INSIDER INTELLIGENCE | eMarketer

MAR 09

Mack DeGeurin

Microsoft's Exchange attack could fan flames for US government response

Article

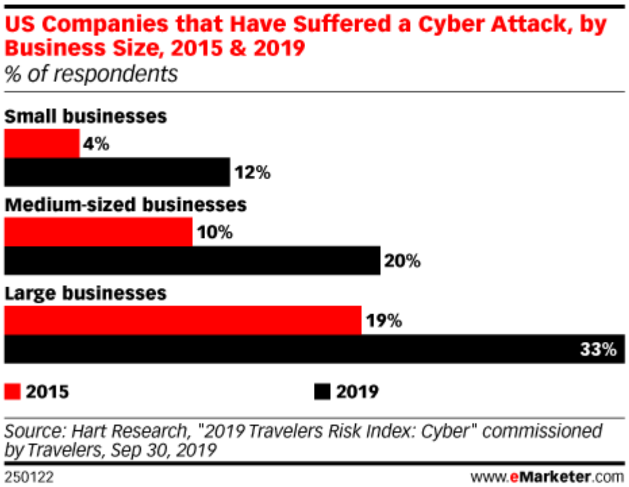
The news: Alleged Chinese hacking of thousands of Microsoft Exchange servers has prompted calls for retaliatory US attacks

How we got here: Researchers believe a hacking group named Hafnium began gaining access to Microsoft Exchange servers as early as January 6 this year. Hafnium, which multiple reports claim operates out of China, reportedly exploited four previously unknown vulnerabilities in Microsoft's Exchange servers' Outlook Web Access to gain access to at least 30,000 servers in the US alone, though that figure is expected to increase.

The hackers appear to have used automated scanning technology to indiscriminately target networks—which included small towns, cities, and local governments—and planted remotely accessible "web shell" backdoors on Exchange servers, per Wired.

- Though Microsoft issued emergency patches on March 2 to address the attack, a White House spokesperson released a statement saying, "Mitigation is not remediation if the servers have already been compromised" and called the situation an "active threat." per Reuters.
- The attacks come as the US recovers from another devastating cyberattack that targeted network management software company SolarWinds.

What's next: Fallout from both SolarWinds and the recent alleged Chinese hacking campaign has fueled calls for a retaliatory US government response. 2019 changes to the Defense Authorization Act allow US Cyber Command—the hacking arm of the Department of Defense — to "defend forward" by operating outside of US networks, making it easier for the US government to gather intelligence and retaliate. US intervention is reportedly underway, per The New York Times.



US Companies that Have Suffered a Cyber Attack, by Business Size, 2015 & 2019
% of respondents

Source: Hart Research, "2019 Travelers Risk Index: Cyber" commissioned by Travelers, Sep 30, 2019
250122 www.eMarketer.com