UK and allies hold Chinese state responsible for a pervasive pattern of hacking

Press release

UK joins likeminded partners to confirm Chinese state-backed actors were responsible for gaining access to computer networks via Microsoft Exchange servers.

The UK is joining likeminded partners to confirm that Chinese state-backed actors were responsible for gaining access to computer networks around the world via Microsoft Exchange servers.

The attacks took place in early 2021, affecting over a quarter of a million servers worldwide.

Foreign Secretary Dominic Raab said:

> The cyber attack on Microsoft Exchange Server by Chinese state-backed groups was a reckless but familiar pattern of behaviour.
>
> The Chinese Government must end this systematic cyber sabotage and can expect to be held account if it does not.

The attack was highly likely to enable large-scale espionage, including acquiring personally identifiable information and intellectual property. At the time of the attack, the UK quickly provided advice and recommended actions to those affected and Microsoft said that by end of March that 92% of customers had patched against the vulnerability.

Today the UK is also attributing the Chinese Ministry of State Security as being behind activity known by cyber security experts as “APT40” and “APT31”.

Widespread, credible evidence demonstrates that sustained, irresponsible

cyber activity emanating from China continues.

The Chinese government has ignored repeated calls to end its reckless campaign, instead allowing its state-backed actors to increase the scale of their attacks and act recklessly when caught.

This coordinated action today sees the international community once again urge the Chinese government to take responsibility for its actions and respect the democratic institutions, personal data and commercial interests of those with whom it seeks to partner.

The UK is calling on China to reaffirm the commitment made to the UK in 2015 and as part of the G20 not to conduct or support cyber-enabled theft of intellectual property of trade secrets.

Notes to editors

- As part of a cross-Government response, the National Cyber Security Centre (NCSC) issued tailored advice to over 70 affected organisations to enable them successfully to mitigate the effects of the compromise.
- In 2018, the UK government and its allies revealed that elements of the Chinese Ministry of State Security (MSS) were responsible for one of the most significant and widespread cyber intrusions stealing trade secrets. [link]
- The European Union has also made an announcement today [link].

The National Cyber Security Centre has assessed that:

Actors	Activity	NCSC Assessment
HAFNIUM	Compromising Microsoft Exchange gave the perpetrator a foothold to pivot further into the IT networks of victims.	NCSC is almost certain that the Microsoft Exchange compromise was initiated and exploited by a Chinese state-backed threat actor. NCSC judge it highly likely that HAFNIUM is associated with the Chinese state. The attack was highly likely to enable large-scale espionage, including acquiring personally identifiable information and intellectual property.
APT40, TEMP.Periscope, TEMP.Jumper. Leviathan	Targeting maritime industries and naval defence contractors in the US and Europe. Targeting regional opponents of the Belt and Road Initiative. Targeting multiple Cambodian electoral entities in the run up to the 2018 election.	NCSC judge it is highly likely that APT40 is linked to the Chinese Ministry of State Security and operates to key Chinese State Intelligence requirements. NCSC judge that APT40 is highly likely sponsored by the regional MSS security office, the MSS Hainan State Security Department (HSSD).

Actors	Activity	NCSC Assessment
APT31, Judgement Panda, Zirconium, Red Keres	Since 2020 targeting government entities, political figures, contractors and service providers. European countries. Targeting Finnish Parliament in 2020.	NCSC judge it is almost certain that APT31 is affiliated to the Chinese State and likely that APT31 is a group of contractors working directly for the Chinese Ministry of State Security.

Published 19 July 2021