Kremlin-backed hacking group puts fresh emphasis on stealing credentials

By Daryna Antoniuk

Published: 2023-06-21 · Archived: 2026-04-06 00:23:34 UTC

Microsoft has detected an increase in credential-stealing attacks conducted by the Russian state-affiliated hacker group often labeled as APT29, Cozy Bear or Nobelium. These attacks are directed at governments, IT service providers, nongovernmental organizations (NGOs), and defense and critical manufacturing industries. Under Microsoft's new naming convention for advanced persistent threats (APTs), the company is calling the group Midnight Blizzard.

Microsoft didn't specify which countries were targeted in the recent campaign, but Nobelium has a history of conducting espionage against foreign ministries and diplomatic entities in countries that are part of NATO and the European Union.

The hackers are using "a variety of password spray, brute force, and token theft techniques," Microsoft said. Spraying involves trying a small set of commonly used or easily guessable passwords on multiple accounts. Brute force attacks use bulk attempts to guess a password. And token thefts involve the capturing of user-authentication information.

Nobelium is responsible for several high-profile incidents, including the SolarWinds supply chain attack in 2020 that affected thousands of organizations globally and led to a series of data breaches.

During the war in Ukraine, Nobelium has carried out cyberattacks against the Ukrainian military and its political parties, as well as international governments, think tanks and nonprofit organizations.

In a recent campaign, Microsoft observed Nobelium hackers using low-reputation proxy services that allowed them to route their internet traffic through regular households instead of commercial entities. This helped hackers to conceal their actual IP address and location.

Moreover, Nobelium typically used these IP addresses for brief periods of time, according to Microsoft. It's more challenging for security teams to identify and track the threat actor's actions when they frequently switch between different IP addresses.

In a recent campaign, Nobelium employed a range of techniques for conducting espionage operations.

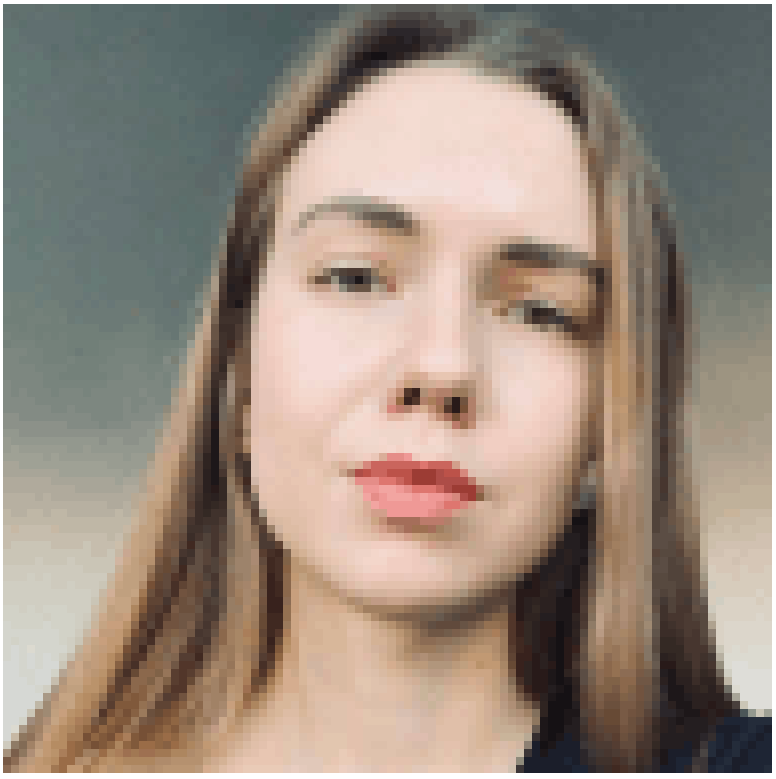
Microsoft said that it informed its customers who were targeted or impacted by the actions of a state-sponsored threat actor. However, the company did not disclose the specific names of Nobelium victims.

Intelligence Cloud.

Learn more.

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.
