Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR CYBER SECURITY

People's Republic of China cyber threat activity

PRC cyber actors target telecommunications companies as part of a global cyberespionage campaign

Cyber threat bulletin

D96-129/2025E-PDF
ISBN 978-0-660-77867-9

Introduction

The Canadian Centre for Cyber Security (Cyber Centre) and the United States' Federal Bureau of Investigation (FBI) are warning Canadians of the threat posed by People's Republic of China (PRC) state-sponsored cyber threat actor tracked in industry reporting as Salt Typhoon. The Cyber Centre previously joined our partners in warning that PRC cyber actors have compromised networks of major global telecommunications providers to conduct a broad and significant cyber espionage campaign. This cyber bulletin aims to raise awareness of the threat posed by PRC cyber threat activity, particularly to Canadian telecommunications organizations, in light of new Salt Typhoon-related compromises of entities in Canada.

The threat to Canadian organizations

The Cyber Centre is aware of malicious cyber activities currently targeting Canadian telecommunications companies. The responsible actors are almost certainly PRC state-sponsored actors, specifically Salt Typhoon.

Three network devices registered to a Canadian telecommunications company were compromised by likely Salt Typhoon actors in mid-February 2025. The actors exploited CVE-2023-20198 to retrieve the running configuration files from all three devices and modified at least one of the files to configure a GRE tunnel, enabling traffic collection from the network.

In separate investigations, the Cyber Centre has found overlaps with malicious indicators associated with Salt Typhoon, reported by our partners and through industry reporting, **which suggests that this targeting is broader than just the telecommunications sector.** Targeting of Canadian devices may allow the threat actors to collect information from the victim's internal network, or use the victim's device to enable the compromise of further victims. In some cases, we assess that the threat actors' activities were very likely limited to network reconnaissance.

While our understanding of this activity continues to evolve, we assess that PRC cyber actors will almost certainly continue to target Canadian organizations as part of this espionage campaign, including telecommunications service providers and their clients, over the next two years. To monitor and mitigate this threat, we encourage Canadian organizations to consult the guidance linked below on hardening networks, security considerations for edge devices, and additional cyber threat information pertaining to the PRC.

The threat to telecommunications

Telecommunications networks are almost certainly among the highest priority espionage targets for state-sponsored cyber threat actors. Hostile state actors very likely rely on access to telecommunications service providers (TSPs) and telecommunications networks around the world as a key source of foreign intelligence collection. TSPs carry telecommunications traffic and collect and store large amounts of customer data that have intelligence value, including communication, location, and device data.

State-sponsored cyber threat actors have persistently compromised TSPs globally, often as part of broad and long-running intelligence programs to exfiltrate bulk customer data and collect information on high-value targets of interest, such as government officials. This includes geolocating and tracking individuals, monitoring phone calls, and intercepting SMS messages. State actors have gained access to telecommunications networks and data by exploiting vulnerabilities in network devices, such as routers, and by taking advantage of insecure design in the systems that route, bill, and manage communications.

In 2024, partner investigations discovered that PRC state-sponsored cyber threat actors had compromised the networks of major global TSPs, including US wireless carriers, very likely as part of a targeted espionage operation. According to our partners, the actors were able to steal customer call records data from the compromised TSPs. The threat actors also collected the private communications of a limited number of individuals primarily involved in government or political activity.

We are also concerned with the potential impacts to the sensitive information of client organizations working directly with telecommunications providers. PRC cyber threat actors frequently attempt to compromise trusted service providers, including telecommunications, managed service providers and cloud service providers, to access client information or networks indirectly.

PRC cyber actors exploit vulnerabilities in edge devices

As we note in the National Cyber Threat Assessment 2025-2026, cyber threat actors are exploiting vulnerabilities in security and networking devices that sit at the perimeter of networks, including routers, firewalls, and virtual private network (VPN) solutions. By compromising these edge devices, a cyber threat actor can enter a network, monitor, modify, and exfiltrate network traffic flowing through the device, or possibly move deeper into the victim network.

As part of this campaign, PRC cyber actors are targeting these network devices, exploiting existing vulnerabilities to gain and maintain access to TSPs. Despite public reporting outlining their activities, it is very likely that the actors continue to operate.

Useful resources

Refer to the following online resources for more information and useful advice and guidance.

Reports and advisories

- Canada's threat assessments
  - National Cyber Threat Assessment 2025-2026
- Advisories and partner publications
  - Enhanced Visibility and Hardening Guidance for Communications Infrastructure
  - Cyber threat bulletin: Cyber Centre urges Canadians to be aware of and protect against PRC cyber threat activity

Advice and guidance

- Cyber Security Readiness Goals (CRGs): Securing Our Most Critical Systems
- Cross-Sector Cyber Security Readiness Goals Toolkit
- Security Considerations for Edge Devices
- Joint guidance on enhanced visibility and hardening for communications infrastructure - Canadian Centre for Cyber Security
- People's Republic of China activity targeting network edge routers: Observations and mitigation strategies