Trellix

TLP:GREEN

Threat Landscape Report

Canadian Government Sector

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Date Range: (January 1 - February 13, 2025)

Threat Intelligence Group
threatintelligenceservices@trellix.com

Introduction

This report provides a snapshot of malicious detections within Canada from Trellix's perspective through the Advanced Threat Landscape Analysis System (ATLAS). ATLAS is a data analysis tool that integrates Trellix's data sources and provides enrichment data for potential emerging threats. It correlates these threats with Trellix's Threat Intelligence Group (TIG) campaign research and open-source data. The report will start with a global view and then transition to Canada, with, where applicable, notes for the government sector within Canada.

Reporting Period: January 1st and February 13th, 2025.

Report Considerations

This report provides information based on telemetry from Trellix products. This detection data offers valuable insights into the current cybersecurity threat landscape; however, it should not be considered a complete picture of all threats to a country or sector.

Table of Contents

Summary Findings

Summary of the threat landscape for the Canadian government sector during the reporting period

The majority of the threats poised, based on Trellix detection data, come from the attempted distribution of malware, specifically information-stealers.

Global

Between January 1st and February 13th, 2025 Trellix globally observed 387,583,905 malicious file detections. Most malicious detections occurred within the United States, accounting for 45% of all detections. Germany was second at 15%, then Australia (4.5%), Canada (4.4%) and India (4.2%).

Figure 1, Top 5 countries for detections during the reporting period.

The government sector received the most detections. Next for the top five were banking/financial/wealth management, services, manufacturing, and Healthcare.

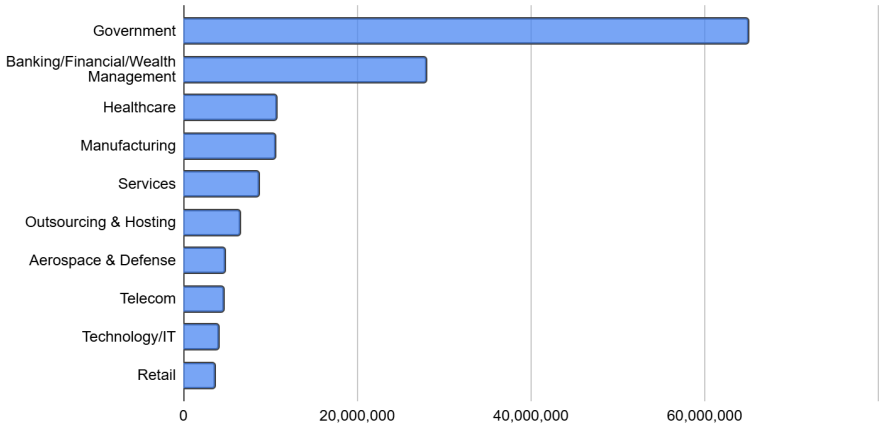

Figure 2, Global detections by sector

Canada

Within Canada, Trellix telemetry observed 17,158,619 malicious file detections. The services sector received the most detections. Next were manufacturing, media

& communications, insurance, and banking/financials/wealth management. The Government sector came in at the 6th spot with 630,623 detections.

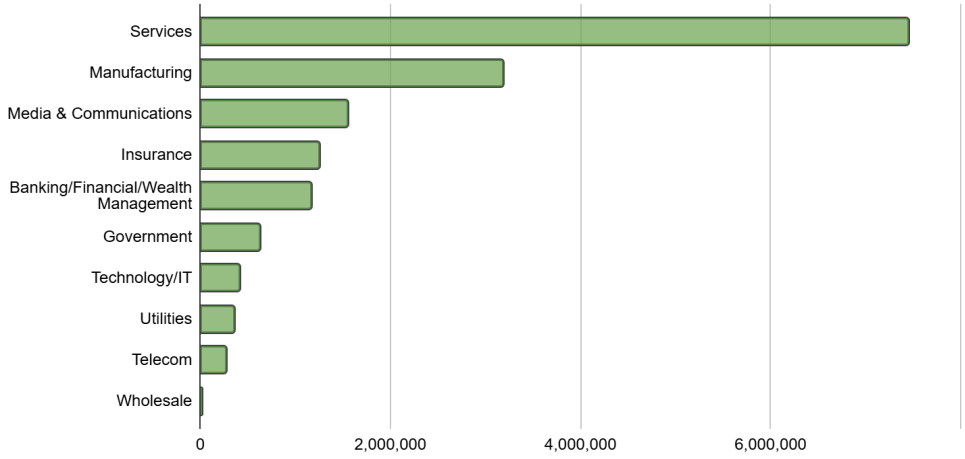

Figure 3, Canadian detections by sector

Recent Past

If we look back at detections for Canada during the last 6 months of 2024 (July 1st to December 31st) the Government sector is in the 6th place again showing a consistent number of detections/targeting related to this sector in Canada.

Top Threat Categories

Canada		Government Sector in Canada
Information-stealer	1	Information-stealer
Remote Access Trojan (RAT)	2	Downloader
Trojan	3	Vulnerability
Downloader	4	Backdoor
Vulnerability	5	Remote Access Trojan (RAT)

Information Stealers

Information stealers have become increasingly popular among threat actors. There is a significant market for stolen personal and financial information which can be sold on dark web marketplaces. Stolen credentials, banking details, and personally identifiable information (PII) are in high demand for identity theft, fraud, and phishing scams. The following additional features have helped make them a tool of choice for threat actors.

- Low barrier to entry: Information stealers are often sold as malware-as-a-service thus allowing less technically proficient individuals to deploy sophisticated attacks without needing extensive knowledge in programming or cyber tactics.
- Automation and Botnets: Many information stealers can be integrated into automated systems or botnets, allowing for large-scale attacks with minimal human intervention.
- Highly modular and customizable: Attackers can modify them to target specific systems, applications, or data types, increasing their effectiveness and allowing them to stay relevant in a constantly evolving cybersecurity landscape.
- Effective Evasion Techniques: Information stealers commonly employ advanced evasion tactics, helping them to avoid detection, increasing the likelihood of successful infections and prolonged access to compromised systems.
- Wide Distribution Methods: These malware types can be propagated through various channels, including phishing emails, malicious attachments, and compromised websites and social engineering tactics.
- Low Risk of Attribution: Cybercriminals, and even advanced persistent threats, can use the decentralized networks and infrastructure of these malware families to make it difficult for cyber defenders to trace attacks back to the perpetrators.

We regularly see government sector accounts collected by these information stealers and for sale on underground forums and markets.

Not surprisingly the largest threat actor campaign detections we saw for the reporting period were all related to information-stealers.

Campaigns Threats

Threat actor campaigns using the following malware families were most prolific for the reporting period.

1. Matiex Snakelogger (aka snake_keylogger)
2. Agent Tesla (aka telegram_rat)
3. Formbook

Analyst Note: Formbook was the highest detected campaign threat in the government sector in Canada for the reporting period.

All three malware families are classified as information stealers and have the following features:

Information Theft

This malware is primarily designed to capture sensitive information, including:

- Login Credentials: It records usernames and passwords from web browsers and applications.

- Keystrokes: As a keylogger, it logs all keystrokes made by the user, allowing attackers to gather sensitive data.
- Clipboard Data: It can access and record any data copied to the clipboard.
- Screenshots: The malware has the ability to take screenshots of the user's desktop, enabling attackers to capture sensitive information visually. *(All)*

Persistence

The malware employs techniques that allow it to remain undetected on the infected system for prolonged periods, maximizing the potential for data theft. *(All)*

Command and Control (C2) Capabilities

The malware can connect to remote servers controlled by attackers, allowing for the exfiltration of stolen data and the receipt of additional commands or updates. *(All)*

Evasion Techniques

The malware employs various techniques to evade detection by security measures, including obfuscation and leveraging legitimate system processes. *(All)*

Modular Architecture

Designed to be adaptable, allowing for updates and modifications that enhance its functionality and make it harder to detect. *(Snakelogger & Agent Tesla)*

Customization

Designed to be easily customized for specific targets, making it a versatile tool for cybercriminals. *(Formbook)*

Multiple Dissemination Methods

These malware families spread through various channels, including:

- Phishing Emails: They often propagate via malicious attachments in phishing emails, tricking users into executing the malware. *(All)*
- Compromised Software: Attackers may distribute the malware through cracked software or hidden within other applications. *(Snakelogger)*
- Compromised Websites: Attackers may use compromised websites to deliver the malware. (FormBook)
- Malicious Links: Attackers may use deceptive links in social engineering tactics to prompt users to download the malware. *(Agent Tesla)*

Targeted Attacks

They have been associated with numerous targeted attacks aimed at both individual users and organizations, demonstrating their versatility and adaptability in cyber operations. *(Agent Tesla)*[1]

Top Detectioned files

The following are the top five detected **Matiex Snakelogger** files in Trellix Telemetry, in Canada, for the reporting period.

78d2d7a86bbcad826e1d04cda24531e0 (MD5) 877016873a7680ee63c28ef14e87271957a60281cf7f578b7ab0ec60233557de (SHA256)	1
574853398c3ff5ef8c2ac98608426376 (MD5) 4531e41ef1492cc58f00d7c785724543a242dca42974d3dd4c0e9d3ef832318c (SHA256)	2
d3f64e6092f711c5f8a619510ead67d5 (MD5) 16677f9c1d5f08b79a593ca7559aa0bfb50ad27ea0395644e16e9f855c9d58b0 (SHA256)	3
8a07fc97103b96931c7078dded644255 (MD5) 8b0cbf076e622dddab2bf9ac40be19ee8db87c6cd5c48b9335da584b7ded6847 (SHA256)	4
bf2be29722bcff0bb97041b869271cea (MD5) 242decd59eacea5ca26bbb09a65e5ee152889afddf2931c63ed712efcce6d7d1 (SHA256)	5

The following are the top five detected **Agent Tesla** files in Trellix Telemetry, in Canada, for the reporting period.

e6c6541c95da090df8c0124b7c9611f4 (MD5) 06b93c4d0c315b97144c799c38317a4be3fb2eb238b7fd1d5bb9941acc1da19c (SHA256)	1
525c8f9d5ebdf8f38d60a474bf8d5450 (MD5) bce0ac94f5fb59ead6808a018e8e11044af82ae55e39e14580c18fca65eff04a (SHA256)	2
82d536a65d5474261f4bec0cf590574b (MD5) 15e55a1c746933955d19246f4f8629d22c086f3eed47c7e0fa470d57498d5cd5 (SHA256)	3
844edd5faff061237308478178887422 (MD5) fdf1b3c4f41e7317f0d7fc42dff37202e3b07a7572fc1f32f3a88ad3edf76b0a (SHA256)	4
c06839f9f103cf2ca8e95553792899ad (MD5) 894009fb9eb6b5b4101b75e57fea7242a53f11e8074999ae6094892a99325547 (SHA256)	5

[1] Recorded Future - Feature summary for Snakelogger, Agent Tesla, and Formbook.

The following are the top five detected **Formbook** files in Trellix Telemetry, in Canada, for the reporting period.

22a1e355e92db8f488724bb9df0de931 (MD5) bbcdb1e680a621a30241a23d8fc9113d0a36602bb7a3702430e564d9f678ca63 (SHA256)	1
734a91f809ef28c16b8f5ac5152dfa3a (MD5) 244735351e7ff85696098b10dfed915480812e51e2699678bfba414f9800592e (SHA256)	2
2990f010eb3dba4e6497958929d53a84 (MD5) 618ccc64e31ec4741e691b7d5462f66729b83062c2bc1e5fba671f9200ec6872 (SHA256)	3
f4baa9409762369cc74c71b874fde345 (MD5) 4ef83ac7a3bdee1a742de8de749c5afa4747acc20f8937301dcba291d1ef83d7 (SHA256)	4
da15d5729ee365d537292b7b3bcebfbc (MD5) c7a1dff9b1cc12833d92df185e2e52fb3d5da32078bb8cf4ea65ae9fb53a00c3 (SHA256)	5

Top Threat Actors

While efforts are made at attribution it is important to note that many of the malicious detections that are captured are not currently linked to a specific threat actor or group. Below we will look at the top threat actors when attribution was possible.

The top 5 threat actors seen in Canada for the reporting period are UAC-0050, RansomHUB, Sandworm Team, UNC3886, and TA505 Group. Let's look at the top 3 more closely.

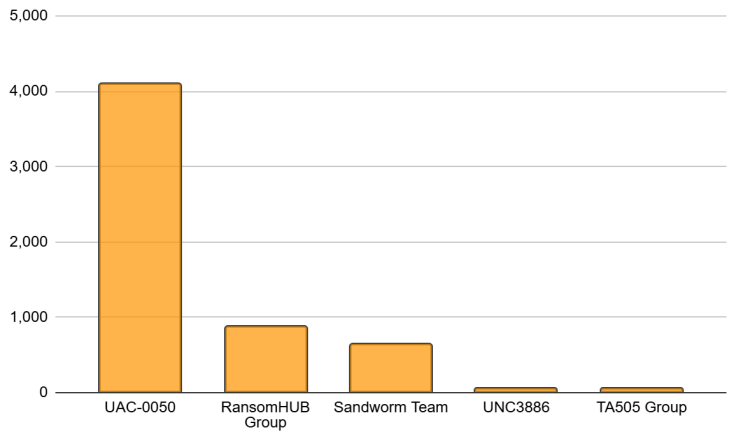

Figure 4, Top 5 Threat Actors in Canada based on number of detections

UAC-0050

The threat actor known as UAC-0050 is a cyber espionage group that primarily targets government agencies in Ukraine. They have been active since 2020 and are known for using the Remcos RAT (Remote Administration Tool) to gain full control over infected systems. The group utilizes various tactics, such as phishing emails, to distribute their malware and evade detection by security software. They often impersonate legitimate organizations to trick recipients into opening malicious attachments.[2]

[2] Recorded Future – UAC-0050 Intelligence Card

Motivations

Their campaigns have geopolitical motivations, with a focus on intelligence gathering in Ukraine. Overall, UAC-0050 poses a significant threat to Ukrainian government entities (and supporting governments) and has been actively evolving their techniques to remain stealthy and effective.

Analyst Note: We did see a significant spike in activity just before and during Prime Minister Trudeau's visit to Kyiv on the two year anniversary of the invasion, on February 24th 2024.

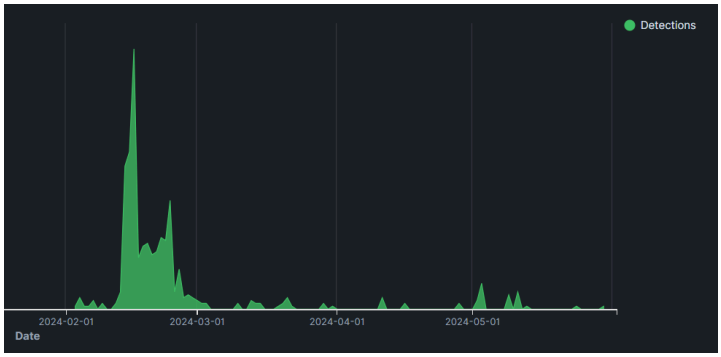

Image 1, UAC-0050 spike in activity in mid to late February last year.

RansomHUB Group

The RansomHUB Ransomware Group, active since February 2024, has been implicated in numerous high-profile cyberattacks across various sectors, including healthcare, finance, retail, and education. Their attack methodology typically involves initial access via phishing emails and exploitation of known vulnerabilities to gain a foothold in target networks. Notably, they employ advanced evasion techniques like EDRKillShifter to disable endpoint detection and response systems, alongside tools like TDSSKiller and LaZagne for credential theft from the Local Security Authority Subsystem Service (LSASS) memory. RansomHUB operates using a ransomware-as-a-service model with an affiliate structure and commonly utilizes double-extortion tactics to pressure victims by threatening to leak stolen data unless a ransom is paid.[3]

Motivations

RansomHUB's motivations revolve around financial gain through extortion, targeting lucrative industries, building a strong reputation within the cybercriminal ecosystem, and employing psychological tactics to increase the likelihood of ransom payments.

Sandworm Team

Sandworm (APT44) is a highly adaptable and prolific Russian state-sponsored hacking group linked to Unit 74455 within the GRU. Sandworm has been active since 2009 and is known for its versatile cyber warfare capabilities, employing phishing, credential harvesting, exploiting vulnerabilities, and conducting supply-chain attacks. They have targeted many organizations globally, focusing on critical infrastructure sectors like energy

Image Source: https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm

[3] Recorded Future – RansomHUB Intelligence Card

and telecommunications. Sandworm's most common TTPs include deploying custom malware variants like Kapeka and FakePenny, utilizing proxy botnets for their operations, and masquerading as hacktivist groups to obfuscate their activities.[4]

Motivations

The Sandworm team's motivations primarily focus on serving Russia's strategic and political goals. They serve as a nation-state-sponsored cyber espionage group that conducts cyberattacks to support Russian military interests. They frequently target Ukrainian organizations, the North Atlantic Treaty Organization (NATO), and NATO partner organizations and institutions. Their attacks are often in line with Russia's continued aggression in Ukraine and aim to gather sensitive information and intelligence. Sandworm's victimology suggests that they primarily target known adversaries of Russia in geopolitical events.

Government Sector in Canada

One threat actor, not on the list above, stood out when detections were examined specifically for the government sector in Canada: Stargazer Goblin.

Stargazer Goblin is known for utilizing seemingly legitimate GitHub projects to distribute malware. Their activities have been linked to several malware families, including Lumma Stealer, Atlantida Stealer, Rhadamanthys, and RedLine. The group is part of a broader network referred to as the Stargazers Ghost Network, which operates under a model called Distribution as a Service (DaaS). This model enables them to spread malicious links and payloads using compromised GitHub accounts and phishing repositories.

Moving Ahead

Canada and its government sector are under constant attack from cybercriminals, organized ransomware groups, and sophisticated state sponsored threats. Based on our detection data, many of these groups are employing information stealers in their toolkit, making this a risk that organizations in this sector should be focusing on.

[4] Recorded Future – Sandworm Intelligence Card