Russian researchers say espionage operation using WinRAR bug is linked to Ukraine

By Daryna Antoniuk

Published: 2024-03-28 · Archived: 2026-04-05 17:02:10 UTC

Russian security researchers said they have discovered a new cyber-espionage group with links to Ukraine that has been operating since at least January of this year.

They named the group PhantomCore and labeled the attackers' previously undescribed remote access malware as PhantomRAT.

During the attacks on unnamed Russian companies, the hackers exploited a known vulnerability in the Windows file archiver tool WinRAR, according to the Moscow-based cybersecurity company F.A.C.C.T.

Identified as CVE-2023-38831, the bug was previously exploited by state-controlled hackers connected to Russia and China in early 2023 before being patched.

The tactics used by PhantomCore differed from previous attacks exploiting this vulnerability, according to F.A.C.C.T. For example, the hackers executed malicious code through the exploitation of a specially crafted RAR archive, instead of a ZIP file as previously observed, the researchers said.

To deliver PhantomRAT into victims' systems, the hackers used phishing emails containing a PDF file disguised as a contract, along with an attached RAR archive protected by a password sent within the email. PDF files are a common lure in cyberespionage campaigns.

An executable file in the archive only launched when the PDF file was opened by a user with a WinRAR version earlier than 6.23.

During the final stages of the attack, the vulnerable systems were infected with PhantomRAT, which is capable of downloading files from a command and control (C2) server and uploading files from a compromised host to the hackers' controlled server, the researchers said.

The information that hackers could obtain during the campaign included the host name, user name, local IP address, and version of the operating system. Typically, this information can help hackers conduct further attacks.

During the analysis, the researchers also found three test samples of PhantomRAT, which, according to F.A.C.C.T., were uploaded from Ukraine.

"We can state with a moderate level of confidence that the attackers conducting these attacks may be located within the territory of Ukraine," researchers said.

Independent review

The attribution of PhantomCore's campaign to Ukraine couldn't be verified. Given that the majority of Western cyber companies left Russia when it invaded Ukraine, they have limited visibility inside Russian networks. Recorded Future News asked several companies to review F.A.C.C.T.'s research.

Researchers at Check Point said they looked into the report and the vulnerability in question, and can confirm that the malware is operational as described.

All systems running WinRAR versions earlier than 6.23 are vulnerable, Check Point said. However, the researchers noted that the specific sample inside the archive is designed only for 64-bit systems — processing power typically found in newer Windows machines. It is possible that in other attacks, the payload could be different, potentially affecting both 32-bit and 64-bit systems if desired by the attacker, Check Point said.

Microsoft's director of threat intelligence strategy, Sherrod DeGrippo, said that the company has not previously observed the specific activity that F.A.C.C.T. has attributed to this group.

However, Microsoft and other companies are familiar with the widespread exploitation of CVE-2023-38831, including by cybercriminals and state-sponsored actors.

For example, Group-IB initially identified the vulnerability after it was abused by unknown cybercriminals targeting traders. Google then reported on Russia-linked attackers exploiting it while targeting the energy sector using malicious ZIP files containing a commercially available infostealer. Google also observed another Russian state-backed group exploiting the vulnerability against users in Ukraine, DeGrippo said.

DeGrippo also disputed one of F.A.C.C.T.'s assertions about how PhantomRAT is delivered.

"Regarding PhantomCore's use of RAR archives instead of ZIP files in the threat actor's attack chain, this technique has been previously observed," DeGrippo added. For example, the group Microsoft tracks as Forest Blizzard targeted organizations globally using lures in a RAR archive exploiting the CVE-2023-38831 vulnerability.

Researchers at Cloud Security Alliance have also observed threat actors tracked as DarkPink using RAR archive files.

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.
