White House formally blames China's Ministry of State Security for Microsoft Exchange Hack

By Martin Matishak

Published: 2022-12-12 · Archived: 2026-04-05 19:22:06 UTC

The U.S. and a coalition of allies on Monday formally attributed the sweeping campaign against Microsoft Exchange email servers to hackers affiliated with China's Ministry of State Security.

The group assessed with "high confidence" that Beijing-linked digital operators carried out the attack that ensnared hundreds of thousands of systems worldwide, a senior Biden administration official told reporters on Sunday.

In addition, the partners alleged the ministry — which oversees the civilian arm of Beijing's intelligence gathering operations — has utilized contract hackers to conduct other malicious cyber activities around the globe, including a ransomware attack on an American company, and other pursuits to line the pockets of MSS officials.

The use of such hired muscle "was really eye-opening and surprising for us," said the official, who was only authorized to speak anonymously.

The coalition includes the U.S., the so-called "Five Eye" nations, Japan, the European Union and NATO. Monday's announcement marks the first time the transatlantic alliance has condemned Chinese digital activities, the official said.

The massive Exchange hack was first disclosed in March — at the same time the Biden administration was dealing with the SolarWinds breach that has since been formally attributed to Russia's foreign intelligence service.

At the time Microsoft announced that it had uncovered new vulnerabilities in its Exchange Server program, which runs businesses' email systems, adding the tech giant had assessed with "high confidence" that a hacking group known as HAFNIUM, a Chinese state-sponsored group, was exploiting the vulnerabilities.

The White House signaled late last month that it was getting closer to pinning the attack on a specific culprit.

The administration official said naming the offender took so long, in part, because of "new attributes" like the sheer breadth of the global campaign, which impacted tens of thousands organizations across the U.S. alone.

The White House also wanted to combine the exposure with "network defensive information," such as malware signatures and other indications of compromise, the official said. The FBI, NSA and CISA issued a joint release that documented over 50 tactics and techniques the Chinese state-sponsored hackers use when targeting U.S. and allied networks and ways to mitigate them.

In addition, the U.S. wanted to include its partners and allies in the attribution process and present a unified front in the face of Beijing's efforts, "which we felt was really critical to conveying our criticism and our concerns about the irresponsible malicious activities coming out of China," according to the official, who added such concerns had been raised the country's Communist government.

Monday's announcement was markedly different from the one that accompanied the attribution for the SolarWinds intrusion, which saw Moscow officially blamed and sanctioned in the operation that compromised multiple government agencies and private sector companies.

The official said the administration had made clear that it would take action to protect the country "no matter who's responsible, and we're not ruling out further actions to hold the [People's Republic of China] accountable."

"We're also aware that no one action can change the PRC behavior, and neither can one country acting on them," the official added. "We felt like the core takeaway here is that we're making it clear to China that, for as long as these irresponsible malicious cyber activities continue, it will unite countries around the world" to call out the nation's behavior and promote joint efforts on cybersecurity and network defense.

The administration official declined to offer additional details about the ransomware incident.

"It literally was what we think about with ransomware … a large ransom request made to an American company, and it really raised concerns for us with regard to the behavior and frankly, … with regard to the fact that individuals affiliated with the MSS conducted it."

Coalition officials pinned the attacks on groups tracked as APT31 and APT40 by cybersecurity experts, according to a press release from the UK National Cyber Security Centre. Supporting statements were also issued by NATO, the UK government, the European Union Council, Australia, Japan, Canada, Latvia, Lithuania, Estonia, Slovenia, Finland, and Denmark.

Moments after the White House announcement, the DOJ also levied formal charges against four Chinese nationals for their role in the APT40 hacking group.

Article updated post publication with links to other formal announcements and the DOJ's APT40 charges. Additional reporting by Catalin Cimpanu.

No previous article

No new articles

Martin Matishak

is the senior cybersecurity reporter for The Record. Prior to joining Recorded Future News in 2021, he spent more than five years at Politico, where he covered digital and national security developments across Capitol Hill, the Pentagon and the U.S. intelligence community. He previously was a reporter at The Hill, National Journal Group and Inside Washington Publishers.
