Remcos software deployed in spying attempt on Ukraine's government, CERT says

By Daryna Antoniuk

Published: 2023-02-10 · Archived: 2026-04-05 14:59:09 UTC

In a recent phishing campaign against Ukrainian government agencies, hackers attempted to install Remcos surveillance software on victims' computers, according to a recent alert.

Remcos is a legitimate remote management software for Windows systems developed by the German firm Breaking Security. However, it is sometimes used by hackers to gain remote access and complete control over victims' computers.

The bogus emails contained a malicious file reminding recipients to pay for services from Ukrtelecom, a major Ukrainian internet service provider, according to an alert issued Monday by Ukraine's computer emergency response team (CERT-UA).

One of the archives attached to the email contained an executable file of more than 600MB in size. Running this file installed the Remcos program on the victim's computer.

CERT-UA did not disclose which Ukrainian government services were targeted by phishing emails or whether hackers managed to successfully install the spyware. The agency pinned the effort on a group labeled UAC-0050 that has been active in Ukraine since 2020. The hackers carried out previous attacks using remote desktop software Remote Utilities, CERT-UA said.

A possible goal of the group is espionage, according to CERT-UA, as its members mostly targeted Ukraine's government services.

Familiar in phishing

Breaking Security openly advertises Remcos on its website, 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 €58 ($62).

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

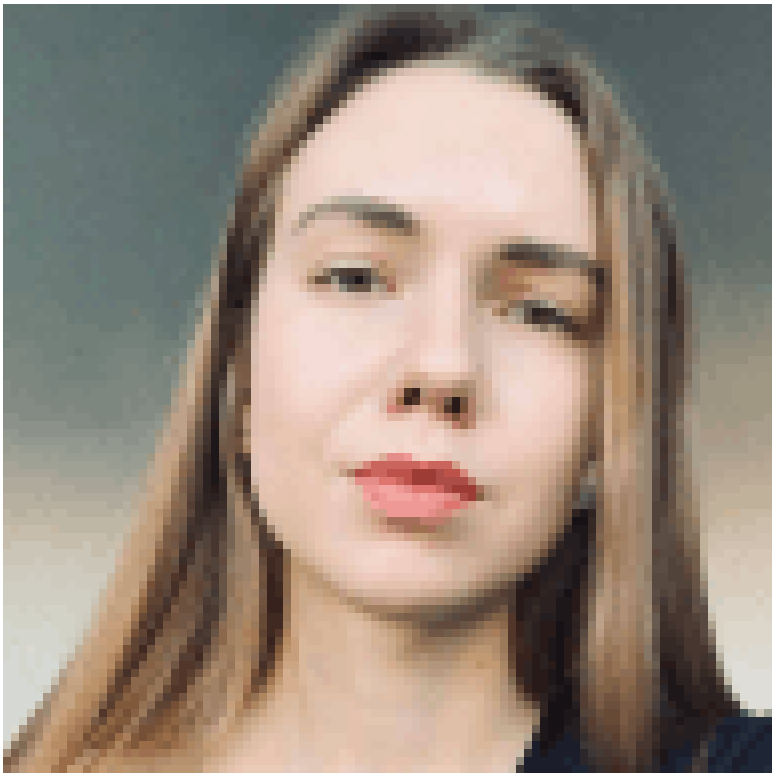
In one attack last year, threat actors disguised a phishing email as a payment notification from a trusted bank and asked the recipient to open the attached Excel file, according to Fortinet research.

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.

With Remcos software, hackers can steal user credentials, gain control over online accounts and deploy additional malware variants on an infected computer, researchers said.

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.
