

China denies Microsoft hack, condemns US allies

20 July 2021, by Sarah Titterton and Shaun Tandon



The Microsoft hack, which exploited flaws in the Microsoft Exchange service, affected at least 30,000 US organizations including local governments as well as organizations worldwide.

China on Tuesday sharply denied US allegations it carried out a massive Microsoft hack, countering that Washington was the "world champion" of cyber attacks while raging at American allies for signing up to a rare joint statement of condemnation.

The United States on Monday [accused](#) Beijing of carrying out the [cyber attack](#) on Microsoft and charged four Chinese nationals over the "malicious" hack in March.

US Secretary of State Antony Blinken said the attack on Microsoft Exchange, a top email server for corporations around the world, was part of a "pattern of irresponsible, disruptive and destabilizing behavior in cyberspace, which poses a major threat to our economic and [national security](#)."

China's Ministry of State Security, or MSS, "has fostered an ecosystem of criminal contract hackers

who carry out both state-sponsored activities and cybercrime for their own financial gain," Blinken said in a statement.

In a simultaneous announcement, the US Department of Justice said four Chinese nationals had been charged with hacking the computers of dozens of companies, universities and government bodies in the United States and abroad between 2011 and 2018.

Pointing to the indictment, Blinken said the United States "will impose consequences on (Chinese) malicious cyber actors for their irresponsible behavior in cyberspace."

President Joe Biden told reporters the United States was still completing an investigation before taking any countermeasures and drew parallels with the murky but prolific cybercrime attributed by Western officials to Russia.

"The Chinese government, not unlike the Russian government, is not doing this themselves, but are protecting those who are doing it, and maybe even accommodating them being able to do it," Biden told reporters.

In a step the Biden administration hailed as unprecedented, the United States coordinated its statement Monday with allies—the European Union, Britain, Australia, Canada, New Zealand, Japan and NATO.

The Chinese embassy in New Zealand issued a swift rebuttal of the "totally groundless and irresponsible" allegations.



US President Joe Biden says that China has protected cyber criminals.

It was backed up by the embassy in Australia, as China took a coordinated stance of its own, accusing Canberra of "parroting the rhetoric of the US."

"It is well known that the US has engaged in unscrupulous, massive and indiscriminate eavesdropping on many countries including its allies," the embassy said in a statement.

"It is the [world champion](#) of malicious cyber attacks."

NATO solidarity

Biden, like his predecessor Donald Trump, has ramped up pressure on China, seeing the rising Asian power's increasingly assertive moves at home and abroad as the main long-term threat to the United States.

Allies backed up the castigation of China with British Foreign Secretary Dominic Raab describing the cyberattack as "reckless."

NATO offered "solidarity" over the Microsoft hacking without directly assigning blame, while noting that allies United States, Britain and Canada found China to be responsible.

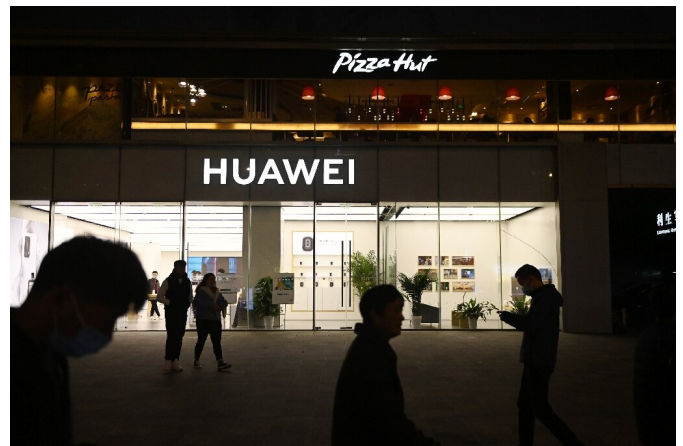
State Department spokesman Ned Price said it was

the first time that NATO—the Western military alliance whose members include Hungary and Turkey, which have comparatively cordial relations with Beijing—has condemned cyber activity from China.

It comes weeks after NATO took up China at a summit attended by Biden.

"We know we'll be stronger, we know we'll be more effective when we act collectively," Price said, saying the United States was not ruling out further action.

Biden has promised a strategy driven by alliances to face Beijing, drawing a contrast with Trump's predilection for harsh rhetoric.



People in Beijing walk in October 2020 past a store of Huawei, the Chinese electronics giant blacklisted by the United States.

Billions seen lost

Frank Cilluffo, director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security, praised the "breadth and depth of international cooperation" in clearly attributing responsibility to China.

"In addition to the indictments, we need to follow through to ensure there are consequences to induce changes in the Chinese government's

behavior and hopefully move toward leveling the cyber playing field," he said.

The Microsoft hack, which exploited flaws in the Microsoft Exchange service, affected at least 30,000 US organizations including local governments as well as organizations worldwide.

"Responsible states do not indiscriminately compromise global network security nor knowingly harbor cyber criminals—let alone sponsor or collaborate with them," Blinken said in his statement.

"These contract hackers cost governments and businesses billions of dollars in stolen intellectual property, ransom payments, and cybersecurity mitigation efforts, all while the MSS had them on its payroll."

Accusations of cyberattacks against the United States have recently focused on Russia, rather than China.

US officials say that many of the attacks originate in Russia, although they have debated to what extent there is state involvement. Russia denies responsibility.

This year has seen a slew of prominent ransomware strikes that have disrupted a major US pipeline, a meat processor and the software firm Kaseya, which affected 1,500 businesses.

Last week, Washington offered \$10 million for information about foreign online extortionists.

© 2021 AFP

APA citation: China denies Microsoft hack, condemns US allies (2021, July 20) retrieved 19 October 2021 from <https://techxplore.com/news/2021-07-china-denies-microsoft-hack-condemns.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.