Executive Summary: Defending against China-nexus covert networks of compromised devices

What is the threat?

- China-nexus cyber actors have moved from using individually procured infrastructure to operating large scale "covert networks" – botnets built from compromised routers, and other edge devices.

- These networks are used for each phase of the Cyber Kill Chain, from reconnaissance and malware delivery, to command and control and data exfiltration against targets of espionage and offensive cyber operations.

- The threat is a dynamic, low-cost, deniable infrastructure model that can be rapidly re-shaped, rendering traditional static IP block lists ineffective.

What is the impact on affected organisations?

- Covert networks enable China-nexus actors to launch cyber attacks against UK organisations, stealing sensitive data and potentially disrupting critical services.

- Because the covert networks are constantly refreshed and share nodes across multiple threat groups, defenders face "IOC extinction" – indicators of compromise disappear as quickly as they are discovered.

- Consequently, organisations that rely solely on static defences risk being bypassed, while those that adopt adaptive, intelligence driven measures can better mitigate the risk.

https://www.ncsc.gov.uk/news/executive-summary-defending-against-china-nexus-covert-networks-of-compromised-devices

23 April 2026

What should I do?

- The NCSC and the Cyber League, in conjunction with the co-sealing agencies, have developed advice specifically to combat this threat.
- The advisory contains guidance for small, medium, and large organisations.
- All organisations should map and baseline their edge device traffic, especially VPN and remote access connections, and adopt dynamic threat feed filtering that includes known covert network indicators.
- Potential victims should implement two-factor authentication for remote access and, where possible, apply zero trust controls, IP allow lists, and machine certificate verification.
- Larger or high-risk entities should consider active hunting of suspicious SOHO/IOT traffic, geographic profiling, and machine learning based anomaly detection.

Conclusion

- Promptly applying the recommended mapping, baseline, and zero trust measures is essential to reduce organisation exposure to China-nexus covert network attacks and to protect critical assets.

https://www.ncsc.gov.uk/news/executive-summary-defending-against-china-nexus-covert-networks-of-compromised-devices

23 April 2026