

Cyber agencies issue joint advice on defending against China-linked covert networks



The UK NCSC and 15 international partners published an advisory on covert networks of compromised devices used by China-linked actors to hide attacks. It offers mitigation guidance and warns of 'IOC extinction'.

- Covert networks, often built from compromised edge devices such as home routers and smart devices, disguise the origin of attacks.
- The advisory says most China-linked actors are believed to use these tactics, and that the networks are used at scale against critical sectors to steal data and keep persistent access.
- It warns of IOC extinction: indicators of compromise vanish as fast as they are found, so defenders need adaptive, intelligence-driven measures.
- The networks are said to be created and maintained externally by Chinese information security

companies.

- One recommended step is to map and baseline edge device traffic, especially VPN and remote access, and use dynamic threat feed filtering.

The UK's National Cyber Security Centre (NCSC), part of GCHQ, has published a joint advisory with industry and 15 international partners on how to defend against covert networks. It was released on the second day of the CYBERUK 2026 conference.

What the advisory says

Covert networks are typically made up of vulnerable everyday internet-connected edge devices, such as home routers and smart devices, that have been compromised. Attackers use them to obscure where an operation really comes from and to avoid attribution. According to the advisory, these networks are used at scale to target critical sectors worldwide, steal sensitive data and maintain persistent access.

The authors describe a deliberate shift by China-based groups towards these networks, and say they are created and maintained externally by Chinese information security companies. The source recalls that in September 2024 the NCSC and partners named Integrity Technology Group as controlling a botnet used by Flax Typhoon, and that the UK government sanctioned the company in December 2025.

Why it matters for defenders

The advisory highlights IOC extinction: indicators of compromise disappear as quickly as they are discovered, so static blocklists lose value. It calls for more adaptive, intelligence-driven measures. Its executive summary advises organisations to map and baseline edge device traffic, especially VPN and remote access connections, and to adopt dynamic threat feed filtering that includes known covert network indicators.

For wider resilience, the NCSC points small organisations to its free Cyber Action Toolkit, and larger ones to Cyber Essentials certification and the updated Cyber Assessment Framework.

The advisory is co-sealed by agencies from Australia, Canada, Germany, Japan, the Netherlands, New Zealand, Spain, Sweden and the United States.

What to do now

1. Inventory edge devices (routers, VPN gateways, remote access appliances) and baseline their normal traffic so deviations stand out.
2. Review VPN and remote access logs for connections from residential or consumer-grade addresses that do not fit expected user behaviour.
3. Move from static IOC blocklists towards dynamic threat feed filtering that includes covert network indicators.

4. Patch, harden and retire unsupported edge devices, and remove unnecessary management exposure to the internet.
5. Read the full advisory and executive summary on the NCSC website and map its mitigations to your NCA ECC and SAMA CSF controls.
6. Ask managed service and threat intelligence providers how they handle fast-changing indicators.