UK and allies expose China-based technology companies for enabling global cyber campaign against critical networks

The NCSC and international partners share technical details of malicious activities and urge organisations to take mitigative actions.

- GCHQ's National Cyber Security Centre and international partners link three China-based companies to campaign targeting foreign governments and critical networks.
- Commercial cyber ecosystem with links to the Chinese intelligence services has enabled global malicious activity.
- New advisory supports UK organisations in critical sectors bolster their security against China state-sponsored cyber activity
- Network defenders urged to proactively hunt for activity and take steps to mitigate threat from attackers exploiting avoidable weaknesses

The UK and international allies have today (Wednesday) publicly linked three technology companies based in China with a global malicious cyber campaign targeting critical networks.

In a new advisory published today, the National Cyber Security Centre (NCSC) – a part of GCHQ - and international partners from twelve other countries have shared technical details about how malicious cyber activities linked with these China-based commercial entities have targeted nationally significant organisations around the world.

Since at least 2021, this activity has targeted organisations in critical sectors including government, telecommunications, transportation, lodging, and military infrastructure globally, with a cluster of activity observed in the UK.

The activities described in the advisory partially overlaps with campaigns previously reported by the cyber security industry most commonly under the name Salt Typhoon.

The data stolen through this activity can ultimately provide the Chinese intelligence services the capability to identify and track targets' communications and movements worldwide.

The advisory describes how the threat actors have had considerable success taking advantage of known common vulnerabilities rather than relying on bespoke malware or zero-day vulnerabilities to carry out their activities, meaning attacks via these vectors could have been avoided with timely patching.

Organisations of national significance in the UK are encouraged to proactively hunt for malicious activity and implement mitigative actions, including ensuring that edge devices are not exposed to known vulnerabilities and implementing security updates.

NCSC Chief Executive Dr Richard Horne said:

> "We are deeply concerned by the irresponsible behaviour of the named commercial entities based in China that has enabled an unrestrained campaign of malicious cyber activities on a global scale.
>
> "It is crucial organisations in targeted critical sectors heed this international warning about the threat posed by cyber actors who have been exploiting publicly known – and so therefore fixable – vulnerabilities.
>
> "In the face of sophisticated threats, network defenders must proactively hunt for malicious activity, as well as apply recommended mitigations based on indicators of compromise and regularly reviewing network device logs for signs of unusual activity."

The UK has led globally in helping to improve cyber risk management with leading legislation including the Telecommunications (Security) Act 2021 and the associated Code of Practice, for which the NCSC was the technical authority.

The government's forthcoming Cyber Security and Resilience Bill will further strengthen the UK's cyber defences, protecting the services the public rely on to go about their normal lives.

The NCSC and government partners have previously warned about the growing range of cyber threats facing critical sectors and provides a range of guidance and resources to improve resilience.

The NCSC's Early Warning service provides timely notifications about potential security issues, including known vulnerabilities, and malicious activities affecting users' networks. All UK organisations can sign up to this free service.

The three China-based technology companies provide cyber-related services to the Chinese intelligence services and are part of a wider commercial ecosystem in China, which includes information security companies, data brokers and hackers for hire.

The named entities are: Sichuan Juxinhe Network Technology Co Ltd, Beijing Huanyu Tianqiong Information Technology Co, and Sichuan Zhixin Ruijie Network Technology Co Ltd.

The NCSC has co-sealed this advisory alongside agencies from the United States, Australia, Canada, New Zealand, Czech Republic, Finland, Germany, Italy, Japan, the Netherlands, Poland and Spain.

It can be read here: https://media.defense.gov/2025/Aug/22/2003786665/-1/-1/0/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.PDF

PUBLISHED

27 August 2025

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector

Small & medium sized organisations

NEWS TYPE

Alert