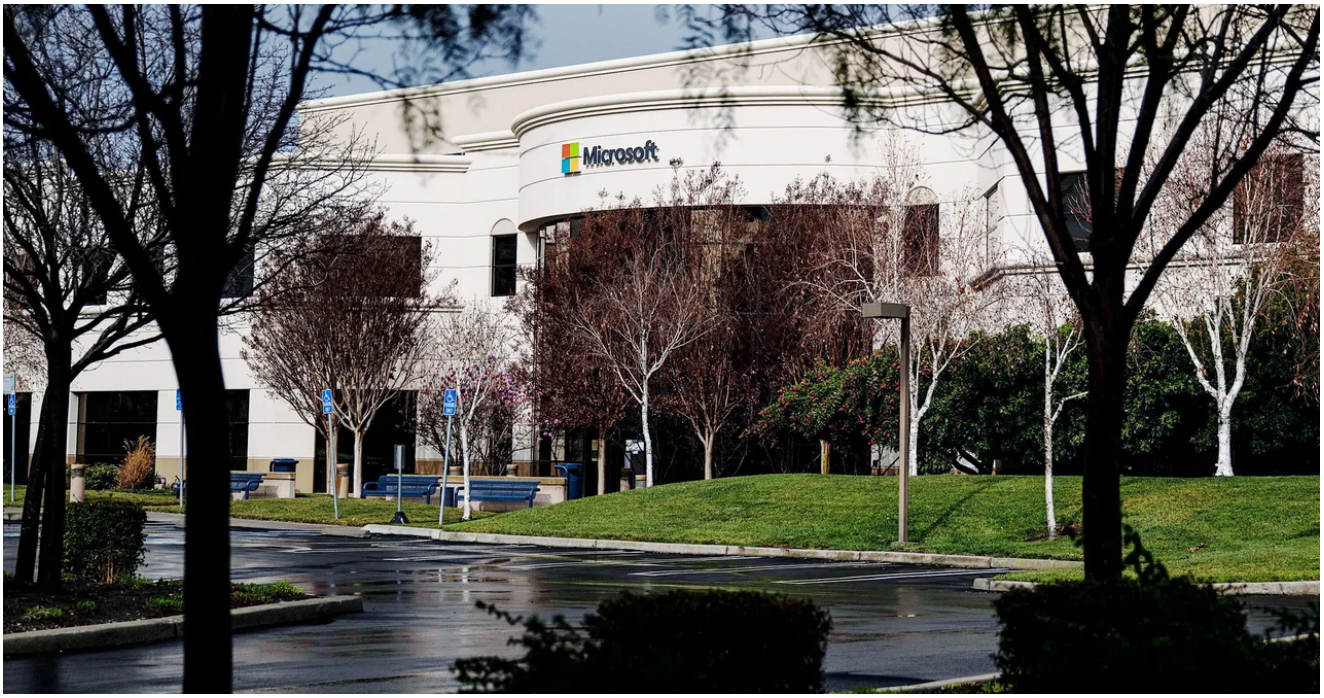
Chinese Hacking Spree Hit an ‘Astronomical’ Number of Victims

wired.com/story/china-microsoft-exchange-server-hack-victims/

Andy Greenberg March 5, 2021



When news hit earlier this week that Chinese hackers were actively targeting Microsoft Exchange servers, the cybersecurity community warned that the zero-day vulnerabilities they were exploiting might have allowed them to hit countless organizations around the world. Now it's becoming clear just many email servers they hacked. By all appearances, the group known as Hafnium breached as many victims they could find across the global internet, leaving behind backdoors to return to later.

Hafnium has now exploited zero-day vulnerabilities in Microsoft's Exchange servers' Outlook Web Access to indiscriminately compromise no fewer than tens of thousands of email servers, according to sources with knowledge of the investigation into the hacking campaign who spoke to WIRED. The intrusions, first spotted by security firm Volexity, began as early as January 6, with a noticeable uptick starting last Friday and spiking early this week. The hackers appear to have responded to Microsoft's patch, released Tuesday, by ramping up and automating their hacking campaign. One security researcher involved in the investigation who spoke to WIRED on the condition of anonymity put the number of hacked Exchange servers at more than 30,000 in the US alone, and hundreds of thousands worldwide, all apparently by the same group. Independent cybersecurity journalist Brian Krebs first reported that 30,000 figure Friday, citing sources who had briefed national security officials.

"It's massive. Absolutely massive," one former national security official with knowledge of the investigation told WIRED. "We're talking thousands of servers compromised per hour, globally."

“It's a ticking time bomb.”

Steven Adair, Volexity

In a press conference Friday afternoon, White House press secretary Jen Psaki warned anyone running the affected Exchange servers to implement Microsoft's patch for the vulnerabilities immediately. "We are concerned that there are a large number of victims and are working with our partners to understand the scope of this," Psaki said in a rare instance of a White House press secretary commenting on specific cybersecurity vulnerabilities. "Network owners also need to consider whether they have already been compromised and should immediately take appropriate steps." That White House advice echoed a tweet from former Cybersecurity and Infrastructure Security Agency director Chris Krebs on Thursday night advising anyone with an exposed Exchange server to "assume compromise" and begin incident response measures to remove the hackers' access.

The affected networks, which likely include those of small and medium-size organizations more than the large enterprises that tend to use cloud-based email systems, appear to have been hacked indiscriminately via automated scanning. The hackers planted a "web shell"—a remotely accessible, web-based backdoor foothold—on the Exchange servers they exploited, allowing them to perform reconnaissance on the target machines and potentially move to other computers on the network.

That means only a small number of the hundreds of thousands of hacked servers around the world are likely to be actively targeted by the Chinese hackers, says Volexity founder Steven Adair. Nonetheless, any organization that doesn't take pains to remove the hackers' backdoor remains compromised, and the hackers could reenter their networks to steal data or cause mayhem until that web shell is removed. "A massive, massive number of organizations are getting that initial foothold," says Adair. "It's a ticking time bomb that can be used against them at any point in time."

Though the vast majority of intrusions appear to have consisted only of those web shells, the "astronomical" scale of those global compromises is uniquely disturbing, one security researcher who participated in the investigation told WIRED. The small to medium-size organizations that were compromised include local government agencies, police, hospitals, Covid response, energy, transportation, airports, and prisons. "China just owned the world—or at least everyone with Outlook Web Access," the researcher said. "When was the last time someone was so bold as to just hit *everyone*?"

In fact, the last such mass intrusion campaign came to light in just December, with the revelation that Russian hackers had compromised IT management tools from Solar Winds' used by 18,000 organizations. That hacking campaign successfully breached at least half a dozen US federal agencies. The Hafnium Exchange hacking campaign now represents the second hacking campaign of that scale, just a few months later.

The Chinese hackers Exchange exploitation spree appears to have begun only months ago, in contrast to the Russia's silent, year-plus SolarWinds espionage campaign. And Hafnium's victim list appears more limited to small- and medium-sized organizations, whereas the SolarWinds hit large US government agencies.

But as with the Russian SolarWinds hackers, investigators have yet to identify who exactly the Hafnium hackers are—beyond Microsoft's assertion that they're state-sponsored and operate out of China—or to pin down the full extent of their motivations. "I don't understand what the strategic objective of maintaining persistence on a local government agency would be for the MSS," says the former national security official, referring to China's Ministry of State Security. "Is this a contractor or a proxy group? Is it a Chinese cybercriminal group? Is it a rogue actor in China that got out ahead of itself?"

While the hacking campaign may be aimed at casting a wide net before filtering targets for espionage, the security researcher who spoke to WIRED warned that it may yet have disruptive effects. "If they push ransomware to this, we're going to have the worst day ever," he says.

But unlike the SolarWinds incident, the researcher points out, the Exchange-hacking campaign was caught early—or at least early in its widespread use. As daunting as the task of cleaning up the hackers' tens of thousands of infections may be, that early detection may give victims a chance to both patch their systems and remove the hackers before they can take advantage of their foothold inside organizations. "If we had a chance to prevent a SolarWinds-scale thing that went on for months, wouldn't we want to act on it?" asks the researcher. "Now we have that chance if we act fast."
