Remcos, again: Ukrainian agencies targeted in a new spying campaign

By Daryna Antoniuk

Published: 2023-11-17 · Archived: 2026-04-05 23:08:34 UTC

A hacking group that has been targeting Ukraine for a while has launched a new campaign on government agencies using a familiar surveillance tool — Remcos.

The sophisticated remote access software, marketed as a legitimate administrative tool, can be abused by hackers to gain full control over an infected system.

In a recent campaign, hackers sent phishing letters to their targets, disguising them as official requests from Ukraine's security service (SBU), according to research by the country's computer emergencies response team (CERT-UA).

In an email, the hackers asked victims to provide certain information, claiming it was crucial for "national security." The malicious letter warned that if recipients did not provide information within the specified period, they would be held liable.

The requested information was allegedly listed in an attached PDF file, which, in reality, installed Remcos on the targeted device.

CERT-UA tracks the threat actor behind this campaign as UAC-0050. The agency's spokesperson told Recorded Future News that this group has been active since at least 2020, attacking government agencies not only in Ukraine but also in the Baltic states and Russia. The group wasn't very active this year, according to CERT-UA.

In February, the group attacked Ukrainian state agencies with Remcos twice. In one instance, the hackers sent phishing letters to their victims, disguising them as official requests from the Kyiv court.

Earlier that month, the group sent its victims fake emails containing a malicious file, posing as reminders to pay for services from Ukrtelecom, a major Ukrainian internet service provider.

CERT-UA's new report didn't specify the goal of the recent campaign, but the agency's spokesperson said that it was most likely an espionage campaign.

Although researchers didn't directly attribute the attacks to Russia, they noted that the domain names used by the hackers were registered via the Russian company REG.RU.

'Highly customizable'

Remcos was developed by the Germany-based firm Breaking Security for remotely managing Windows systems, according to research from cybersecurity firm Trend Micro.

Breaking Security openly advertises Remcos, describing it as “a lightweight, fast, and highly customizable remote administration tool with a wide array of functionalities.” Users can download the free version of the software or buy the premium version for $85.

In addition to providing remote access, Remcos can also collect data from targeted devices, including computer information such as name, system type and processor revision number, as well as user credentials and personal information.

Remcos can bypass antivirus protection by running as a legitimate process on Windows and gain admin privileges to disable user account control.

The software is usually embedded in a malicious ZIP file masquerading as a PDF that claims to contain an invoice or order, according to cybersecurity company Check Point.

In one attack last year, threat actors disguised a phishing email as a payment notification from a trusted bank and asked the recipient to open the attached Excel file, according to Fortinet research.

This Excel file displayed a yellow security bar warning the victim about dangerous macro code. The file message lured the victim into clicking the button to bypass the warning and execute the malicious macro code, Fortinet explains.

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.
