RedCurl hackers return to spy on 'major Russian bank,' Australian company

By Daryna Antoniuk

Published: 2023-07-17 · Archived: 2026-04-05 13:52:57 UTC

The Russian-speaking hacking group RedCurl attacked a “major Russian bank” and an unidentified Australian company earlier this year to steal corporate secrets, according to recent research.

The incidents were the latest in a string of at least 34 attacks in the last four years, according to a report published on Monday by Russia-based company F.A.C.C.T., an offshoot of cybersecurity firm Group-IB.

RedCurl has been conducting commercial espionage since at least 2018, targeting a wide range of organizations including construction, finance, consulting firms, retailers, banks, insurance companies, and legal entities.

About half of the attacks have been aimed at victims in Russia, while the other half targeted organizations in Ukraine, Canada, and Europe, F.A.C.C.T. said.

The group does not encrypt the data of its victims and does not demand a ransom. It hunts for documents with commercial secrets and personal data of employees, and tries to get them “as discreetly as possible," the researchers said.

RedCurl made two attempts to attack the undisclosed Russian bank. During the first attempt in November 2022, they used phishing emails but failed, F.A.C.C.T. said. However, in May of this year, the group successfully targeted one of the bank's contractors to gain access to the victim's infrastructure. In June, RedCurl used the same tactics and tools in the attack on the Australian company.

Tools and strategy

The group mostly makes its own tools or modifies existing malware, the researchers said.

In both recent attacks, the tool was called RedCurl.SimpleDownloader, which is currently still being developed, F.A.A.C.T. said.

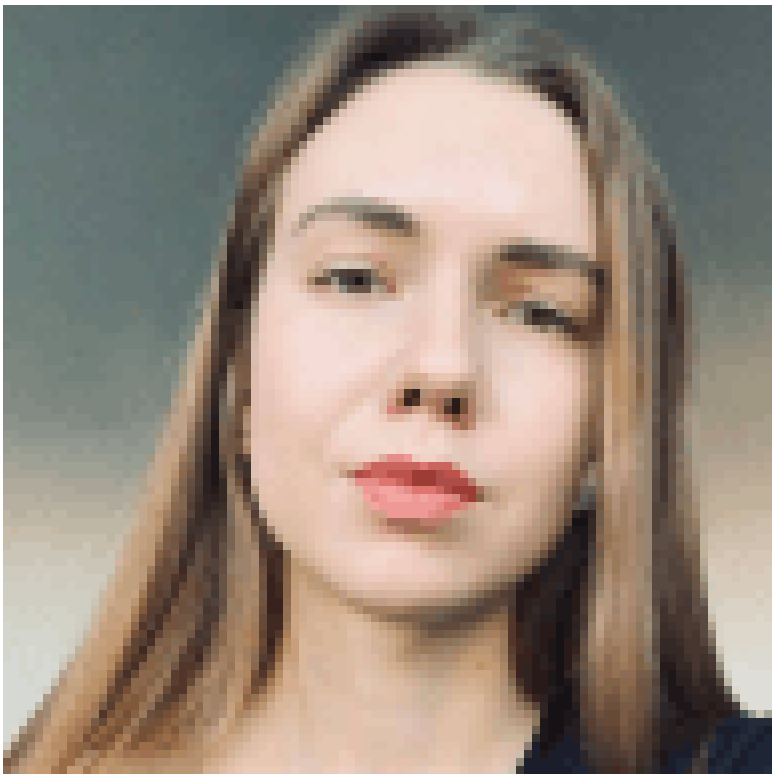
When targeting Russian organizations, the hackers employed the initial version of this tool, which lacked any protection against analysis and detection. However, the version employed in the attack on the Australian company includes new protective features, such as string encryption using an algorithm.

“RedCurl is constantly evolving, refining both their techniques and tools,” F.A.C.C.T. said.

The group's hackers can stay undetected for long periods, between two and six months, before stealing corporate data, the researchers said, and the attacks can include a long and complex infection chain.

It is still not clear who is behind this campaign and what their motives are, F.A.C.C.T. said.

“RedCurl remains one of the most interesting Russian-language cybercrime groups, especially the uncommon targeting of both Russian and non-Russian entities,” Russian cyber analyst Ian Litschko wrote on Twitter.



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.
