Statement on People's Republic of China reconnaissance of Canadian systems - Canadian Centre for Cyber Security

Archived: 2026-04-05 15:30:45 UTC

The Canadian Centre for Cyber Security The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability. (Cyber Centre), a part of the Communications Security Establishment Canada (CSE), is urging Canadian organizations to remain vigilant and bolster their defences against reconnaissance Activity conducted by a threat actor to obtain information and identify vulnerabilities to facilitate future compromise(s). scanning, a low-level but constant cyber threat A threat actor, using the internet, who takes advantage of a known vulnerability in a product for the purposes of exploiting a network and the information the network carries. facing the country.

The Cyber Centre is aware that a sophisticated state-sponsored threat actor from the People’s Republic of China has performed broad based reconnaissance scanning over several months against numerous domains in Canada. While we observe reconnaissance scanning on a near-constant basis, this widespread activity from a sophisticated threat actor against multiple organizations across multiple sectors is an opportunity to increase awareness of the potential threats facing Canadian organizations and share simple steps everyone can take to protect against them.

These reconnaissance scans have occurred throughout 2024. The majority of affected organizations targeted were Government of Canada departments and agencies, and includes federal political parties, the House of Commons and Senate. They also targeted dozens of organizations, including democratic institutions, critical infrastructure Processes, systems, facilities, technologies, networks, assets, and services essential to the health, safety, security, or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories, and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence. , the defence sector, media organizations, think tanks and NGOs.

It’s important to understand what exactly these scans are.

Reconnaissance scanning is not an indication of compromise The intentional or unintentional disclosure of information, which adversely impacts its confidentiality, integrity, or availability. . It is used to gather information, look for possible vulnerabilities, and may be a precursor to further malicious actions. It is the equivalent of someone walking around a building to see if there is an alarm or security camera, or trying the windows and doors to see which ones are unlocked. It is about gathering information in case they want to return to carry out a crime and figuring out the best way to do it.

We strongly recommend you defend against reconnaissance scans by following cyber security best practices, such as the Cyber Centre’s Top 10 IT Security Actions. Threat actors often take advantage of unpatched systems.

Organizations can protect themselves by ensuring they have updated their operating systems and applications to protect against all known vulnerabilities.

Other important measures you can take:

- Implement multi-factor authentication
- Increase logging to check for suspicious activity
- Educate your employees about phishing and how to spot fraudulent emails and text messages

For more information on the scale and scope of this threat, please see our PRC cyber threat bulletin.

To learn about the cyber threats to civil society organizations and how to protect yourself, please see our joint cyber security advisory on mitigating cyber threats with limited resources.

The Cyber Centre offers a range of advice and guidance, including on how to protect your personal accounts.

For more on vulnerabilities, you can visit the Cyber Centre's Alerts and advisories page.

For more on best practices, please visit the Cyber Centre's Guidance page.
