HP Enterprise discloses hack by suspected state-backed Russian hackers

January 25 2024, by Frank Bajak

A sign marks the entry way into Hewlett Packard Enterprise, May 24, 2016, in Andover, Mass. Hewlett Packard Enterprise disclosed Wednesday, Jan. 24, 2024, that suspected state-backed Russian hackers broke into its cloud-based email system and stole data from cybersecurity and other employees. Credit: AP Photo/Elise Amendola, File

Hewlett Packard Enterprise disclosed Wednesday that suspected state-backed Russian hackers broke into its cloud-based email system and stole data from cybersecurity and other employees.

The provider of information technology products and services said in a Securities and Exchange Commission regulatory filing that it was informed of the intrusion on Jan. 12. It said it believed the hackers were from Cozy Bear, a unit of Russia's SVR foreign intelligence service.

Microsoft reported last week that it also discovered an intrusion of its corporate network on Jan. 12. The Redmond, Washington, tech giant said the breach began in late November and also blamed Cozy Bear. It said the Russian hackers accessed accounts of senior Microsoft executives as well as cybersecurity and legal employees.

Cozy Bear was behind the SolarWinds breach and focuses stealth intelligence-gathering on Western governments, IT service providers and think tanks in the U.S. and Europe.

"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," HPE, which is based in Spring, Texas, said in the filing.

Company spokesman Adam R. Bauer, reached by email, would not say who informed HPE of the breach. "We're not sharing that information at this time." Bauer said the compromised email boxes were running Microsoft software.

In the filing, HPE said the intrusion was "likely related to earlier activity by this threat actor, of which we were notified in June 2023, involving unauthorized access to and exfiltration of a limited number of

SharePoint files." SharePoint is part of Microsoft's 365 suite, formerly known as Office, which includes email, word-processing and spreadsheet apps.

Bauer said HPE is unable to say whether the breach of its network was related to the hack that Microsoft disclosed last week as "we do not have the details of the incident Microsoft disclosed."

He did not specify the seniority of the HPE employees whose accounts were accessed by the hackers. "The total scope of mailboxes and emails accessed remains under investigation." HPE said in the filing that it has so far determined that the hack has had no material impact on its operations or financial health. Both disclosures come 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.

HPE was spun off in 2015 from the storied Silicon Valley computing company Hewlett-Packard Inc., which is best known today for its printer business.

Citation: HP Enterprise discloses hack by suspected state-backed Russian hackers (2024, January 25) retrieved 9 May 2024 from https://techxplore.com/news/2024-01-hp-enterprise-discloses-hack-state.html