

Covert networks of compromised devices: joint advisory on defending against China-nexus actors



NCSC-UK and partner agencies report that China-nexus actors now route activity through large networks of compromised devices, mainly SOHO routers and IoT. Static IP blocklists lose value; the advisory sets out layered defences.

- China-nexus actors have shifted from individually procured infrastructure to large, externally provisioned networks of compromised devices.
- The networks consist mostly of SOHO routers, plus IoT devices, firewalls and NAS devices; end-of-life edge devices were a key weakness.
- Actors use them in every phase of an attack, from reconnaissance to data exfiltration, and one network may serve several actors.
- Because nodes change constantly, static malicious-IP blocklists are less effective.

- Advice is tiered by organisation size and risk, from edge-device mapping and MFA to active hunting.

What has changed

NCSC-UK, together with agencies from Australia, Canada, Germany, Japan, the Netherlands, New Zealand, Spain, Sweden and the United States, reports a major shift in how China-nexus actors operate. Instead of buying their own infrastructure, most now use large networks of compromised devices, which the advisory calls covert networks. They are made up mainly of Small Office Home Office (SOHO) routers, along with IoT and smart devices.

The advisory names Volt Typhoon, which used such networks to pre-position capabilities on critical national infrastructure, and Flax Typhoon, which used a different one for espionage. It cites Raptor Train, which infected more than 200,000 devices in 2024, and the KV Botnet, built largely on vulnerable end-of-life Cisco and NetGear routers.

Why it matters for defenders

Traffic typically enters through an on-ramp node, passes through several compromised traversal nodes and leaves from an exit node, usually in the target's own region. Attacks can therefore appear to come from ordinary domestic devices. Because the networks change constantly and may serve several actors, static IP blocklists become less effective.

What the advisory recommends

All organisations should map their edge devices, baseline normal connections to VPNs, use dynamic threat feeds covering covert networks and enforce multi-factor authentication for remote access. Higher-risk organisations should consider allow lists, zero trust, machine certificates and a smaller internet-facing footprint. The most exposed should hunt actively and track covert networks as threat actors in their own right. The advisory notes these steps do not remove all risk.

What to do now

1. Inventory all network edge devices (routers, firewalls, NAS, cameras) and retire or replace end-of-life models.
2. Baseline legitimate VPN and remote-access sources and review connections from consumer broadband ranges.
3. Enforce multi-factor authentication on all remote access.
4. Subscribe to dynamic threat feeds that include covert network infrastructure and replace reliance on static blocklists.

5. For high-risk systems, apply allow lists, zero trust and machine certificates for VPN connections, and reduce internet-facing services.
6. Where capability exists, hunt for connections from SOHO or IoT address ranges and track reported covert networks.