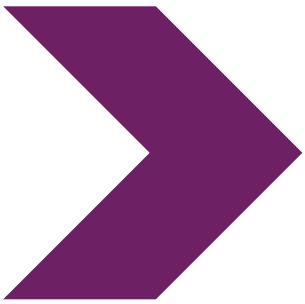
Advisory

Defending against China-nexus covert networks of compromised devices



23 April 2026

National Cyber Security Centre
a part of GCHQ

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

BND

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Verfassungsschutz

国家サイバー統括室
National Cybersecurity Office

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
NEW ZEALAND

Defending against China-nexus covert networks of compromised devices

Explaining the widespread shift in tactics, techniques and procedures (TTPs) towards networks of compromised infrastructure, and how to defend against it

Summary

With support from the UK Cyber League, this advisory has been jointly released by the National Cyber Security Centre (NCSC-UK) and international partners:

- Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC)
- Communications Security Establishment Canada's (CSE's) Canadian Centre for Cyber Security (Cyber Centre)
- Germany Federal Office for the Protection of the Constitution - Bundesamt für Verfassungsschutz (BfV)
- Germany Federal Intelligence Service – Bundesnachrichtendienst (BND)
- Germany Federal Office for Information Security - Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Japan National Cybersecurity Office (NCO) - 国家サイバー統括室
- Netherlands General Intelligence and Security Service - Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
- Netherlands Defence Intelligence and Security Service - Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
- New Zealand National Cyber Security Centre (NCSC-NZ)
- Spain National Cryptologic Centre – Centro Criptológico Nacional (CCN)
- Sweden National Cyber Security Centre - Nationellt cybersäkerhetscenter (NCSC-SE)
- United States Cybersecurity and Infrastructure Security Agency (CISA)
- United States Department of Defense Cyber Crime Center (DC3)
- United States Federal Bureau of Investigation (FBI)
- United States National Security Agency (NSA)

Its purpose is to provide network defenders with the tools needed to defend against China-nexus cyber actors and their tactic of using large scale networks of compromised devices (covert networks) to route their cyber activity.

Introduction

Over the past few years there has been a major shift in the tactics, techniques and procedures (TTPs) used by China-nexus cyber actors, moving away from the use of individually procured infrastructure, and towards the use of externally provisioned, large-scale networks of compromised devices.

The NCSC believes that the majority of China-nexus threat actors are using these networks (hereafter "covert networks"), that multiple covert networks have been created and are being constantly updated, and that a single covert network could be being used by multiple actors. These networks are mainly made up of compromised Small Office Home Office (SOHO) routers, as well as Internet of Things (IoT) and smart devices.

Anyone who is a target of China-nexus cyber actors may be impacted by the use of covert networks. They have been used by Chinese state-sponsored actors Volt Typhoon to pre-position offensive cyber capabilities on critical national infrastructure. The group Flax Typhoon used a different covert network of compromised infrastructure to conduct cyber espionage.

The use of covert networks of compromised devices - also known as botnets - to facilitate malicious cyber activity is not new, but China-nexus cyber actors are now using them strategically, and at scale.

This advisory describes the typical makeup of a covert network and what they are being used for. It also includes protective advice for organisations being targeted by cyber activity using a covert network as an access vector.

Covert Networks

Covert networks are used to connect across the internet in a low-cost, low-risk, deniable way, disguising the origin and attribution of malicious activity. Actors have been observed using them for each phase of their Cyber Kill Chains, from performing scans as part of reconnaissance, to the delivery of malware, communicating with said malware, and exfiltrating stolen data from a victim. They can also be used for general deniable internet browsing, allowing threat actors to research exploitation techniques, new TTPs, and their victims without attribution. Some covert networks are also used by legitimate customers to browse the internet, making it challenging to attribute malicious activity.

There is evidence that covert networks used by China-nexus actors are created and maintained by Chinese information security companies. A network known to network defenders as Raptor Train, which in 2024 infected more than 200,000 devices worldwide, was controlled and managed by the Chinese company, Integrity Technology Group. This company was also assessed by the FBI to be responsible for the computer intrusion activities attributed to China-based hackers known as Flax Typhoon.

"Botnet operations represent a significant threat to the UK by exploiting vulnerabilities in everyday internet-connected devices with the potential to carry out large-scale cyber attacks" – NCSC Director of Operations, Paul Chichester

Covert networks mostly consist of compromised SOHO routers, but they also pull in any vulnerable device they can exploit at scale. Raptor Train was made up of thousands of SOHO routers and IoT devices, such as web cameras and video recorders, as well as firewalls and Network Attached Storage (NAS) devices. The KV Botnet used by Volt Typhoon was mainly made up of vulnerable Cisco and NetGear routers. The edge devices were vulnerable because they were "end of life" – out of date and no longer receiving updates or security patches by their manufacturers.

The cyber security industry has been aware of examples of these networks for some time and has publicly reported on the widespread scale of the threat and its implications. Mandiant Intelligence produced a public blog in May 2024 talking about covert networks in which they highlighted a key issue for defenders – indicator of compromise (IOC) Extinction. If a particular threat group could now

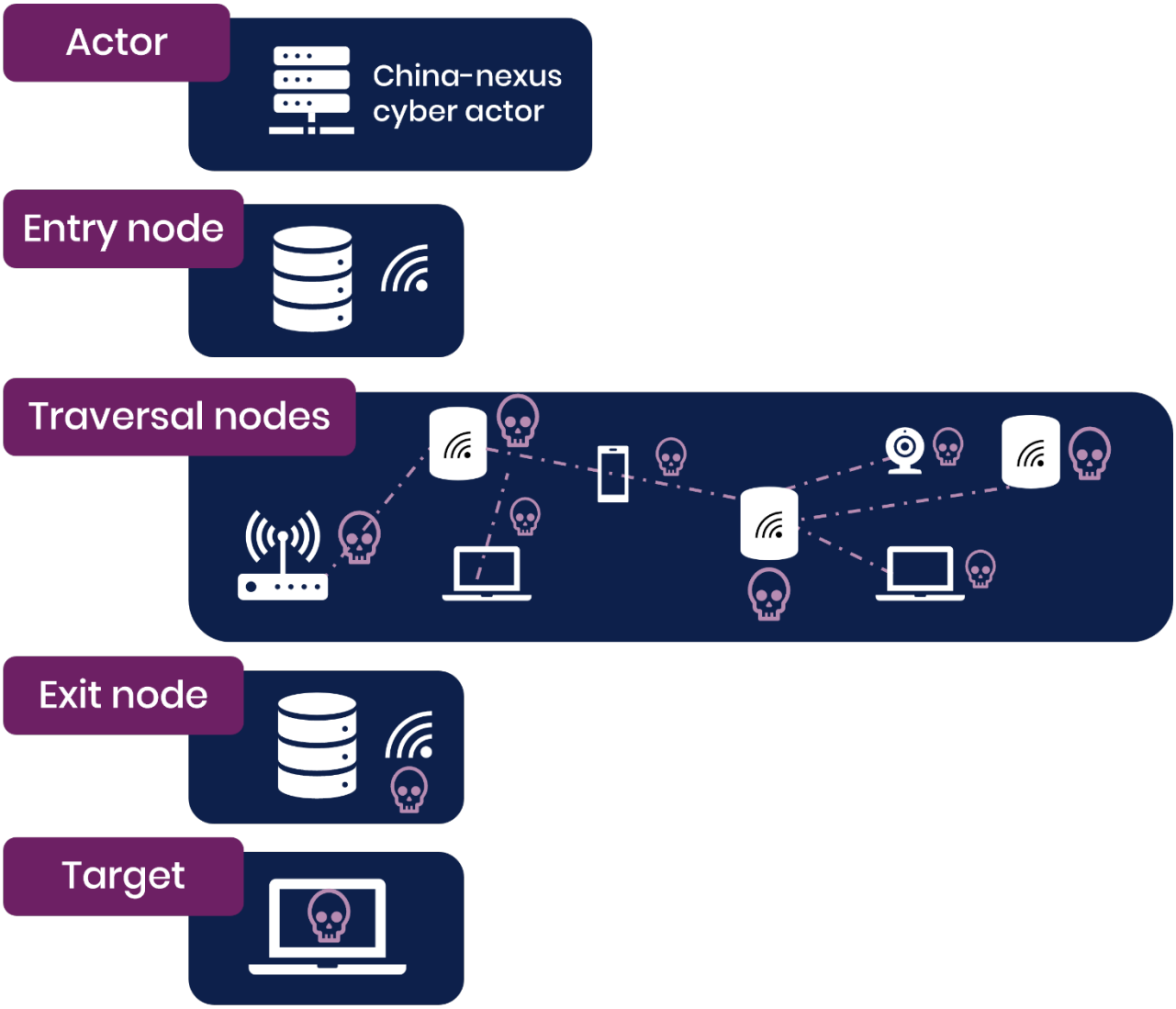
come from one of many covert networks, each with potentially hundreds of thousands of endpoints, and each used by multiple threat actors, old network defence paradigms of static malicious IP block lists will be less effective. This is compounded by the dynamic nature of these networks where new nodes will be added as old devices are patched or removed from use.

Typical Network Topology

The number of covert networks used by China-nexus cyber actors is large, with new networks regularly developed and deployed. The existing covert networks change too, either because of defensive or legal action, or simply as a result of software updates and new exploits being used to target different technologies for incorporation into the network.

Because of this, a description of all known covert networks in detail, including how they are constructed and how they communicate, would immediately be out of date – and for most network defenders would not be practically useful.

However, most covert networks of compromised devices use the same basic set up. Understanding this generalised structure can aid researchers and defenders by helping them to understand which part of a network they may have found, and how to defend against it.



A diagram illustrating the basic setup of a covert network.

The diagram above illustrates the basic setup of a covert network, where typically an actor will connect to the network via an on-ramp or entry node. Their traffic will be forwarded through multiple compromised devices, used as traversal nodes, before exiting the network from an exit node, usually in the same geographic region as the target.

Protective Advice

Defending from attackers using covert networks is not straightforward, and defensive tactics will be different based on the levels of resource and the nature of the target organisation. General advice for good cyber security practice should be followed, and some key messages can be found in the appendix of this advisory.

The following advice is specifically tailored to steps which can be taken to combat the risk of attacks coming from large, dynamic networks of compromised devices.

Further guidance for all organisations facing cyber security threats is available on the NCSC website.

This guidance should be considered alongside all applicable laws and regulations of the UK and co-sealing countries relating to the security of networks and data. It will be each organisation's responsibility to ensure compliance with any such laws and regulations. Organisations should note that following the recommended actions set out below will not remove all risks.

All organisations

The NCSC recommends the following steps for all affected organisations to either take themselves, or ask their managed service and/or security providers to investigate for them:

- Map and understand network edge devices, developing a clear understanding of organisational assets and what should be connecting to them.
- Baseline normal connections, especially to corporate virtual private networks (VPNs) or other similar services.
    - Would you expect connections from consumer broadband ranges?
- Leverage available dynamic threat feeds which include covert network infrastructure.
- Implement multi-factor authentication for remote connections.

Smaller organisations should consider creating and actioning a free NCSC Cyber Action Toolkit.

Larger or more at-risk organisations

Some more comprehensive measures may be appropriate if the risk to an organisation is high enough, to be conducted either in-house or through a security provider:

- Apply IP address allow lists rather than deny lists for connections to corporate VPNs for remote workers.
- Use geographic allow lists or profile incoming connections based on operating system, time zones, and/or organisation specific system configuration settings.
- Implement zero trust policies for connections.
- Enforce machine certificates for Secure Sockets Layer (SSL) connections.
- Reduce the internet-facing presence of the IT estate.
- Investigate machine learning techniques to profile normal network edge activity to detect and block anomalies.

The NCSC's Cyber Essentials can help protect organisations of all sizes.

Largest or most at-risk organisations

If Advanced Persistent Threat (APT) tracking is part of an organisation's in-house capability, or if it is part of the service provided by a security vendor, consider tracking China-nexus covert networks as APTs in their own right.

- Active hunting – look for connections from IP addresses likely to be part of a covert network of compromised devices, for instance those hosting SOHO routers or IoT devices.
- Track and map covert networks reported by industry or government by looking at banners and certificates.
- Use threat reporting and threat feeds to create and implement dynamic blocklists and create alert rules to detect incoming threats.
- Consider using NetFlow feeds to look upstream and map covert networks to find new nodes.

The NCSC Cyber Assessment Framework provides guidance for organisations under the highest levels of threat, including those operating essential services, in sectors such as energy, healthcare, transport, digital infrastructure and government.

MITRE ATT&CK®

This advisory has been compiled with respect to the MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

Tactic	ID	Technique	Procedure
Resource Development	T1584.005	Compromise Infrastructure: Botnet	Botnets are used as core components of covert networks
Resource Development	T1584.008	Compromise Infrastructure: Network Devices	Devices are compromised and added to botnets
Resource Development	T1583.003	Acquire Infrastructure: Virtual Private Server	Virtual private servers (VPS) are used in covert networks, typically as on-ramps
Command and Control	T1090.003	Proxy: Multi-hop Proxy	Used by China-nexus cyber actors to route traffic

Appendix: Cyber Security Best Practices

In addition to the protective advice outlined in this advisory, a number of cyber security best practices will also be useful in defending against the activity described in this advisory.

- **Protect your devices and networks by keeping them up to date**: use the latest supported versions, apply security updates promptly, use antivirus and scan regularly to guard against known malware threats. See NCSC Guidance: https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/antivirus-and-other-security-software

- **Prevent and detect lateral movement in your organisation's networks**. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/preventing-lateral-movement

- **Implement architectural controls for network segregation**. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/10-steps-network-security

- **Set up a security monitoring capability** so you are collecting the data that will be needed to analyse network intrusions. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes and https://www.ncsc.gov.uk/information/logging-made-easy

- **Use modern systems and software.** These have better security built-in. If you cannot move off out-of-date platforms and applications straight away, there are short term steps you can take to improve your position. See NCSC Guidance: https://www.ncsc.gov.uk/collection/mobile-device-guidance/managing-the-risks-from-obsolete-products

- **Restrict intruders' ability to move freely around your systems and networks**. Pay particular attention to potentially vulnerable entry points such as third-party systems with onward access to your core network. During an incident, disable remote access from third-party systems until you are sure they are clean. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/preventing-lateral-movement and https://www.ncsc.gov.uk/guidance/assessing-supply-chain-security.

- **Deploy a host-based intrusion detection system**. A variety of products are available, free and paid-for, to suit different needs and budgets.

- **Further information**: Invest in preventing malware-based attacks across various scenarios. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

Disclaimer

This report draws on information derived from NCSC and industry sources. Any NCSC findings and recommendations made have not been provided with the intention of avoiding all risks and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favouring by co-sealers. UK readers should refer to the NCSC website for information about NCSC assured services.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation.

Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.