# 1-The Guardian-UK and allies accuse Chinese

This article is more than 7 months old

UK and allies accuse Chinese state-backed group of Microsoft hack

This article is more than 7 months old

British foreign secretary says Beijing will be held to account if it does not stop ‘systematic cyber sabotage’

In early March, Microsoft released a patch to Exchange after discovering hackers were stealing email communications . Photograph: Omar Marques/SOPA Images/Rex/Shutterstock

In early March, Microsoft released a patch to Exchange after discovering hackers were stealing email communications . Photograph: Omar Marques/SOPA Images/Rex/Shutterstock

Mon 19 Jul 2021 10.21 EDT

First published on Mon 19 Jul 2021 07.37 EDT

Britain has joined with the US and other allies in formally accusing Chinese state-based hacking groups of being behind the exploitation of an estimated 250,000 Microsoft Exchange servers worldwide earlier this year.

The UK foreign secretary said the cyber-attack amounted to “a reckless but familiar pattern of behaviour”, in an announcement released on Monday.

Dominic Raab called on Beijing to “end this systematic cyber-sabotage” and said it “can expect to be held to account if it does not”, as the UK steps up complaints about Chinese hacking.

In early March, Microsoft released a patch to Exchange after discovering that hackers were stealing email communications from internet-facing systems running its business software *[Rebuild]*.

At the time Microsoft said the hacking was conducted by a Chinese group called Hafnium but did not say whether it believed the Chinese state was behind it.

Last year, Microsoft accused hackers – including those from China – of attempting to snoop on individuals and groups involved with the 2020 US presidential election campaigns, "including people associated with the Joe Biden for president campaign", as well as "prominent leaders in the international affairs community". China's foreign ministry spokesperson denied the allegations and said Microsoft "should not make accusations against China out of nothing".

Monday's announcement marks a formal attribution of responsibility by the west. Britain's National Cyber Security Centre (NCSC), an arm of GCHQ, said it was "highly likely that Hafnium is associated with the Chinese state".

It is believed the group is supported, sustained and directed by China's powerful ministry of state security (MSS) and is part of a wider pattern of the ministry's directed activity that also includes other specialist hacker groups.

Further announcements by other countries are expected shortly. Companies were advised to implement Microsoft patches if they had not already done so; 8% of firms had not done so by the end of March, according to Microsoft.

Downing Street said the UK would "consider our options" over what, if any, action to take in response.

Tom Tugendhat, who chairs the Commons foreign affairs committee, said the use of such cyber-attacks by China was "deeply concerning".

He said: “We should be particularly alarmed by the NCSC’s judgment that it is ‘almost certain’ that the Chinese MSS was behind the attack on Finland’s parliament in 2020.

“This is an appalling demonstration of the reality of the kind of relationship Beijing is seeking. Win-win in Beijing means winning openly and, if not, trying to steal a victory.”

The White House said China’s “pattern of irresponsible behaviour in cyberspace” was “inconsistent with its stated objective of being seen as a responsible leader in the world”. It indicated that other countries would be expected to follow suit.

Diplomats hope that by publicly calling out the links between hacking groups – two others were also cited by the UK as being backed by the MSS – Beijing will be forced to close them down.

They believe China dislikes being compared with Russia, another country accused of directing hacking groups or giving the groups cover to engage in cyber-espionage. But beyond seeking to embarrass, no further sanctions were outlined.

British and other officials were understood to have presented dossiers to the Chinese government with further information justifying their attribution. Sources said that in general, Chinese officials tended to respond with surprise and ask for further information.

Joe Biden has been particularly keen to sharpen the west’s focus on China. In June, the US president helped persuade Nato, the military alliance traditionally concentrated on Russia, to declare that China represents a security risk for the first time .

However, unlike the UK and US, the EU did not blame the Chinese government for the “malicious” attacks, noting merely they were “conducted from the territory of China for the purpose of intellectual property theft and espionage”.

In a separate statement, the EU said its institutions, member state governments and “key European industries” had been hit by the cyber-attack on Microsoft Exchange. The EU’s diplomatic service described the behaviour as “irresponsible and harmful”.

EU foreign policy is made by unanimity and the bloc is often criticised for being slow to respond to violations of international law and crises. The spokesperson declined to give more details on the nature of the attacks. *[Deny]*

Topics