

China-linked malicious actors called out by UK and international partners for targeting sensitive data globally

Joint advisory with international partners highlights exploitation and compromise of networks belonging to organisations across the globe.

- China-linked company Integrity Technology Group has been exposed by the UK and international partners for enabling cyber actors to target organisations worldwide.
- AI-enabled tools, large-scale botnets and hands-on exploitation techniques being used to compromise networks and steal sensitive data.
- Organisations are being urged to strengthen their cyber resilience and defend against this evolving threat.

A range of malicious cyber activities enabled by a China-linked technology company and the wider ecosystem poses a significant threat as the UK and international partners urge organisations to improve their defences.

Alongside eight international partners from six countries, the National Cyber Security Centre – a part of GCHQ – has issued a new advisory revealing how, Integrity Technology Group (Integrity Tech), a company based in China with links to the Chinese Government, has enabled malicious China-linked cyber actors to exploit and compromise networks belonging to organisations across the globe.

Malicious cyber actors, enabled by Integrity Tech, are uniquely using AI tools, such as automated scanning, alongside large-scale botnets and manual exploitation techniques to compromise and steal confidential data from companies around the world, including critical sectors.

Last year, the [UK government sanctioned Integrity Tech](#), alongside another China-based information security company for their part in heedless malicious cyber activity against the UK and its allies.

The advisory also highlights that the company employs individuals who support a range of malicious cyber activities and contribute to the wider Chinese cyber ecosystem, including developing tools for use and sale, acquiring and hosting infrastructure and compromising networks across the globe.

The activity in the advisory is reported to be consistent with campaigns also publicly known as Flax Typhoon, Ethereal Panda and Red Juliett among others.

The activity in the advisory is reported to be consistent with campaigns also publicly known as Flax Typhoon, Ethereal Panda and Red Juliett among others.

“ *The extensive malicious cyber activities, and services by Integrity Tech, that have been exposed today should be extremely concerning for all network defenders.*

The breadth of sectors that have been targeted across the globe demonstrate the extent of the threat and all organisations should take note of this warning and engage with NCSC advice and guidance.

We will continue to call out malicious actors and the malevolent ecosystem they operate in.

Paul Chichester, NCSC Director of Operations

”

Organisations are being urged to understand the threat and techniques used by these cyber actors and follow the mitigation advice to help defend against the activity highlighted in the advisory.

In September 2024, the NCSC alongside international partners, [exposed Integrity Tech as the operator of a substantial botnet](#), where a network of internet-connected devices are infected with malware and controlled to carry out cyber

attacks, and was utilised by advanced persistent threat group, Flax Typhoon.

Earlier this year, the NCSC alongside industry and 15 international partners from across nine countries [issued an advisory and guidance](#) highlighting how organisations can better defend against the cyber threat from covert networks.

The NCSC has co-sealed this new advisory alongside agencies from Australia, Canada, Japan, New Zealand, Spain and the United States.

It can be read on the FBI website: <https://www.ic3.gov/CSA/2026/261008.pdf>

PUBLISHED

8 October 2026

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector

NEWS TYPE

Alert