Russia, Moldova targeted by obscure hacking group in new cyberespionage campaign

By Daryna Antoniuk

Published: 2024-07-30 · Archived: 2026-04-06 02:52:26 UTC

A cyberespionage group known as XDSpy recently targeted victims in Russia and Moldova with a new malware variant, researchers have found.

In a campaign earlier this month, the suspected nation state-linked group sent phishing emails to targets in Russia, including a tech company that develops software for cash registers, as well as to an unidentified organization in Transnistria, the Russian-controlled breakaway region in Moldova.

The malicious emails, discovered by Russian cybersecurity firm F.A.C.C.T., contained a link to an archive with a legitimate executable file, which allowed attackers to run malicious code without raising suspicion.

During these attacks, the hackers used a previously unknown tool, which the researchers called XDSpy.DSDownloader. F.A.C.C.T. didn’t disclose whether the hackers managed to penetrate the victims’ systems and steal data.

XDSpy is believed to be a state-controlled threat actor, active since 2011, that primarily attacks countries in Eastern Europe and the Balkans. Despite the group's long history, researchers have been unable to identify the country backing it.

Most of XDSpy's targets are related to the military, finance, energy, research and mining industries in Russia, according to F.A.C.C.T.

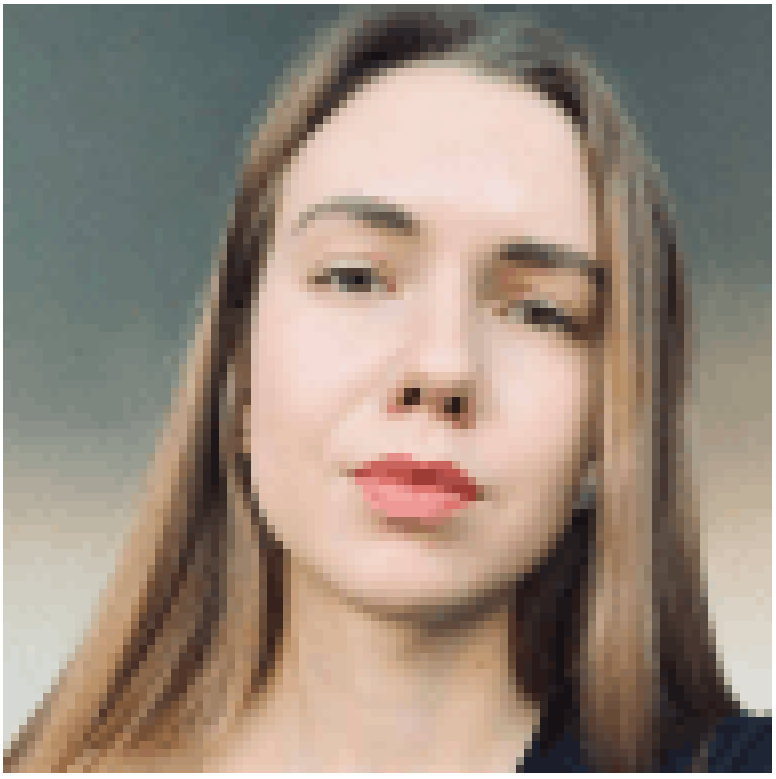
Earlier in December, the group targeted a Russian metallurgical enterprise and a research institute involved in the development and production of guided missile weapons. In an attack last July, the hackers sent phishing letters with malicious PDF attachments to an unnamed but “well-known” research institute.

XDSpy doesn’t operate a particularly sophisticated toolkit, but “they have very decent operational security,” researchers at cybersecurity firm ESET told Recorded Future News in a previous interview.

“They are putting quite a lot of effort into the obfuscation of their implants in order to try to evade security solutions. As such, it is likely they have a decent percentage of success, even if we have been able to track their operations in the long run,” ESET 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.
