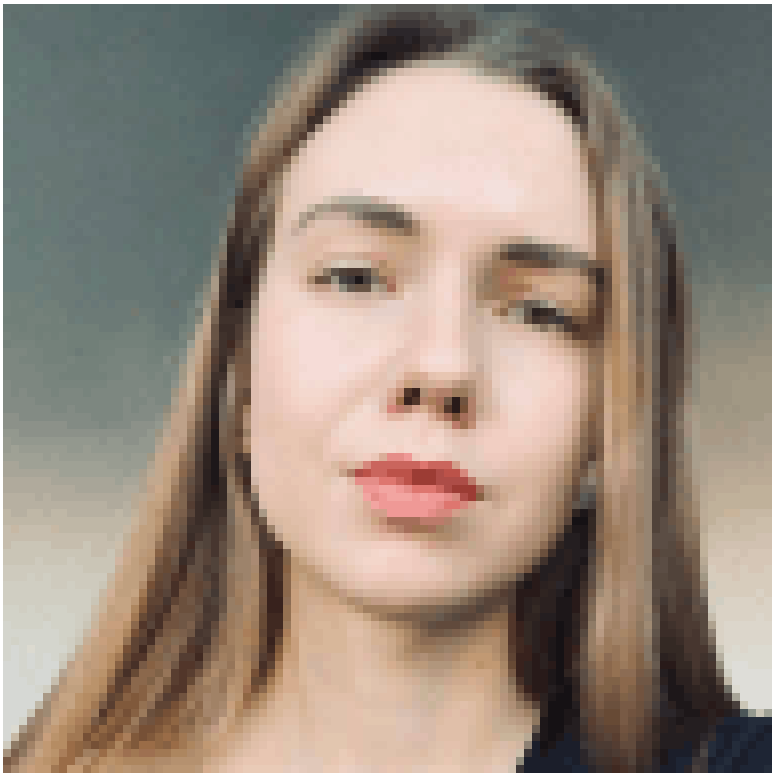
In 2022, Ukraine registered more than 70 incidents related to the group, the agency said.

Gamaredon also attacks Ukraine's allies. In late January, Latvia confirmed a phishing attack on its Ministry of Defense, linking it to the group.

Ukrainian cybersecurity officials described their attacks as intrusive and audacious, and said the group's main purpose was "to conduct targeted cyberintelligence operations."

No previous article

No new articles



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.
