Pro-Ukraine hacker group Bearlyfy targets Russian companies with custom ransomware

By Daryna Antoniuk

Published: 2026-03-26 · Archived: 2026-04-10 02:12:46 UTC

A pro-Ukrainian hacker group known as Bearlyfy has carried out more than 70 cyberattacks against Russian companies over the past year and is now escalating its campaign with newly developed ransomware tools, researchers have found.

Bearlyfy first appeared in January 2025 and initially targeted smaller Russian businesses. In its early operations, the attackers showed limited skills and demanded modest ransoms of only a few thousand dollars, according to a report by the Russian cybersecurity firm F6.

“Within a year this group has become a real nightmare for large Russian businesses,” researchers said, adding that the group’s ransom demands in recent attacks have grown to hundreds of thousands of dollars.

According to the researchers, the group’s primary goals are both financial and political. They appear to be causing “maximum damage” to Russian companies while also generating revenue through ransomware payments.

F6 estimates that roughly one in five victims ultimately pays the ransom.

The group has recently begun deploying its own malware, marking a new stage in its operations. Since early March, Bearlyfy has used a custom-built Windows ransomware strain known as GenieLocker, which researchers believe was developed by the group itself.

Unlike many ransomware operations, Bearlyfy’s malware does not always automatically generate ransom notes. Instead, attackers sometimes create their own messages manually, ranging from short instructions with contact details to longer messages mocking the victim company.

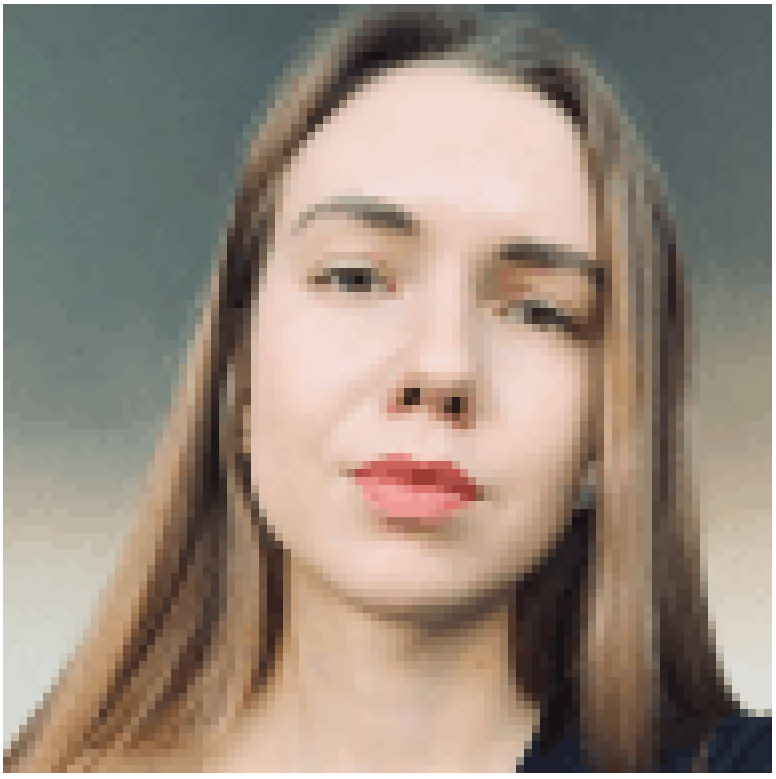
Earlier Bearlyfy attacks relied heavily on existing ransomware tools derived from leaked code. For example, Bearlyfy often used LockBit 3 Black, created with a builder for the LockBit ransomware-as-a-service platform that leaked online in 2022. On Linux systems, the group deployed a modified version of the Babuk ransomware based on publicly leaked source code.

F6 has also observed collaboration between Bearlyfy and other, more experienced pro-Ukrainian groups, such as Head Mare, although the group has maintained its own distinct operational style, researchers said.

Western researchers have not reported on Bearlyfy’s activity, likely because many lack visibility into Russian networks.

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.
