



Cyber threat bulletin: Cyber Centre urges Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity



The Canadian Centre for Cyber Security encourages the Canadian cybersecurity community—especially critical infrastructure network defenders—to bolster their awareness of and protection against Russian state-sponsored cyber threats. The Cyber Centre joins our partners in [the US](#) and [the UK](#) in recommending proactive network monitoring and mitigations.

Canada's Cyber Centre, part of the Communications Security Establishment, is aware of foreign cyber threat activities, including by Russian-backed actors, to target Canadian critical infrastructure network operators, their operational and information technology (OT/IT). The advisory issued by our US partners usefully highlights vulnerabilities known to have been exploited by Russian cyber threat actors, as well as information about their tactics, techniques and procedures (TTPs).

The Cyber Centre urges Canadian critical infrastructure network defenders to:

- Be prepared to isolate critical infrastructure components and services from the internet and corporate/internal networks if those components would be considered attractive to a hostile threat actor to disrupt. When using industrial control systems or operational technology, conduct a test of manual controls to ensure that critical functions remain operable if the organization's network is unavailable or untrusted.
- Increase organizational vigilance. Monitor your networks with a focus on the TTPs reported in the [CISA advisory](#) (link available in English only). Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior. Enable logging in order to better investigate issues or events.
- Enhance your security posture: Patch your systems with a focus on the vulnerabilities in the [CISA advisory](#) (link available in English only) enable logging and backup. Deploy network and endpoint monitoring (such as anti-virus software), and implement multifactor authentication where appropriate. Create and test offline backups.
- Have a cyber incident response plan, a continuity of operations and a communications plan and be prepared to use

them.

- Inform the Cyber Centre of suspicious or malicious cyber activity.

overlay
(escape
key)

Please refer to the following on-line resources for more information and for useful advice and guidance:

Threat detection and mitigation:

- [Destructive malware targeting Ukrainian organizations](#). Microsoft Threat Intelligence Center (MSTIC). January 15, 2022
- [Joint Cybersecurity Advisory: Technical Approaches to Uncovering and Remediating Malicious Activity](#)
- [Secure your accounts and devices with multi-factor authentication \(ITSAP.30.030\)](#)
- [Security considerations for your website \(ITSM.60.005\)](#)
- [Security considerations for industrial control systems \(ITSAP.00.050\)](#)
- [Top 10 IT security actions to protect Internet connected networks and information \(ITSM.10.089\)](#)
- [Security Vulnerabilities and Patches Explained - IT Security Bulletin for the Government of Canada \(ITSB-96\)](#)

Threat assessment:

- [National Cyber Threat Assessment 2020](#)
- [Cyber Threat Bulletin: The Cyber Threat to Operational Technology](#)
- [Cyber Threat Bulletin: The Cyber Threat to Canada's Electricity Sector](#)

Planning

- [Public Safety Canada guide](#)
- [Ransomware playbook \(ITSM.00.099\)](#)


You can find more helpful advice and guidance within the [information and guidance](#) section of our website or by subscribing to our [social media feeds](#).

Close

Please [contact us](#) for additional advice and guidance or to [report an incident](#).

Email: contact@cyber.gc.ca

Toll Free: 1-833-CYBER-88 (1-833-292-3788)

 Share this page

Date modified:

2022-01-26