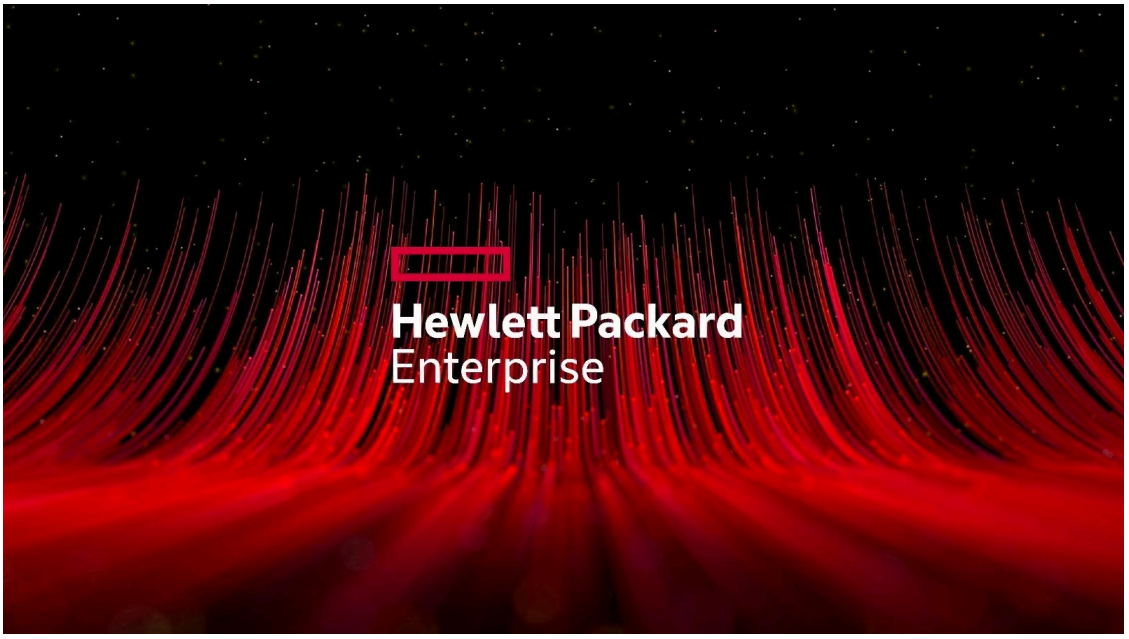
HPE: Russian hackers breached security team's email accounts

By Lawrence Abrams

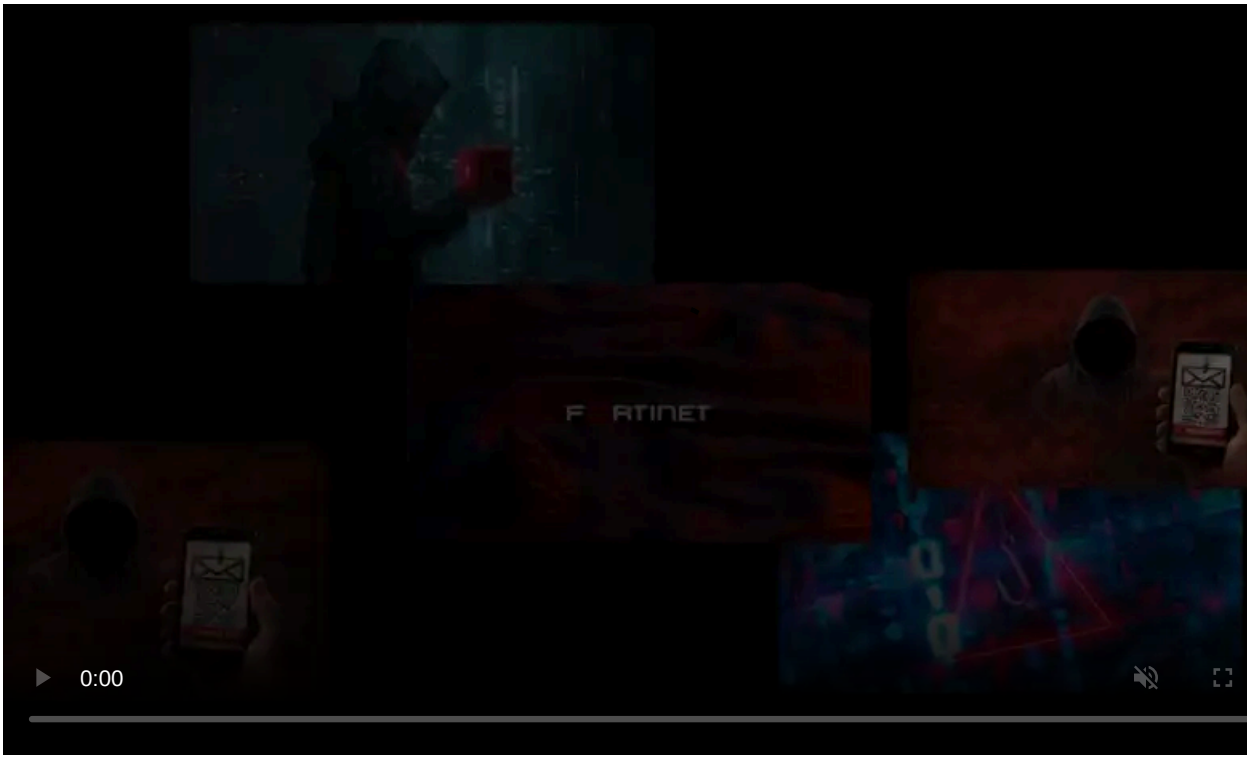
Published: 2024-01-24 · Archived: 2026-04-05 21:54:36 UTC



Hewlett Packard Enterprise (HPE) disclosed today that suspected Russian hackers known as Midnight Blizzard gained access to the company's Microsoft Office 365 email environment to steal data from its cybersecurity team and other departments.

Midnight Blizzard, aka Cozy Bear, APT29, and Nobelium, is a Russian state-sponsored hacking group believed to be part of Russia's Foreign Intelligence Service (SVR). The threat actors have been linked to multiple attacks throughout the year, including the infamous 2020 SolarWinds supply chain attack.

In a new Form 8-K SEC filing, HPE says they were notified on December 12th that the suspected Russian hackers breached their cloud-based email environment in May 2023.


F RTINET
0:00

"Based on our investigation, we now believe that the threat actor accessed and exfiltrated data beginning in May 2023 from a small percentage of HPE mailboxes belonging to individuals in our cybersecurity, go-to-market, business segments, and other functions," reads the SEC filing.

HPE says they are still investigating the breach but believe it is related to a previous breach in May 2023, when threat actors gained access to the company's SharePoint server and stole files.

The company continues to work with external cybersecurity experts and law enforcement to investigate the incident.

In response to further questions about the breach, HPE shared the following statement with BleepingComputer.

"On December 12, 2023, HPE was notified that a suspected nation-state actor had gained unauthorized access to the company's Office 365 email environment. HPE immediately activated cyber response protocols to begin an investigation, remediate the incident, and eradicate the activity. Through that investigation, which remains ongoing, we determined that this nation-state actor accessed and exfiltrated data beginning in May 2023 from a small percentage of HPE mailboxes belonging to individuals in our cybersecurity, go-to-market, business segments, and other functions. We believe the nation-state actor is Midnight Blizzard, also known as Cozy Bear.

The accessed data is limited to information contained in the users' mailboxes. We continue to investigate and will make appropriate notifications as required.

Out of an abundance of caution and a desire to comply with the spirit of new regulatory disclosure guidelines, we have filed a form 8-K with the Securities & Exchange Commission to notify that body, and investors, about this incident. That said, there has been no operational impact on our business and, to date, we have not determined that this incident is likely to have a material financial impact."

While HPE has not provided any further details, Microsoft recently reported a security breach by Midnight Blizzard that also involved data theft from the company's corporate email accounts, including its leadership team.

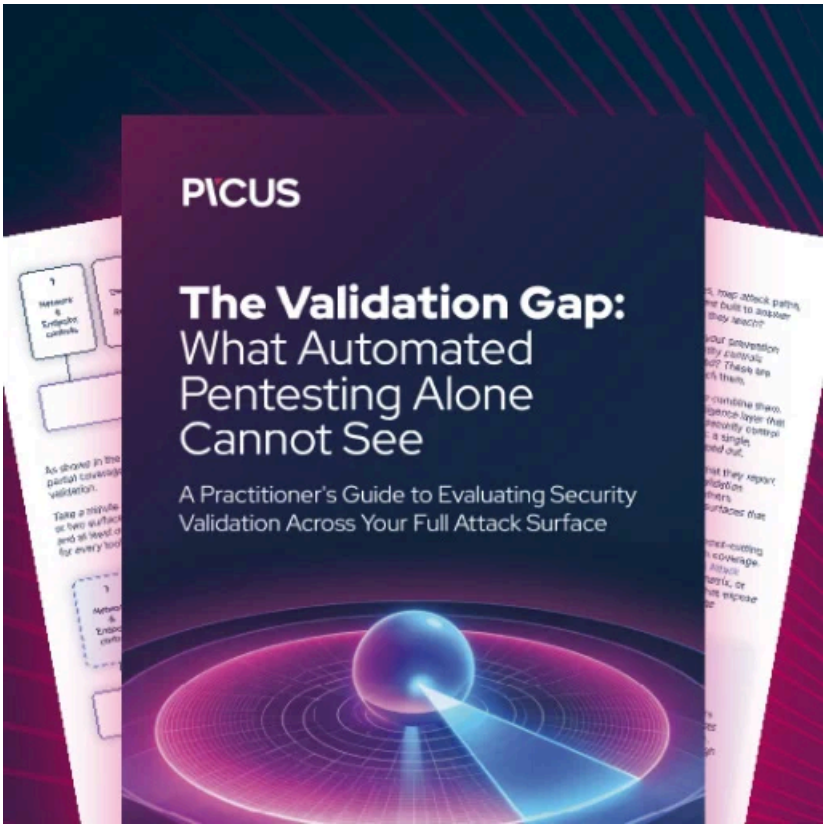
Microsoft's breach was caused by a misconfigured test tenant account that allowed the threat actors to brute force the account's password and log in to their systems.

Using this access, Midnight Blizzard gained access to corporate email accounts to steal data from Microsoft's senior leadership team and employees in its cybersecurity and legal departments.

HPE told BleepingComputer that they do not know if its incident is related to Microsoft's.

The company was previously breached in 2018 when Chinese hackers breached its and IBM's network and then used that access to hack into their customers' devices.

More recently, in 2021, HPE disclosed that the data repositories for its Aruba Central network monitoring platform were compromised, allowing a threat actor to access data about monitored devices and their locations.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/hpe-russian-hackers-breached-its-security-teams-email-accounts/