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

Published: 2021-07-19 · Archived: 2026-04-05 16:58:36 UTC

The UK has revealed that Chinese state-backed actors were responsible for gaining access to computer networks around the world via Microsoft Exchange servers.

The National Cyber Security Centre – which is a part of GCHQ – assessed that it was highly likely that a group known as HAFNIUM, which is associated with the Chinese state, was responsible for the activity.

The attacks took place in early 2021 and open-source reporting indicates that at least 30,000 organisations have been compromised in the US alone, with many more affected worldwide. As part of a cross-Government response, the NCSC issued tailored advice to over 70 affected organisations to enable them successfully to mitigate the effects of the compromise.

NCSC Director of Operations Paul Chichester said:

“The attack on Microsoft Exchange servers is another serious example of a malicious act by Chinese state-backed actors in cyberspace.

“This kind of behaviour is completely unacceptable, and alongside our partners we will not hesitate to call it out when we see it.

“It is vital that all organisations continue to promptly apply security updates and report any suspected compromises to the NCSC via our website.”

The NCSC recommends following vendor best practice advice in the mitigation of vulnerabilities, and any organisations which have yet to install security updates released for Microsoft Exchange servers should do so. More information can be found on Microsoft’s website.

The attack on Microsoft Exchange software was highly likely to enable large-scale espionage, including acquiring personally identifiable information and intellectual property.

It is the most significant and widespread cyber intrusion against the UK and allies uncovered to date.

The UK is also attributing the Chinese Ministry of State Security as being behind activity known in open source as “APT40” and “APT31”.

Activity relating to APT40 included the targeting maritime industries and naval defence contractors in the US and Europe, and for APT31 the targeting of government entities, including the Finnish parliament in 2020.

Read the UK Foreign Secretary’s statement.

Source: https://www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking