Cyber Threat Intelligence Report

State-Sponsored Cyber Threat Actors

Cybersecurity Division
Compiled by Tasha-Gaye Braham

Date: 21 December 2022

Summary of Threat

In today's age, the number of internet users is climbing each day. According to Statistics Canada, 75% of Canadians aged 15 years and older engage in various internet-related activities more often since the onset of the pandemic. The usage of technology in the corporate world has also increased since COVID-19, and while we are post-pandemic, there are no signs of that decreasing. In this report we detail threats which are impacting Canadians through state-sponsor cyber threat activities, based on the *National Cyber Threat Assessment* by the Canadian Centre for Cyber Security [CCCS]. The increase in technology usage, including the high-volume use of cloud computing, has made Canadians' valuable information vulnerable, due to risks such as cloud servers potentially being located outside of Canada's borders. These changes in technology use increases the likelihood that threats against Canadians will be carried out by state-sponsored cyber threat actors.

State-sponsored cyber threat actors are cybercriminals working on behalf of nation-states. These groups are usually the most sophisticated cybercriminals, as they have access to dedicated resources, the best cybercriminal personnel, extensive budgets, and time. The state-sponsored cyber threat actors detailed in the National Cyber Threat Assessment as targeting Canadians were shown to come primarily from China, Iran, and Saudi Arabia.

How state-sponsored threat actors target Canadians using cyber means can vary greatly. Below we will explore some methods that are known to be used.

Weaponizing Disaffected Groups and Activists in Canada

State-sponsored groups often target Canadians who may be sympathetic to their cause, like activists and members of specific groups (such as ethnic or religious groups), who are located in various geographic locations across the country or world. These state groups include resource heavy, skilled individuals who utilize content monitoring, social media campaigns, intelligence gained from spyware, and other cyber threat vectors in an effort to monitor Canadians' online presence to identify the groups they associate with and their stance on and involvement in activism.

According to reports from *The Citizen Lab* at the University of Toronto, "cyber threat activity targets activists in Canada through disinformation or intimidation on social media, denial of service attacks against their organizations, and compromise of their personal devices" (CCCS, 2022, p. 13).

State-sponsored attackers with highly sophisticated attack methods and governments behind them, are able to gain access to monitor, track, and compromise the privacy of Canadians. This is accomplished through a number of different means such as:

- the group accessing large databases of personal information and using data science to identify, profile, and track individuals;
- foreign states compelling private organization to supply personal data, which threaten the privacy of Canadians; and
- the target having a lack of appropriate safeguards, through which Personal Identifiable Information [PII] can be compromised.

Compromising Canadians via Worldwide Campaigns

State-sponsored threat actors are attempting to compromise Canadians in worldwide, widespread campaigns by taking advantage of zero-day vulnerabilities. A zero-day vulnerability is an unpatched but known vulnerability in a software program. The state-sponsor's goal using this threat vector is to carry out widespread cyberattack campaigns, in hopes of stealing intellectual property and personal information.

Threat actors usually aim for software or programs that have widespread use around the world, such as a web browser or commonly used product. This is because a successful compromise will give them access to as many peoples' personal information or intellectual property as possible, which includes a great amount of Canadian data and PII. An example of this is the Microsoft Exchange server compromise, which affected an estimated 400,000 servers, and over 9,000 of these servers which are likely to have been vulnerable were Canadian servers.

Targeting Canada's Economic Value through Commercial Cyber Espionage

According to *Crowd Strike*, cyber espionage is a type of cyberattack in which an unauthorized user attempts to access sensitive or classified data or intellectual property for economic gain, competitive advantage, or for political reasons.

Commercial cyber espionage is a subset of cyber espionage and focuses on the unsanctioned access of confidential data or trade secrets related to commercial endeavours.

This can include the:

- exploitation of supply chain vulnerabilities;
- theft of Intellectual property;
- foreign intelligence operations;
- underhanded or secretive procurement of equipment or materials; and
- violation of export controls.

Using Tools to Obfuscate Activities and Avoid Attribution

Ransomware is used to carry out commercial cyber espionage as well. State-sponsored threat actors use ransomware to steal valuable information from corporations, and then demand a ransom to release back the information to the rightful owners. Sometimes ransomware also includes cybercriminals locking access to the data and information systems, holding access behind a ransom.

These threat actors also use techniques, tools, and procedures to cover their tracks so that organizations and individuals do not recognize it as an attack until the ransom is sent, making it difficult to determine the root cause or ascribe blame.

Focusing on Cyber Means to Raise Money

Cryptocurrency is the new "get rich quick" scheme that has flooded the world in recent years and cyberattackers have latched onto this as a means of gaining funds. For example, North Korean state-sponsored cyber threat actors have made a move to alleviate the impact of international economic sanctions by garnering financial support through malicious cryptocurrency trading applications. These malicious applications compromise users' credentials and allow the threat actors to access and steal the money the individual has linked to their cryptocurrency account.

Due to the newness of cryptocurrency and people not understanding the potential for these applications to be compromised, several individuals have fallen, and will continue to fall, victim to this type of cyberattack.

What is a zero-day vulnerability?

A zero-day vulnerability is a vulnerability in a system or device that has been disclosed but is not yet patched. (TrendMicro, 2022)

Assessment of Threats

Threat Activity Description	Issues	How is the GoA Affected?
Social Media Campaign – internet users use social media to connect with friends, family, and their communities. There is also the business side of social media, where professional networking takes place and companies and employees post company-related news and information. Cyber threat actors use social media to aid in gathering information about their targets.	According to Trend Micro researchers, "[p]osting on social media has become ubiquitous not just for people but also for businesses and governments around the world" (Gibson et al, 2022). Social media, when used for personal reasons, is intended to share personal moments. For organizations, social media is meant to aid with connecting and communicating with its users/ customers. Professionals use social media as a way to network and make money.	▪ The personal social media accounts of GoA officials can be monitored by threat actors for biometrics from photos, videos, audio recording, and other information that is posted. Information from social media can be used in an inference attack; this is a data mining technique where threat actors analyze available public data to gain knowledge about protected information, (e.g., piecing together public information from various sources to access protected data). ▪ Advertising, promoting, or informing users/customers about project initiation or completion on social media can expose critical information that threat actors can use to aid in attack against the organization.
Spyware is a malicious piece of software that finds its way onto our internet connected devices. It usually gets installed on our devices just by visiting a vulnerable web page or even through accepting terms and conditions without reading the fine print. This piece of software monitors everything we do on our devices, from websites we visit, to information we type into these websites to sensitive information.	State-sponsored cyber threat actors' use spyware tools to compromise personal and company devices. These threat actors have access to sophisticated, powerful tools which do not even require any additional actions from users, apart from visiting a website. Spyware is usually a small piece of software that is extremely hard to detect and uninstall from the infected device or system. State-sponsored threat actors can gain an enormous amount of classified data from users this way.	▪ Spyware downloads are usually obscured in the form of accepting user agreement policies/terms and condition. Once these policies are accepted, the spyware is downloaded to the system/ device, unbeknownst to the user. ▪ Pegasus is a spyware developed by the Israeli cyber arms company NSO group.
Zero-day vulnerabilities are unpatched vulnerabilities found in a vendor supplied application before security researchers, or software developers have a chance to build a security patch. Cyber threat actors can exploit these vulnerabilities prior to them being fixed.	According to DarkReading "Zero-Day Exploit Use Exploded in 2021" (Vijayan, 2022). Ransomware and other financially motivated threat actors joined nation-state-backed groups in leveraging unpatched flaws in attack campaigns, new data shows, aided by the increased use of Cloud applications, Internet of Things [IOT] devices, and Agile development.	▪ Zero-day exploits are out of the control of the organization using the application/software; however, there are ways to protect against falling victim of a zero-day exploit.

Threat Activity Description	Issues	How is the GoA Affected?
Commercial cyber espionage is a subset of cyber espionage and focuses on the unsanctioned access of confidential data or trade secrets related to commercial endeavours.	According to a CrowdStrike write up on cyber espionage, “target campaigns can be waged against individuals, such as prominent political leaders and government officials, and business executives” (Baker, 2022) Commercial espionage is usually conducted by state-sponsored threat actors, who use many different vectors to establish an undetected presence on networks as a means to steal sensitive data over time.	▪ Most commercial cyber espionage carried out by state-sponsored nations are well-funded. The vectors include, but are not limited to, zero-day exploits, spyware, ransomware, etc.
Ransomware is an ever-changing type of malware that cyber threat actors use to gain unauthorized access to and encrypt critical information, making it inaccessible for legitimate users. The threat actors then request a ransom be paid before providing a decryption key and releasing the information back to the users. Payment does not guarantee anything though, as the data is usually already breached and sometimes is not released upon receipt of the ransom payment.	According to the National Cyber Threat Assessment, “ransomware is almost certainly the most disruptive form of cybercrime facing Canadians” (CCCS, 2022, p. iv). This threat uses various threat vectors to find its way to the targets. No organization can fully protect against these threat vectors; however, they can put things in place to safeguard against them. State-sponsored actors will use ransomware to enable other malicious threat activities on governments and organizations while hiding their hands. Ransomware as a service (RaaS) creates an easier avenue to launch and profit from ransomware attacks, as it allows threat actors to hire professional hackers specializing in ransomware to complete the technical work.	▪ Ransomware usually enters a system through phishing, opening attachments, drive-by-downloading, or by taking advantage of software vulnerabilities.
Supply Chain Attacks are when cyber threat actors seek to cause damage and exploit an organization by attacking weaker elements in the supply chain to gain access and attack an organization.	Organizations use applications from different vendors (e.g., Microsoft, Adobe, Cisco, etc.) to complete their work. Cyber threat actors will often target these applications’ source codes, usually through application updates, to get the malicious code into the trusted applications. Government entities do not have the capability to develop complex in-house software. As a result, the government will continue to be dependent on supply chains, which are becoming more enticing for threat actors.	▪ The GoA uses products from a number of outside partners and providers, who have access to GoA systems as a result. Any companies that supply these third-party software/services are vulnerable to supply chain attacks. According to a CSO data breach report, “[n]ation-state actors have deep resources and the skills to penetrate even the most security-conscious firms” (Korolov, 2021). ▪ The GoA is dependent on multiple software vendors in order to operate effectively, so it is also at risk for supply chain attacks.

Recommendations

Use Strong Passwords

Passwords are one of the most popular methods used to protect digital information in today's world. Having a strong password is paramount as cybercriminals know that people only password protect things that are important, making passwords prime targets for their attacks. This is the same reason why car keys are popular targets for pickpockets. It isn't just about getting into the car or the system protected by the password, it is about what is stored inside, such as personal information, financial information, protected work documents, or access to other applications. Most people protect their car keys when they are out and passwords should be treated in the same way.

Some **DOs** and **DON'Ts** of creating strong passwords include:

Do	Don't
▣ Make them at least 12 characters long ▣ Use at least three of the following types of characters: ▣ upper case letters ▣ lower case letters ▣ numbers ▣ special characters ▣ Unicode characters ▣ Use a passphrase rather than a password	▣ Use the same password across different services or applications ▣ Share passwords with other people ▣ Write your passwords down ▣ Use the default password that comes with the device, service, or application ▣ Use passwords that are easy for a computer to guess (i.e., common words, pattern-based passwords, etc.)

We understand that we have just listed a bunch of rules that will help make your password more secure, but it also makes it harder to remember. This can be mitigated by creating your secure password or passphrase and using a password manager. KeePass is a GoA approved password manager that can manage your strong passwords without you having to remember all of them. There are other options, such as 1Password, NordPass, and Dashlane, that can be used for personal use as well!

For more information about creating strong passwords, please review the Cybersecurity Services eCourse on *Secure Passwords*.

Use Multi-factor Authentication

Multi-factor authentication [MFA], sometimes referred to as two-factor authentication or 2FA, is an additional layer of identity and access management security. MFA is used in conjunction with credentials, such as a username and password, when logging into an account. MFA falls into three categories:

What you know	What you have	Who you are
e.g., password, PIN	e.g., smart card, fob	e.g., facial scan, fingerprint

For credentials to be considered MFA, they need to be from two categories, such as something you know (a password) and something you have (Microsoft Authenticator on your cell phone).

MFA adds another level of security in the event of a compromised password. A threat actor would need to steal your cellphone and be able to access your Microsoft Authenticator app in order to gain access to your MFA protected accounts. As mentioned above, state-sponsored actors usually act remotely which limits their access to your physical devices. According to a 2015 Google survey, "[u]sing 2FA is one of the top three things that security experts do to protect their security online" (Ion, 2015, as cited in NIST, 2022).

The GoA uses MFA to protect the organization from state-sponsored attacks. MFA should be used whenever possible, especially on accounts which host the most sensitive or protected data, such as personal identifiable information, financial information, classified government information, etc. The most popular MFA authenticator apps are the Microsoft Authenticator and Google Authenticator apps. Some accounts offer MFA settings through sending a code via text message, email, or a phone call; however, it is recommended to use an MFA authenticator app over these other methods as it is the most secure.

MFA is required to access the GoA internal applications (i.e., an application that is not accessible by non-GoA users). An example of an internal application is 1GX. If a user's credentials are compromised and their 1GX account is breached, PII can be compromised and cause great damage to the organization and to the individuals impacted. MFA provides an additional layer of security that will prevent an attacker from accessing 1GX accounts, even if they have the credentials to the account. In the same way it can protect information in 1GX, MFA is also able to prevent data/account breaches on social media, banking, personal email and other personal accounts. It is highly recommended to enable MFA on all accounts with MFA options offered.

For more information about setting up MFA for your GoA account, please view the *GoA MFA Enrollment Portal*. For more details about the risks and benefits of using MFA, consider reviewing the MFA section of the *Secure Passwords* course.

Use Virtual Private Network

According to Surfshark, a virtual private network [VPN] "sets up a secure tunnel between two devices over the internet and encrypts your information. Encryption happens on your device before this data is forwarded to the VPN server. There, it is decrypted again and sent to its online destination" (Rimeikis, 2022). VPNs are especially important, when using home or public Wi-Fi, as these are the internet connections that are most vulnerable to cyber-attack. These types of connection do not usually have maximum security configurations applied.

VPNs do not prevent spyware from being downloaded onto your devices, but a VPN will protect your activities from being monitored. They are also able to hide your location from state-sponsored threat actors who are targeting Canadians. VPNs also protect the confidentiality of data being transmitted across networks, which protects information from eavesdropping whilst in transit.

Whenever using GoA provided devices, personal devices used for GoA business, or working on GoA materials the AnyConnect VPN is required to be used. As for personal use, a VPN is recommended for privacy protection. A few recommended personal VPN providers are Surfshark, Private Internet Access, CyberGhost, and NordVPN.

Use Secure Backups

Backing up your data securely is very important in case something goes wrong. This could be something as minor as accidentally deleting a file to the theft of a device to a calculated cyberattack. Data backups are useful because they allow for information to be restored in cases where the original is unavailable in some way.

Instances of ransomware are prime examples of when having a secure backup has been helpful, as it often can allow the systems to be restored to a previous state with reduced loss of information and without paying a ransom.

In the GoA, your files are backed up automatically if you store your files in OneDrive. At home, there are several methods you can use ranging from regularly copying and pasting your files to an external storage drive and storing that drive in a fireproof safe to using the native backup application on your device (for example, Time Machine for Apple or File History for Windows). Cloud backups are also a tool that can be used to backup personal files. This method saves your data offsite in a remote Cloud database, a technique mirroring how OneDrive works.

Use Anti-Malware

Anti-Malware is used to protect information technology [IT] systems and individual devices from malicious software or viruses. Anti-malware programs are able to actively scan systems and devices for threats. These programs are constantly running and can quickly detect any malicious piece of software and once detected, the program is able to quarantine the malware/virus from infecting the other parts of the system or device. It will then notify you that a threat has been detected and quarantined. Anti-malware programs should be on all your devices; however, more than one anti-malware program should not be installed at the same time. This is because having multiple anti-malware programs running concurrently will have a negative impact on the effectiveness of how these programs do their jobs. All GoA devices have anti-malware programs installed. In regard to personal devices, there are a number of free anti-malware programs that are available, such as Malwarebytes, Avast, Kaspersky, Assemblyline, and TrendMicro. Anti-malware programs will protect our systems against malware and viruses downloaded from the internet.

Maintain Educational Awareness

One of the biggest things you can do to protect yourself is be aware of potential risks and threats that could affect your cybersecurity. This doesn't mean you have to be an expert in cybersecurity but do be aware of notices that are sent out about specific threats or issues that are ongoing. Keeping on top of the training provided by the GoA is another good way to keep yourself educated about potential issues or red flags regarding cyber threats.

Cybercriminals are getting better with their attacks and are using more sophisticated programs to hack people, so it is getting harder and harder to keep yourself educated. However, by always taking the time to question and verify things that seem slightly off or unusual you can keep yourself both safe and knowledgeable. Remember, with the security of your information, it is always better to be safe than sorry.

If you have any questions about cybersecurity or any of the information provided in this report, please feel free to contact the *Cybersecurity Division* and we will be happy to answer any questions you may have!

References & Further Reading

Baker, K. (2022, June 1). What is cyber espionage?. *CrowdStrike*. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

Canadian Centre for Cyber Security. (2022). *National Cyber Threat Assessment*. https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf

Gibson, C., Kropotov, V., Lin, P.Z., McArdle, R., & Yarochkin, F. (2022, October 18). Leaked today, exploited for life: How social media biometric patterns affect your future. *Trend Micro*. https://tinyurl.com/mpcb76uf

Ion, I. (2015, July 23). New research: Comparing how security experts and non-experts stay safe online. *Google Security Blog*. https://security.googleblog.com/2015/07/new-research-comparing-how-security.html

Korolov, M. (2021, December 27). Supply chain attacks show why you should be wary of third-party providers. *CSO*. https://tinyurl.com/2tvfw4aa

NIST. (2022, February 16). Back to basics: Multi-factor authentication (MFA). *NIST*. https://www.nist.gov/back-basics-multi-factor-authentication

Rimeikis, A. (2022, November 14). Does a VPN protect you from hackers in 2022?. *Surfshark*. https://surfshark.com/blog/does-vpn-protect-you-from-hackers

Trend Micro. (2022). Zero-day vulnerability. *Trend Micro*. https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability

Vijayan, J. (2022, April 21). Zero-day exploit use exploded in 2021. *DarkReading*. https://www.darkreading.com/threat-intelligence/zero-day-exploit-use-exploded-in-2021