

# [***Who Is Midnight Blizzard? Russian-Linked Group Has Repeatedly Targeted Microsoft, Company Says***](https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:6BHB-8MX1-JBCM-F3P2-00000-00&context=1516831)

Forbes.com

March 8, 2024 Friday

Copyright 2024 Forbes LLC All Rights Reserved

**Length:** 723 words

**Byline:** James Farrell, Forbes Staff

**Highlight:** Microsoft is facing an ongoing threat from Midnight Blizzard, the Russian-linked group that hacked the Democratic National Convention before the 2016 election.

**Body**

**Topline**

Microsoftsaysthat the Russian-linked group known as Midnight Blizzard or Nobelium has made repeated attempts to access Microsoft s systems in recent weeks, escalating its efforts against Microsoft since the company first disclosed in January that Midnight Blizzard hadaccessedsome of its corporate email accounts.

<figure>

<figcaption>

FILE - A logo of Microsoft is displayed during an event at the Chatham House think tank in London, Monday, Jan. 15, 2024. (AP Photo/Kin Cheung, File)

Copyright 2024 The Associated Press. All rights reserved

</figcaption></figure>

**Key Facts**

The group first launched its attack on Microsoft in November, with the company disclosing in January that the group had successfully used a password spray attack, trying a large number of potential passwords on known accounts, to finally access a very small percentage of Microsoft corporate email accounts.

On Friday, Microsoft announced in both a blog post and anSEC filing that Midnight Blizzard was using information lifted from that attack to gain, or attempt to gain, unauthorized access to the company s source code repositories and internal systems.

Microsoft says that Midnight Blizzard has increased the volume of its attacks by as much as 10-fold compared to what the company had already seen in January.

While Microsoft maintains that none of its customer-facing systems have been compromised, it noted that Midnight Blizzard may have accessed some emails between customers and Microsoft, and Microsoft has begun reaching out to affected customers.

Midnight Blizzard, as Microsoft refers to it, goes byseveral names, including Nobelium, APT29 and perhaps most recognizably Cozy Bear the name that made headlines when it targeted the Democratic National Convention ahead of the 2016 elections, part of the hack which led to the discovery of Russian efforts to manipulate U.S. ***politics*** that year.

**What Was Midnight Blizzard s Role In The Dnc Hack?**

Midnight Blizzard, reported at the time as Cozy Bear, was one of twoRussian-linkedgroups cited for the infamous hack of the Democratic National Convention ahead of the 2016 election. The other group, Fancy Bear, is believed to be linked to Russian military intelligence, also known as the GRU, which likely played a more active role in the hack and Russia s widely reported disinformation campaign, according to Adam Meyers, head of counter adversary operations at CrowdStrike, the cybersecurity firm thatfirst investigatedthe DNC hack. Cozy Bear, on the other hand, is associated with the Russian SVR, which is Russia s external intelligence agency and was likely doing intelligence collection in the hack, Meyers said.

**Key Background**

Cozy Bear has a long operational history dating back to the 2010s, Meyers told Forbes, often engaging in campaigns targeting diplomatic and political intelligence collection. The DNC hack wasn t its only high-profile campaign. The group has been pinned for the 2020 hack ofSolarWinds, a Texas-based IT firm, which then passed along compromised system updates to thousands of customers,includingMicrosoft, the Pentagon and the Department of Homeland Security though the company hassaidit believes only fewer than 100 customers were ultimately impacted. More recently, the hacks targeting Microsoft and also hacks in Januarytargeting Hewlett Packard, have brought the group back into public awareness.

**What To Watch For**

Microsoft wrote in its filing that its investigation into the attacks is ongoing, that findings will continue to evolve and further unauthorized access may occur.

**Chief Critic**

Meyers raised concern about Microsoft s ability to contain the attack, given its warning about potential further unauthorized access. He noted Microsoft was also breached in the SolarWinds attack and noted howChinese hackerspreviously accessed emails from State Department officials through Microsoft. He said he believed that Microsoft is a national security threat due to this history of breaches, noting the company s many contracts with governments around the world many of whom are electing new leaders this year and its own advanced artificial intelligence models. Think about what a Russian threat actor like Cozy Bear can do with some of the most advanced AI models known to man, Meyers told Forbes. Forbes has contacted Microsoft for comment.

**Further Reading**

**Load-Date:** May 3, 2024

**End of Document**