TechXplore

Microsoft says state-backed Russian hackers accessed emails of senior leadership team members

January 20 2024, by Frank Bajak

The Microsoft logo is shown at the Mobile World Congress 2023 in Barcelona, Spain, on March 2, 2023. In a blog post Friday, Jan. 19, 2024, Microsoft says state-backed Russian hackers broke into its corporate email system and accessed accounts of members of the company's leadership team as well as those of cybersecurity and legal employees. Credit: AP Photo/Joan Mateu Parra, File

State-backed Russian hackers broke into Microsoft's corporate email system and accessed the accounts of members of the company's leadership team, as well as those of employees on its cybersecurity and legal teams, the company said Friday.

In a blog post, Microsoft said the intrusion began in late November and was discovered on Jan. 12. It said the same highly skilled Russian hacking team behind the SolarWinds breach was responsible.

"A very small percentage" of Microsoft corporate accounts were accessed, the company said, and some emails and attached documents were stolen.

A company spokesperson said Microsoft had no immediate comment on which or how many members of its senior leadership had their email accounts breached. In a regulatory filing Friday, Microsoft said it was able to remove the hackers' access from the compromised accounts on or about Jan. 13.

"We are in the process of notifying employees whose email was accessed," Microsoft said, adding that its investigation indicates the hackers were initially targeting email accounts for information related to their activities.

The Microsoft disclosure comes a month after a new U.S. Securities and Exchange Commission rule took effect that compels publicly traded companies to disclose breaches that could negatively impact their business. It gives them four days to do so unless they obtain a national-security waiver.

In Friday's SEC regulatory filing, Microsoft said that "as of the date of this filing, the incident has not had a material impact" on its operations. It added that it has not, however, "determined whether the incident is reasonably likely to materially impact" its finances.

Microsoft, which is based in Redmond, Washington, said the hackers from Russia's SVR foreign intelligence agency were able to gain access by compromising credentials on a "legacy" test account, suggesting it had outdated code. After gaining a foothold, they used the account's permissions to access the accounts of the senior leadership team and others. The brute-force attack technique used by the hackers is called "password spraying."

The threat actor uses a single common password to try to log into multiple accounts. In an August blog post, Microsoft described how its threat-intelligence team discovered that the same Russian hacking team had used the technique to try to steal credentials from at least 40 different global organizations through Microsoft Teams chats.

"The attack was not the result of a vulnerability in Microsoft products or services," the company said in the blog. "To date, there is no evidence that the threat actor had any access to customer environments, production systems, source code, or AI systems. We will notify customers if any action is required."

Microsoft calls the hacking unit Midnight Blizzard. Prior to revamping its threat-actor nomenclature last year, it called the group Nobelium. The cybersecurity firm Mandiant, owned by Google, calls the group Cozy Bear.

In a 2021 blog post, Microsoft called the SolarWinds hacking campaign "the most sophisticated nation-state attack in history." In addition to U.S. government agencies, including the departments of Justice and Treasury, more than 100 private companies and think tanks were compromised, including software and telecommunications providers.

The main focus of the SVR is intelligence-gathering. It primarily targets governments, diplomats, think tanks and IT service providers in the U.S.

and Europe.

Citation: Microsoft says state-backed Russian hackers accessed emails of senior leadership team members (2024, January 20) retrieved 27 April 2024 from https://techxplore.com/news/2024-01-microsoft-state-russian-hackers-accessed.html