Microsoft: China-based hackers found bug to target US firms

3 March 2021, by Matt O'brien

In this Nov. 10, 2016, file photo, people walk past a Microsoft office in New York. China-based government hackers have exploited a bug in Microsoft's email server software to target U.S. organizations, the company said Tuesday, March 2, 2021. (AP Photo/Swayne B. Hall, File)

China-based government hackers have exploited a bug in Microsoft's email server software to target U.S. organizations, the company said Tuesday.

Microsoft said that a "highly skilled and sophisticated" state-sponsored group operating from China has been trying to steal information from a number of American targets, including universities, defense contractors, law firms and infectious-disease researchers.

Microsoft said it has released security upgrades to fix the vulnerabilities to its Exchange Server software, which is used for work email and calendar services, mostly for larger organizations that have their own in-person email servers. It doesn't affect personal email accounts or Microsoft's cloud-based services.

The company said the hacking group it calls Hafnium was able to trick Exchange servers into allowing it to gain access. The hackers then masqueraded as someone who should have access and created a way to control the server remotely so that they could steal data from an organization's network.

Microsoft said the group is based in China but operates from leased virtual private servers in the U.S., helping it avoid detection.

The company based in Redmond, Washington, declined to name any specific targets or say how many organizations were affected.

Reston, Virginia-based cybersecurity firm Volexity, which Microsoft credits for helping to detect the intrusions, said its network security monitoring service began picking up on a suspiciously large data transfer in late January.

"They're just downloading email, literally going to town," said Steven Adair, Volexity's president, who said the targets have included "defense contractors, international aid and development organizations, the NGO think-tank community."

Adair said he's concerned that the hackers will accelerate their activity in the coming days before organizations are able to install Microsoft's security upgrades.

"As bad as it is now, I think it's about to get a lot worse," he said. "This gives them a limited amount of opportunity to go and exploit something. The patch isn't going to fix that if they left their backdoor behind."