Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY | NATIONAL CYBER THREAT ASSESSMENT 2018

# STATE-SPONSORED ESPIONAGE AND THREATS TO CRITICAL INFRASTRUCTURE

Critical infrastructure includes the networks and systems that Canadians rely on for essential services and resources every day, such as our energy, water and utility systems, transportation systems, food supply chains and financial networks.

State-sponsored threat actors conduct cyber espionage against critical infrastructure in Canada and other allied nations. This includes reconnaissance and intelligence-gathering in the energy, aerospace and defence sectors. Public institutions are also attractive targets because they hold personal information, valuable research data and other sensitive information. It is expected that state-sponsored threat actors will continue to conduct espionage against Canadian businesses and critical infrastructure to advance their national strategic objectives.

*Canada's critical infrastructure sectors*

Food | Water | Energy and Utilities | Government | Information & Communication | Safety | Manufacturing | Health | Transportation | Finance

Cyber threat activity against Canada's critical infrastructure can have severe and far-reaching consequences. The proliferation of malicious cyber tools, along with the increasingly interconnected nature of industrial equipment and systems, means less sophisticated cyber threat actors may interfere, even inadvertently, with Canada's critical infrastructure.

## WHAT IS THE GOVERNMENT OF CANADA DOING?

One of the important objectives of the new Canadian Centre for Cyber Security is to work collaboratively with Canada's critical infrastructure owners and operators, as well as all levels of government, private industry and academia to combat these ever evolving cyber threats. These strategic partnerships will enhance information sharing, integrate cyber defence technology and help strengthen Canada's cyber resiliency.

In support of these goals, last year CSE publicly released one of its malware detection and analysis tools, known as *Assemblyline*. This tool has been used nationally and internationally to automate malware detection and support the work of cyber security analysts in many sectors.

The proposed Bill C-59: *An Act Respecting National Security*, would allow the CSE and the Cyber Centre to more extensively share information about specific cyber threats with owners and operators of Canada's critical infrastructure and provide operational and technical assistance to help protect these networks, if requested.

**In 2017, the Communications Security Establishment (CSE) alerted partners in the United States to a cyber compromise affecting the energy sector. In this case, foreign cyber threat actors gained access to secure and isolated systems to the point where the state sponsored threat actor could have disrupted power flows.**

## TOP TIPS FOR CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS

- Implement application whitelisting
- Isolate web-facing applications
- Apply protection at the host level
- Protect information at the enterprise level
- Consolidate, monitor and defend internet gateways
- Patch operating systems and applications
- For more go to cyber.gc.ca

Canada