New hacker group uses LockBit ransomware variant to target Russian companies

By Daryna Antoniuk

Published: 2025-06-09 · Archived: 2026-04-05 13:30:44 UTC

A financially motivated cybercrime group dubbed DarkGaboon has been targeting Russian companies in a series of ransomware attacks, researchers have found.

The group was first identified by Russian cybersecurity firm Positive Technologies in January, but researchers have traced its operations back to 2023. Since then, DarkGaboon has targeted Russian organizations across various sectors, including banking, retail, tourism and public services.

Positive Technologies was sanctioned by the U.S. in 2021 for allegedly providing IT support to Russia's civilian and military intelligence agencies.

In its latest campaign this spring, DarkGaboon was observed deploying LockBit 3.0 ransomware against victims in Russia, Positive Technologies said in a report last week.

The version of LockBit used by the group was leaked publicly in 2022 and is now employed by numerous cybercriminals. However, unlike typical LockBit affiliates operating under the ransomware-as-a-service model, DarkGaboon appears to function independently, according to the report.

In its operations, DarkGaboon relies on phishing emails written in Russian. These messages are crafted to appear urgent and are usually directed at employees in financial departments. They contain malicious attachments disguised as legitimate financial documents.

According to the report, the lure documents used by DarkGaboon are based on templates downloaded from legitimate Russian-language sources. These decoy files have remained relatively unchanged since 2023.

Once inside a victim's network, the group deploys LockBit 3.0 to encrypt files and leaves behind a ransom note written in Russian containing two contact email addresses. No signs of data exfiltration were found during recent incidents, according to Positive Technologies.

The same email addresses listed in the current ransom notes were previously linked to LockBit-based attacks on Russian financial institutions between March and April 2023.

The company has not been able to identify the individuals behind DarkGaboon but said the perpetrators are likely fluent in Russian.

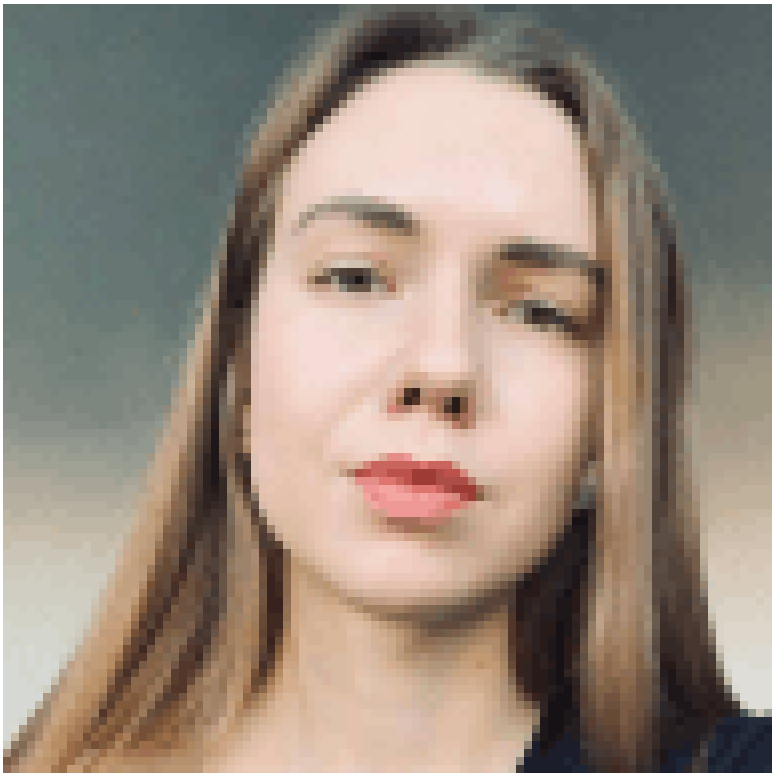
Researchers say the group uses open-source tools such as Revenge RAT, XWorm and LockBit ransomware to blend in with broader cybercriminal activity, making attribution more difficult.

Russian entities have previously been targeted with LockBit ransomware variants. In December, hackers reportedly used it in an attack on the largest dairy processing plant in southern Siberia.

Local media reported that the cyberattack occurred shortly after the company provided humanitarian aid — including drones — for Russian soldiers fighting in Ukraine. The attack has not been attributed to any specific threat actor.

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.
