XDSpy hackers attack military-industrial companies in Russia

By Daryna Antoniuk

Published: 2023-12-01 · Archived: 2026-04-05 21:46:28 UTC

A cyberespionage group known as XDSpy recently targeted Russian military-industrial enterprises, according to new research.

XDSpy is believed to be a state-controlled threat actor, active since 2011, that primarily attacks countries in Eastern Europe and the Balkans. In its latest campaign in November, hackers attempted to gain access to the systems of a Russian metallurgical enterprise and a research institute involved in the development and production of guided missile weapons, according to Russian cybersecurity firm F.A.C.C.T.

In a report published earlier this week, F.A.C.C.T. — an offshoot of Singapore-based cybersecurity firm Group IB — said that hackers sent phishing emails to their victims, masquerading as a research institute specializing in the design of nuclear weapons.

The group's tactics mirrored their previous attack on Russian companies, including a well-known research institute in July. During that incident, the hackers posed as Russia's Ministry of Emergency Situations, sending phishing letters containing malicious PDF attachments. Researchers didn't disclose whether the hackers managed to penetrate the victims' systems and steal data.

F.A.C.C.T. claimed that Russia is the primary target of XDSpy hackers. The group has previously targeted the country's government, military, and financial institutions, along with energy, research, and mining companies, researchers said.

Although the group has been active for years, there is limited evidence of its attacks on Russia, especially since many foreign cybersecurity firms exited the country following its invasion of Ukraine.

Slovak-based cybersecurity firm ESET has monitored XDSpy's activity since 2020 and researcher Matthieu Faou told Recorded Future News that the group has consistently conducted spearphishing campaigns that mainly target strategic organizations in Eastern Europe.

After exiting Russia and Belarus — both targets of XDSpy — ESET lost first-hand visibility into cyberattacks occurring in these countries. However, last week, the company said it detected the group's attack on a Ukrainian aerospace company.

In this attack, which was not publicly reported by Ukrainian security agencies and was likely unsuccessful, hackers used a compromise chain almost identical to the one described by F.A.C.C.T. "We do agree with their analysis and also attribute this to XDSpy," Faou said.

Despite the group's long history, researchers have been unable to identify the country backing it. XDSpy doesn't operate a particularly sophisticated toolkit, but "they have a very decent operational security," according to Faou. "So far, we haven't found any mistake that could point toward a specific country."

"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," he added.

Cyberttacks on Russia

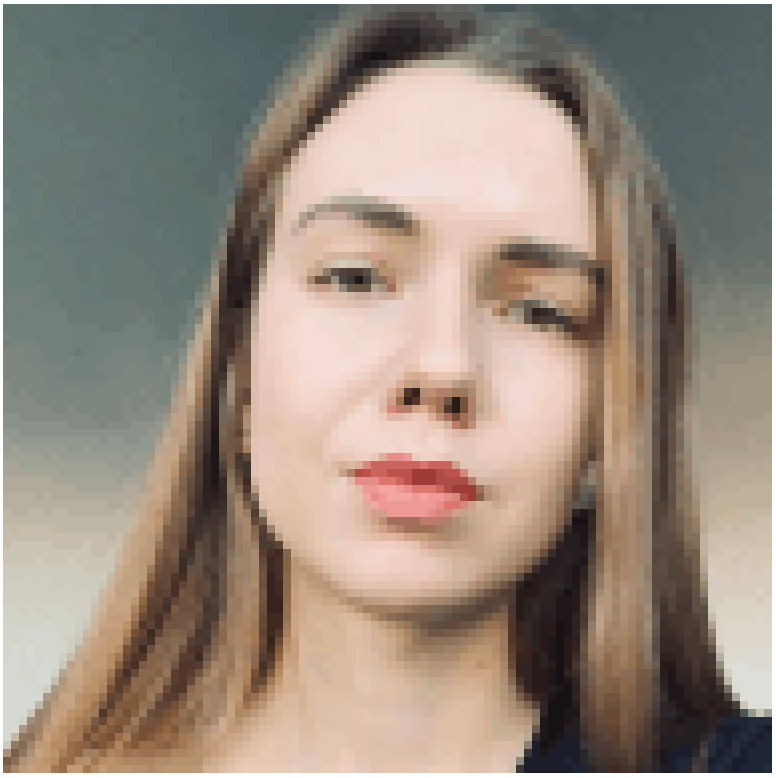
Reports on cyberattacks against Russia are rare, given that many Western companies have limited visibility into computer systems in the region.

This week, however, has been rich with reports from Russian cybersecurity firms. In addition to XDSpy's attack, F.A.C.C.T. recorded a cyberattack on Russian banks, telecom operators, logistics, and tech companies using DarkWatchman malware. The hackers disguised a phishing email as a newsletter from a Russian courier delivery service. The results of these attacks are unknown.

Another cyberattack was conducted by a new hacker group, Hellhounds, according to the Russian cybersecurity company Positive Technologies, which has been sanctioned by the U.S. Hellhounds has already compromised at least 20 Russian organizations, including government agencies, tech companies, and space and energy enterprises.

Cybersecurity firm BI.ZONE also recorded attacks conducted by Rare Wolf hackers. Since 2019, the group has attacked nearly 400 Russian companies, researchers said.

These reports do not disclose which countries are behind the attacks on Russia. However, in a report in November, researchers at the cybersecurity firm Solar said that the majority of state-sponsored cyberattacks against Russia originate from North Korea and China, with a primary interest in data theft.



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.
