

US and allies accuse Chinese government of masterminding Microsoft Exchange cyberattack

The United States and key allies have accused the Chinese government for the first time of hiring gangs of hackers to carry out cyberattacks in the West. Attacks attributed to China include the recent Microsoft Exchange hack, a significant and widespread breach that gave attackers access to the email servers of an estimated 30,000 organizations in the US alone.

The Microsoft Exchange attack was initially blamed on Hafnium, a hacking group sponsored by the Chinese state. A senior official in the White House told reporters in a briefing at the weekend that the US government had “high confidence” that the Exchange hackers were being paid by the Chinese government.

China is accused of hiring gangs of hackers to carry out cyberattacks

“[China’s] MSS – Ministry of State Security – uses criminal contract hackers to conduct unsanctioned cyber operations globally, including for their own personal profit,” said the official. “Their operations include criminal activities, such as cyber-enabled extortion, crypto-jacking and theft from victims around the world for financial gain.”

The accusation against China was made by the US, EU, UK, Australia, Canada, New Zealand, Japan, and NATO, reports *Bloomberg News*.

In a press statement, the European Union said these and other attacks were linked to hacking groups known as Advanced Persistent Threat 40 and Advanced Persistent Threat 31 (these labels are used by cybersecurity professionals to track the activity of known organizations). The UK's National Cyber Security Centre (NCSC) said that the APT40 group had targeted "maritime industries and naval defence contractors in the US and Europe" while APT30 had attacked "government entities, including the Finnish parliament in 2020."

"The attack on Microsoft Exchange servers is another serious example of a malicious act by Chinese state-backed actors in cyberspace," said NCSC Director of Operations Paul Chichester in a press statement. "This kind of behaviour is completely unacceptable, and alongside our partners we will not hesitate to call it out when we see it."

Cyberattacks and ransomware incidents have been on the rise in recent years, with gangs of hackers apparently targeting larger organizations. This year alone, hackers have targeted America's largest meat supplier and a key oil pipeline, though in both cases the groups responsible are thought to be based in Eastern Europe, and most likely Russia.

Russia was also blamed for 2020's SolarWinds hack, which breached a number of US federal government entities, and to which the US responded with new economic sanctions.

However, today's announcement includes no similar sanctions against China for its role in the Microsoft Exchange attack (though these could follow). "The US and our allies and partners are not ruling out further actions to hold the PRC accountable," said a senior White House official during a briefing. The US Department of Justice did, though, announce criminal charges against four hackers sponsored by China's MSS for "a multiyear campaign targeting foreign governments and entities in key sectors, including maritime, aviation, defense, education, and healthcare in at least a dozen

countries.”

The most notable aspect of today’s accusation is instead the broad coalition of countries that are publicly condemning China. It also the first time the military alliance NATO has formally accused the country of organizing cyberattacks.

<https://www.theverge.com/2021/7/19/22583251/us-government-blames-china-cyberattacks-microsoft-exchange-hack>