



CANADA

Regional Threat Landscape Report





Table of Contents

Executive Summary	3
Dark Web Threats	4
Ransomware Threats	9
Stealer Log Statistics	17
Phishing Threats	18
DDoS Attack Statistics	21
Lessons Learned: Key Insights and Strategic Recommendations	22

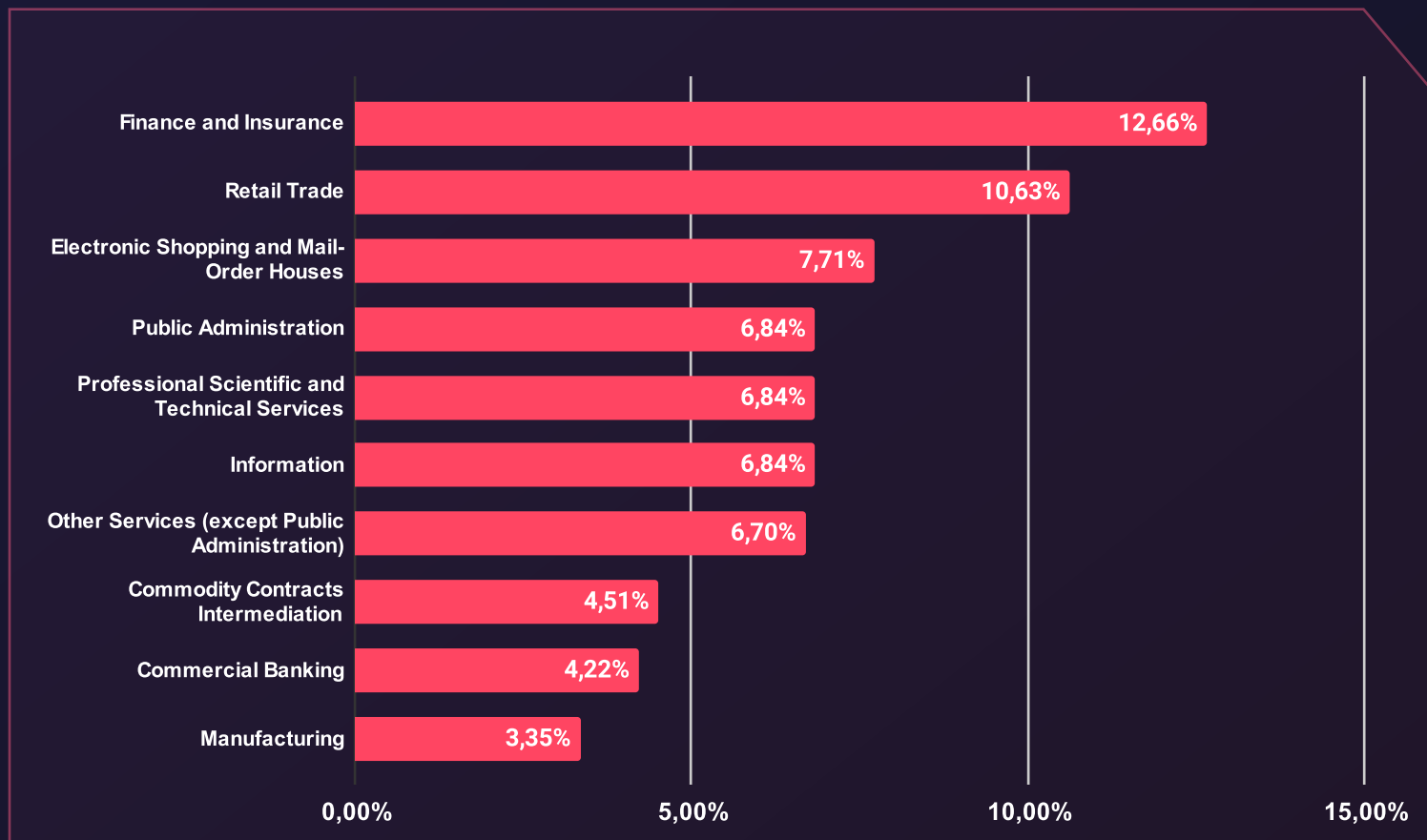
Executive Summary

Top Takeaways

- **Finance and insurance are the most targeted industries in Canada, with 12,66% of all the posts targeting them.** The **retail trade** industry takes second place with **10,63%** of the posts, and **electronic shopping and mail-order houses** were third, with **7,71%** of all the Dark Web forum posts.
- Threat actors targeting Canada mostly sold the content they obtained. The **Selling** category is in first place with 60,88% of all the posts from Dark Web forums, followed by **Sharing**, which comprises 31,52%. We have **Hack Announcements** in third place, with 7,60% of the posts.
- When we look at the type of information published on dark web forums, we see that **Databases** take the first spot with 48,92% of all the posts. The second most popular type of information threat actors share is content related to **Access** (sales/shares, etc.,) which takes 32,60% of the posts. On the third spot, we have **Website attacks** (defacements, DDoS attacks, etc.) with 8,9% of the posts.
- Ransomware groups targeted the **Manufacturing** industry in Canada, with **21,11%** of all attacks. The **Professional, scientific, and Technical Services** industry took the second spot, with **12,22%** of the attacks, and **Retail Trade** was the third one, with **5,56%** of the attacks.
- Our analysis shows that the most active ransomware group targeting Canada was **LockBit**, which is responsible for **30.3%** of all the attacks. The second most active group was **Play Ransomware**, with **24.4%** of all the attacks. In third place, we have **Medusa Ransomware**, with **22.7%** of all the ransomware attacks targeting Canada.
- SOCRadar's stealer log data from Canada's most visited platforms reveals sensitive information, including **208,010 email and password** combinations, **45,742 password hashes**, **30,804 unique victim IP addresses**, and **18,392 credit card** details.
- The **cryptocurrency** industry in Canada faced the most phishing attacks, with **31,66%** of the total attempts. The **public administration** industry was in the second spot, with **11,24%** of the attacks, and **information services** were targeted at **10,95%**.

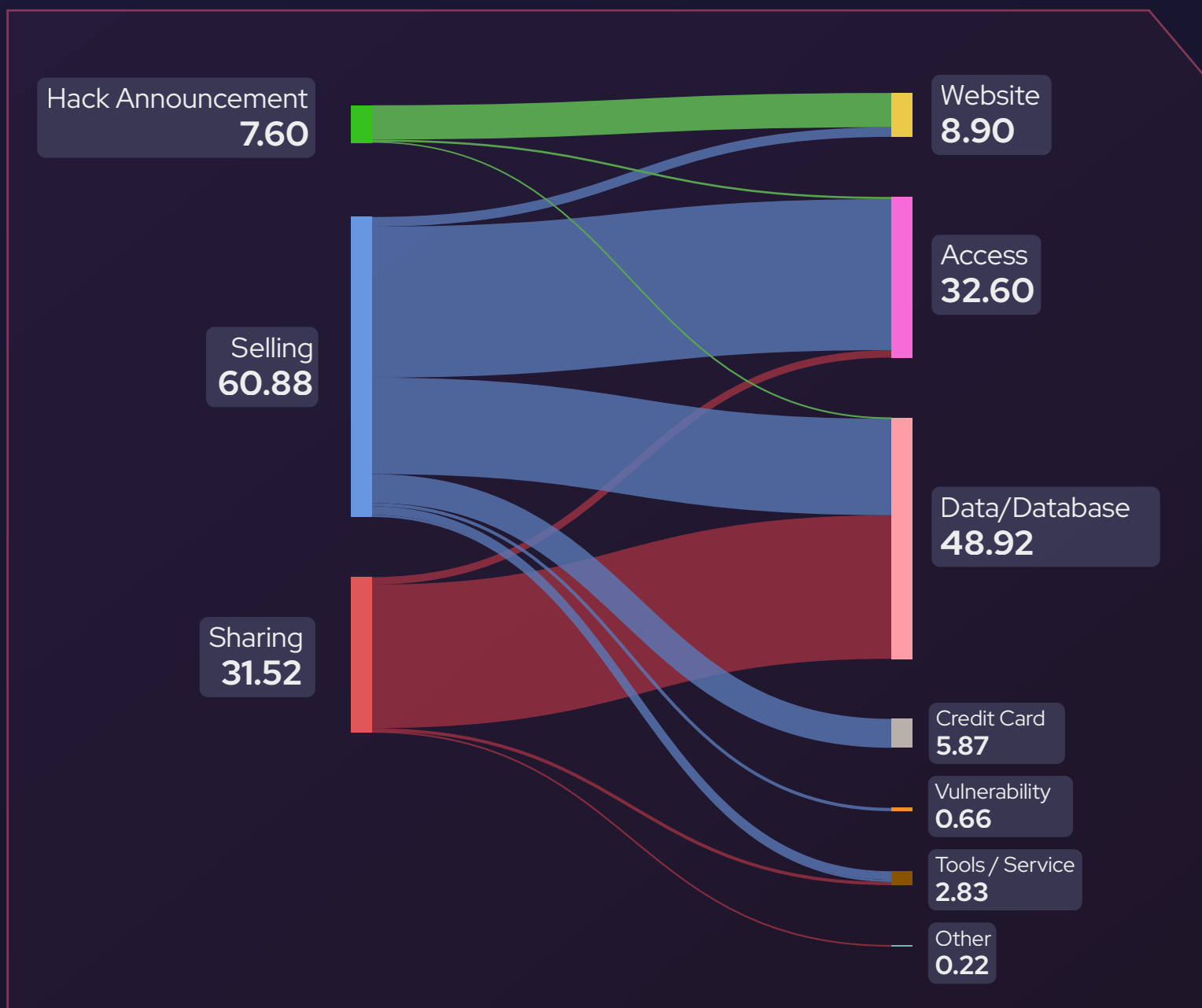
Dark Web Threats

Distribution of Dark Web Threats by Industry



Finance and insurance are the most targeted industries in Canada, with **12,66%** of all the posts targeting them. The **retail trade** industry takes second place with **10,63%** of the posts, and **electronic shopping and mail-order houses** were third, with **7,71%** of all the Dark Web forum posts.

Distribution of Dark Web Threats by Threat Categories

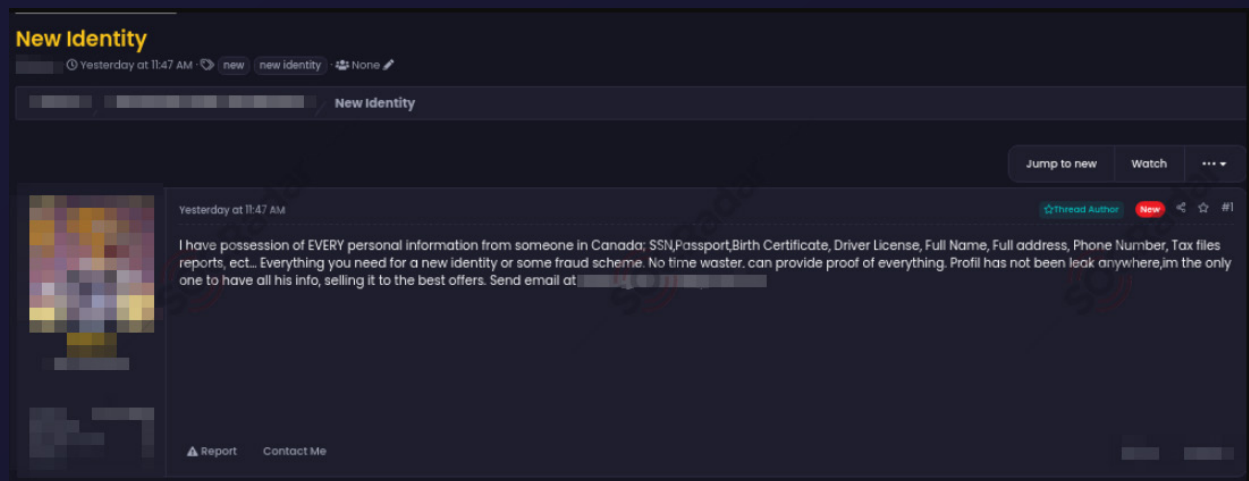


Threat actors targeting Canada mostly sold the content they obtained. The Selling category is in first place with 60,88% of all the posts from Dark Web forums, followed by Sharing, which comprises 31,52%. We have Hack Announcements in third place, with 7,60% of the posts.

When we look at the type of information published on Dark Web forums, we see that Databases take the first spot with 48,92% of all the posts. The second most popular type of information on the forums is content related to Access (sales/shares, etc.), which accounts for 32,60% of the posts. On the third spot, we have Website attacks (defacements, DDoS attacks, etc.) with 8,9% of the posts.

Recent Dark Web Activities Targeting the Entities in Canada

The Alleged Sensitive Data of Canadian Citizens are on Sale



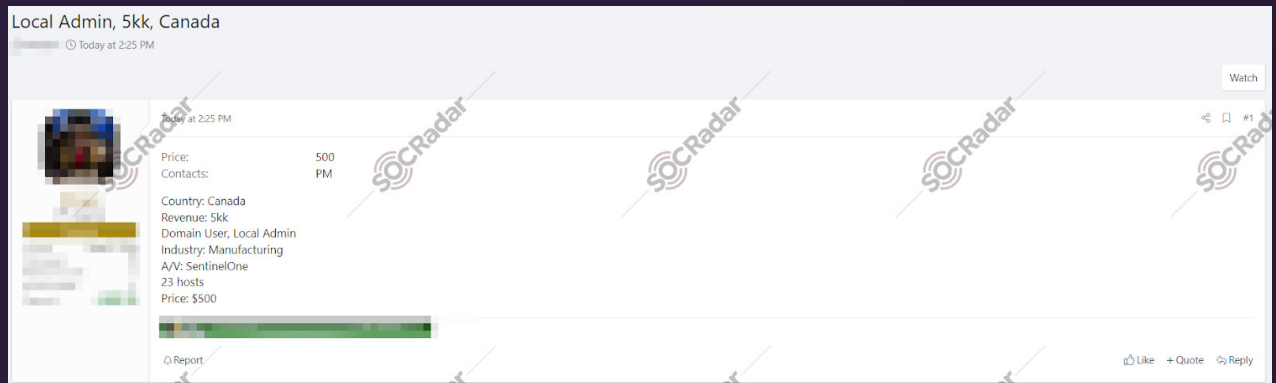
In a recent post discovered on a Dark Web forum by SOCRadar, a threat actor claimed to possess highly sensitive personal information belonging to Canadian citizens.

The post reads:

"I possess EVERY personal information from someone in Canada: SSN, Passport, Birth Certificate, Driver's License, Full Name, Full address, Phone Number, Tax file reports, etc. Everything you need for a new identity or some fraud scheme. I'm no time waster; I can provide proof of everything. Profil has not been leaked anywhere. I'm the only one to have all his info, and I'm selling it to the best offers."

This development highlights the risks the Dark Web poses as a marketplace for illicit activities and reinforces the need for vigilance and robust security measures to safeguard sensitive data.

The Alleged Unauthorized Admin Access Sale is Detected for a Canadian Manufacturing Company



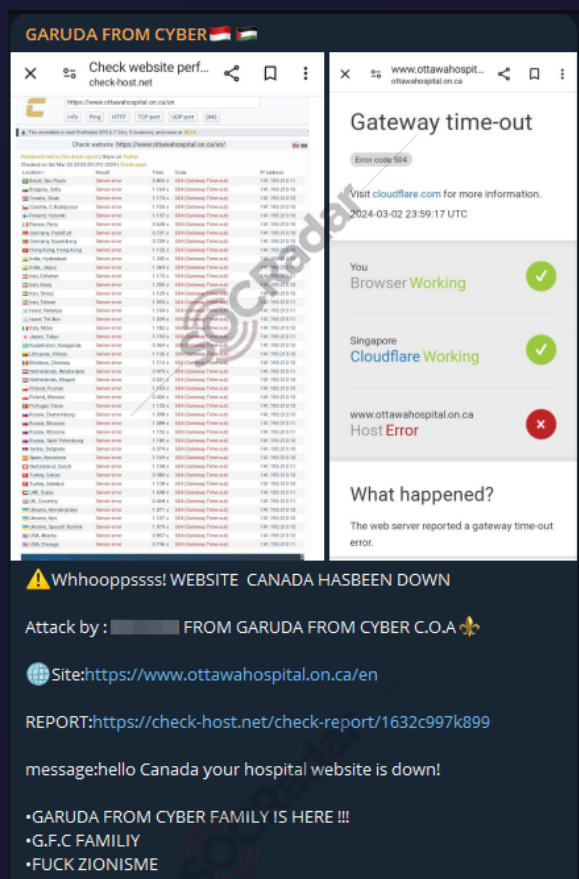
The post, from a forum monitored by SOCRadar, alleges the sale of unauthorized administrative access credentials purportedly belonging to a Canadian manufacturing company.

The threat actor claims the access is priced at \$500, offering potential buyers control over what is described as a "domain user and local admin" account within the organization's network. Additional details in the post suggest the compromised network comprises 23 hosts and utilizes SentinelOne as its antivirus solution.

According to the alleged information, the company operates in the manufacturing sector and reportedly generates an annual revenue of \$5 million (USD). The seller has invited interested parties to initiate contact via private messaging.

It is important to emphasize that these allegations are unverified and represent claims made by the threat actor.

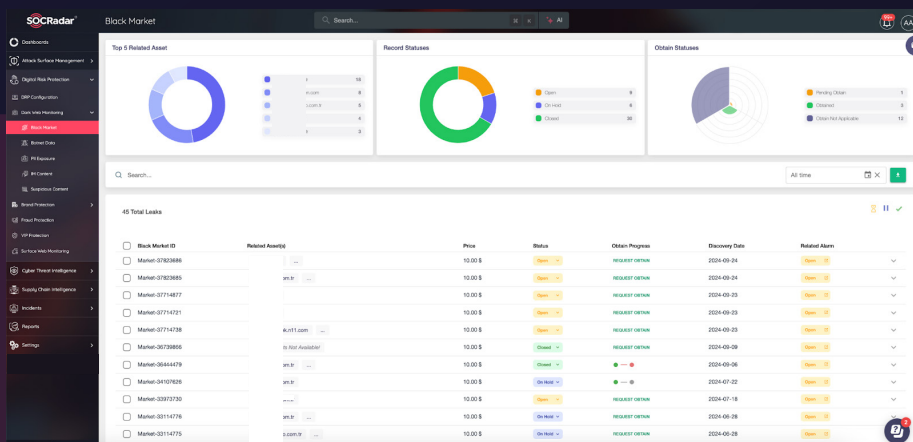
Garuda From Cyber Conducted DDoS Attack on The Ottawa Hospital



In a post on the Telegram channel associated with the threat actor group Garuda From Cyber, claims of a Distributed Denial of Service (DDoS) attack targeting The Ottawa Hospital's website have surfaced.

As monitored by SOCRadar, the post announced the purported takedown of the hospital's online presence. The post included a link to a reported check-host report to purportedly substantiate the claim of the attack.

It is important to emphasize that these allegations remain unverified. Threat actors frequently use platforms such as Telegram to amplify their claims, whether verified or not, to sow fear, disrupt operations, or draw attention to their causes.

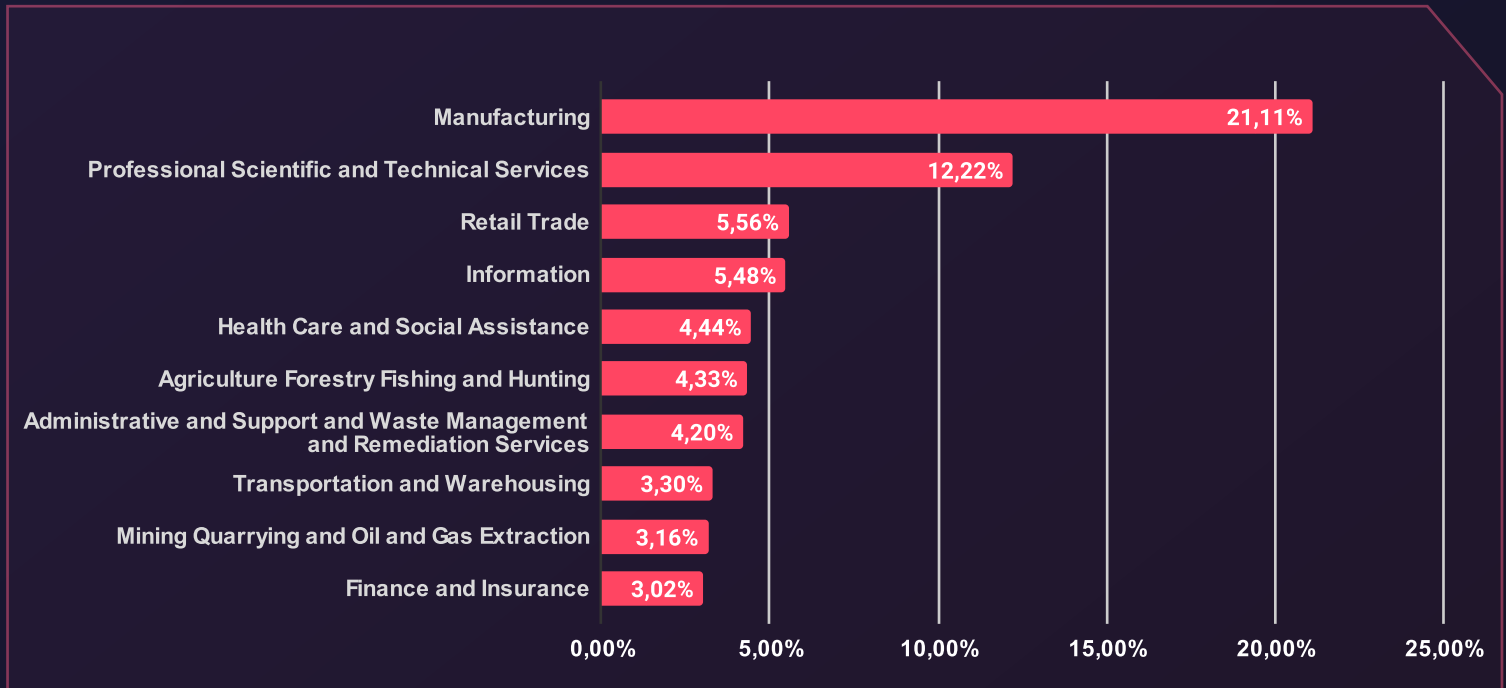


SOCRadar's Advanced Dark Web Monitoring equips organizations in Canada with vital insights into hidden threats targeting key industries such as finance, insurance, and information technology, which have faced significant risks over the past year. By providing real-time monitoring of underground chatter and sensitive data exposure, SOCRadar empowers proactive defenses against Dark Web threats.

Activate your free trial today to safeguard your organization's most valuable assets.

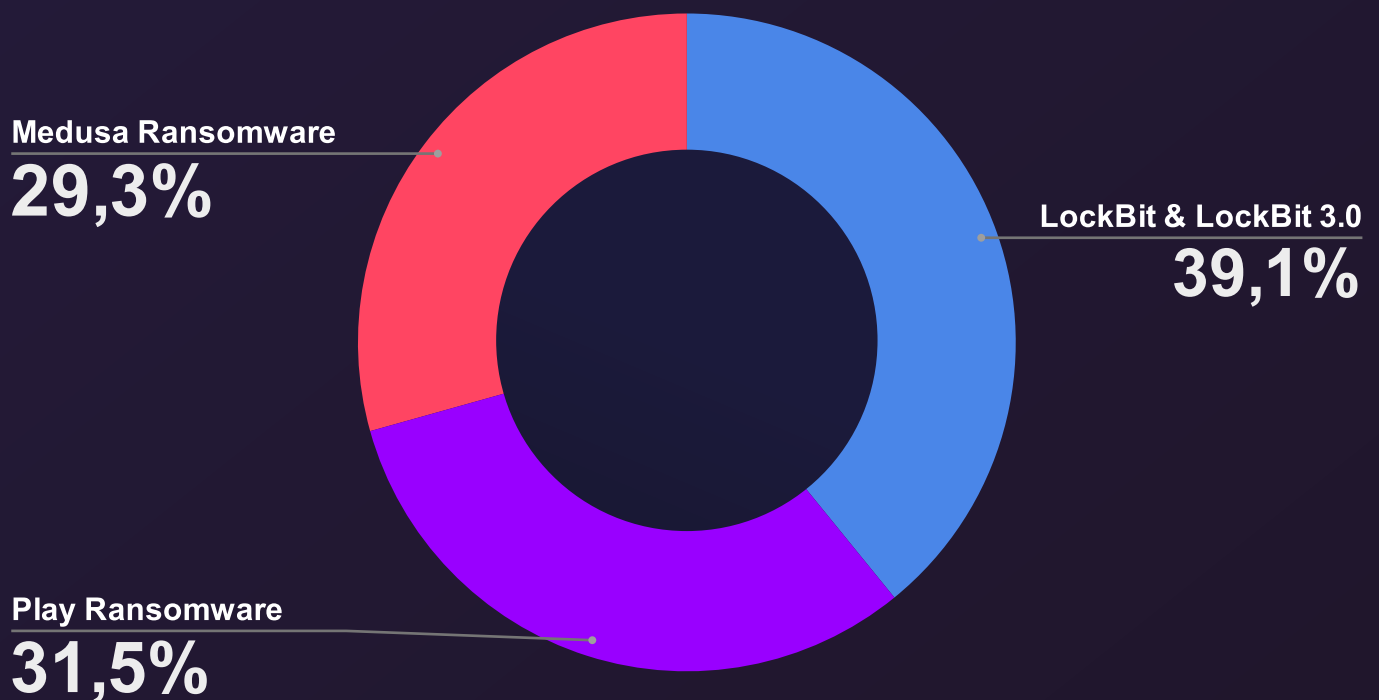
Ransomware Threats

Distribution of Ransomware Attacks by Industry



Ransomware groups targeted the Manufacturing industry in Canada, with 21,11% of all attacks. The Professional, scientific, and Technical Services industry took the second spot, with 12,22% of the attacks, and Retail Trade was the third one, with 5,56% of the attacks.

Top Ransomware Groups Targeting Canada



Our analysis shows that the most active ransomware group targeting Canada was **LockBit**, which is responsible for **30.3%** of all the attacks. The second most active group was **Play Ransomware**, with **24.4%** of all the attacks. In third place, we have **Medusa Ransomware**, with **22.7%** of all the ransomware attacks targeting Canada.



Threat Actor Card of Lockbit 3.0 Ransomware Group

LockBit 3.0, succeeding LockBit and LockBit 2.0, functions as a Ransomware-as-a-Service (RaaS) entity.

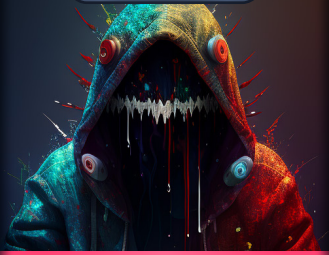
Since January 2020, LockBit has transitioned to an affiliate-based model, employing diverse methodologies to target businesses and critical infrastructure entities. Noteworthy tactics include double extortion and the utilization of initial access broker affiliates, alongside recruitment efforts involving insiders and hacker recruitment competitions.

With over 1,500 victim disclosures on the SOCRadar platform, LockBit emerged as the most active ransomware group in 2022 following Conti's cessation. As of the first quarter of 2023, they retain their position as the most prolific group, with over 300 disclosed victims.

You can visit our [blog post](#) for more detailed Lockbit 3.0 Ransomware Group information.

Play Ransomware

Play Ransomware



Country of Origin: Unknown

Play Ransomware (PlayCrypt) is a ransomware group first observed in June 2022. The group commonly targets organizations based in Latin America but mainly focuses on Brazil.

-Ransomware Group-

Motivation: Financial Gain

Target Countries: Latin America, India, Hungary, Spain, Netherlands, United States

Target Sectors: Manufacturing, Education, Real Estate, Technology, Transportation, Healthcare

Attack Type: Compromised Valid Accounts, LOLBins, Ransomware, Data Exfiltration

-TTPs-

Process Injection: T1055

Input Capture: T1068

Proxy: T1090

Threat Actor Card of Play Ransomware Group

Play Ransomware's main target is the Latin American region, and Brazil is at the top of the list. Even though they seem like a new ransomware group, their identified TTPs resemble the Hive and Nokayawa ransomware families. One of the behaviors that makes them look similar is using AdFind, a command-line query tool capable of collecting information from Active Directory.

Double extortion is a widespread technique in which cyber actors threaten to exfiltrate sensitive data. Play Ransomware also uses double extortion against its victims. They can archive the breached data with WinRAR and then upload it to file-sharing sites.

You can visit our [blog post](#) to read the rest of the threat actor profile.

Medusa Ransomware



The image displays a 'Threat Actor Card' for the Medusa Ransomware Group. On the left is a card with a portrait of a woman with glowing green eyes and the text 'Medusa Ransomware' and 'Country of Origin: Unknown'. On the right is a larger card titled '-Ransomware Group-' containing details about the group's motivation, targets, sectors, attack types, and TTPs.

-Ransomware Group-	
Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Canada, India, Turkey, Australia
Target Sectors:	Manufacturing, Education, Professional Services, Finance and Insurance
Attack Type:	RDP, Phishing, Ransomware, Double Extortion, Exploiting Google Chrome Vulnerabilities (CVE-2022-2295)
-TTPs-	
External Remote Services:	T1133
PowerShell:	T1059.001
Exfiltration Over Alternative Protocol:	T1048

Threat Actor Card of Medusa Ransomware Group

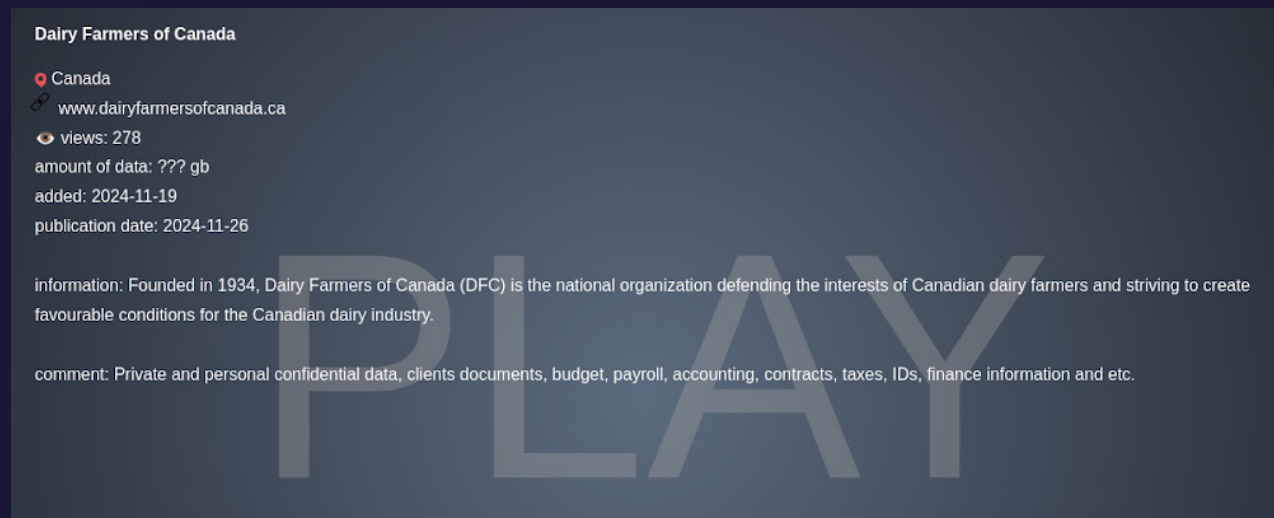
Since its first sighting in June 2021, Medusa Ransomware (or MedusaLocker) has been on the radar of cybersecurity experts. Operating under the **Ransomware-as-a-Service** (RaaS) model, the Medusa Ransomware group collaborates with global affiliates, making its reach and impact even more widespread.

Medusa Ransomware is not just another name in the long list of ransomware threats; it is a multifaceted menace, much like the many serpentine tendrils of Medusa's hair. Each encrypted file, bearing a variety of extensions, reminds us of the numerous snakes that crowned the Gorgon's head. The most prominent is the unmistakable ".MEDUSA" extension, a signature mark of this ransomware's venomous touch.

You can visit our **blog post** to read the rest of the threat actor profile.

Recent Ransomware Attacks Targeting Entities in Canada

Play Ransomware Claims Data Breach at Dairy Farmers of Canada



The Play Ransomware group has claimed responsibility for a data breach involving Dairy Farmers of Canada (DFC), alleging the theft of sensitive organizational and personal information.

According to the post, the breach purportedly targeted DFC's systems, compromising private and sensitive information. The threat actor claims to have accessed a wide range of data, including confidential documents, budget details, payroll and accounting records, contracts, tax-related files, identification information, and financial records. The exact volume of the allegedly stolen data has not been disclosed.

Dairy Farmers of Canada, founded in 1934, is crucial in advocating for policies that support the Canadian dairy industry and its farmers. The organization also promotes dairy consumption and ensures sustainable practices across the sector.

While these allegations are serious, it is important to note that they remain unverified at this stage. This incident highlights the growing risk of cyberattacks to organizations of all sizes, underscoring the importance of robust cybersecurity measures.

Canadian Healthcare Provider Medigroup.ca Allegedly Targeted by Ransomware Group

RansomHub

Medigroup.ca

ABOUT

medigroup.ca

Beverly Towne Medical Clinic and Pharmacy
11730 34 Street NW
Edmonton, AB T5W 1Z1
780-758-7900

5818 Terrace Rd NW
Edmonton, AB T6A 3Y8
780-756-5442

12620A 132 Ave NW
Edmonton, AB T5L 3P9
780-990-1820

8731 118 Ave NW
Edmonton, AB T5B 0T2
info@nolandrugs.ca
780-477-2748

11035 Groat Rd NW
Edmonton, AB T5M 3J9
780-705-4090

Dave Hill Pharmacy
1-200 Thickwood Blvd
Fort McMurray, AB T9K 1X9
Email: davehillpharmacy@medigroup.ca
Text: 780-743-1111
Facebook/Messenger: facebook.com/DaveHillPharmacy
780-750-1111

Medigroup Health Services' locations are progressive patient-centred medical facilities. We have created a network of family physicians, nurses, pharmacists, specialists, and other healthcare professionals who have patient care as their top priority.

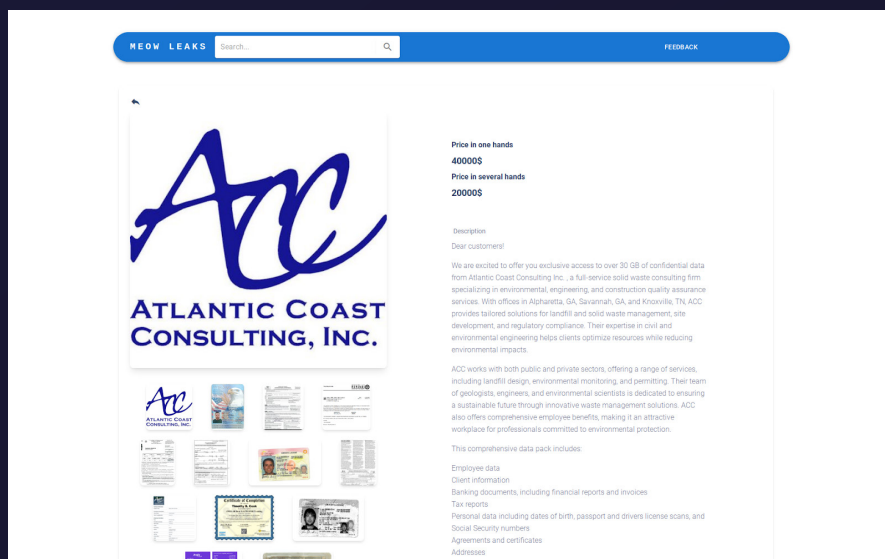
From common illnesses and injuries to pediatric care and internal medicine, our clinical teams are proud to provide care for patients of all ages. All clinics have adjacent pharmacies.

In an update on the RansomHub group's website, they claimed responsibility for targeting Medigroup.ca, a Canadian healthcare company. SOCRadar detected this announcement.

The company delivers comprehensive medical services, including healthcare management, consultations, and coordination of care.

Ransomware attacks on healthcare organizations are a growing concern, given the critical nature of their services and the sensitive data they manage.

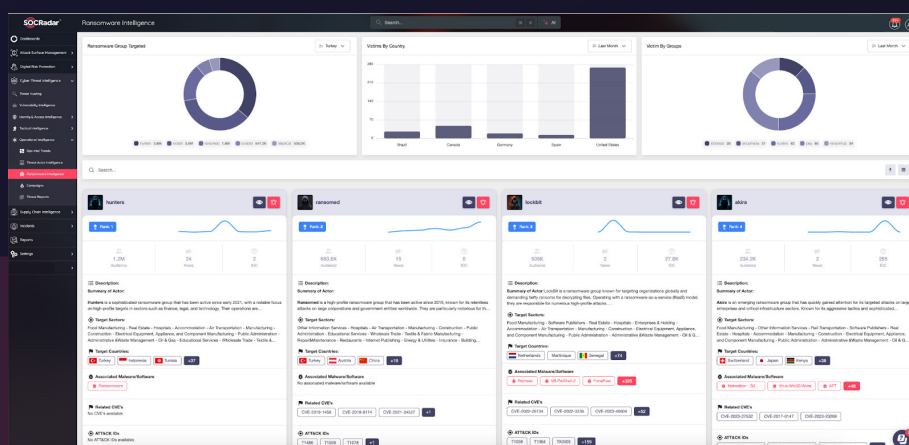
Canadian Healthcare Provider Medigroup.ca Allegedly Targeted by Ransomware Group



In the meow ransomware group website monitored by SOCRadar, Atlantic Coast Consulting Inc. was announced as an alleged ransomware victim.

Atlantic Coast Consulting Inc. is a professional firm specializing in environmental consulting and engineering services. They focus on waste management, environmental compliance, and sustainable solutions for various industries.

The company is known for its expertise in permitting, site assessments, and regulatory compliance, helping clients navigate complex environmental regulations efficiently.



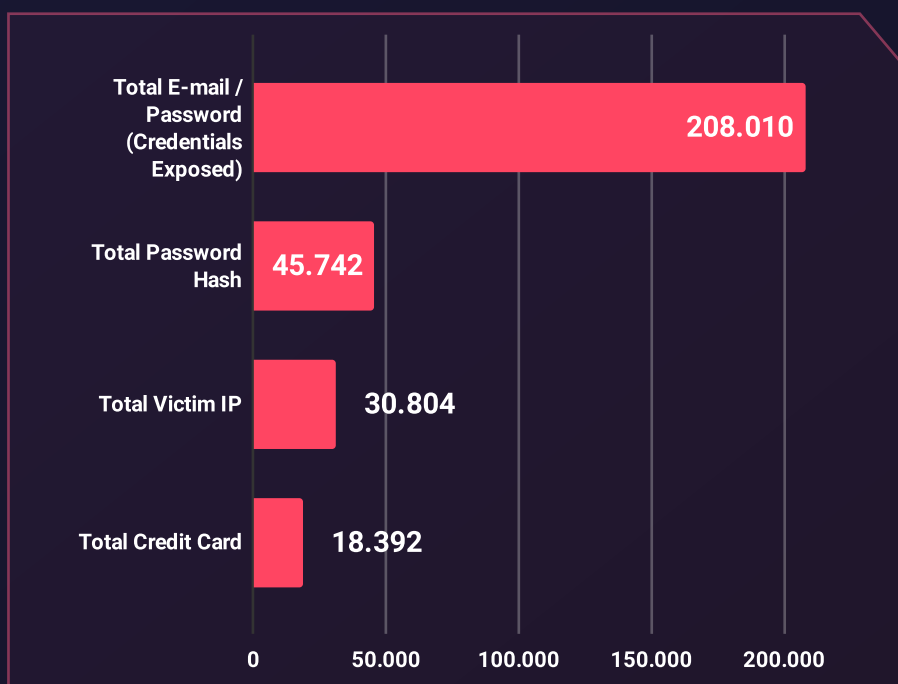
[Explore SOCRadar's Ransomware Intelligence module](#) and gain comprehensive insights with detailed group profiles, MITRE Visualizer, and actionable IOCs. These insights will empower you to stay ahead of evolving threats and enhance your cybersecurity strategy.

Stealer Log Statistics

Stealer Log Statistics: Top Domains in Canada

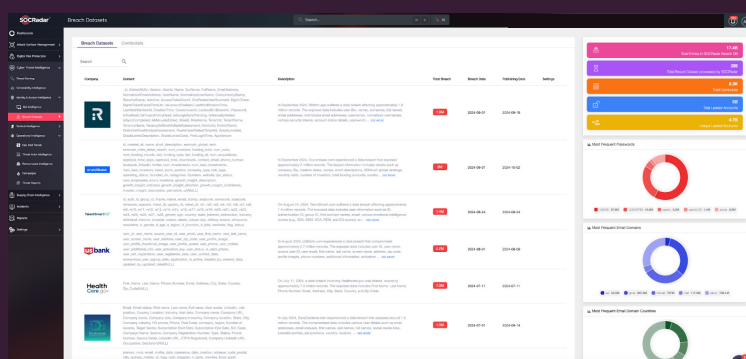
Domains	
canada.ca	radio-canada.ca
ctvnews.ca	homedepot.ca
walmart.ca	globalnews.ca
realtor.ca	canadiantire.ca
lapresse.ca	kijiji.ca

Stealer Logs - Distribution of the Compromised Data



SOCRadar's stealer log data from Canada's most visited platforms reveals sensitive information, including 208,010 email and password combinations, 45,742 password hashes, 30,804 unique victim IP addresses and 18,392 credit card details.

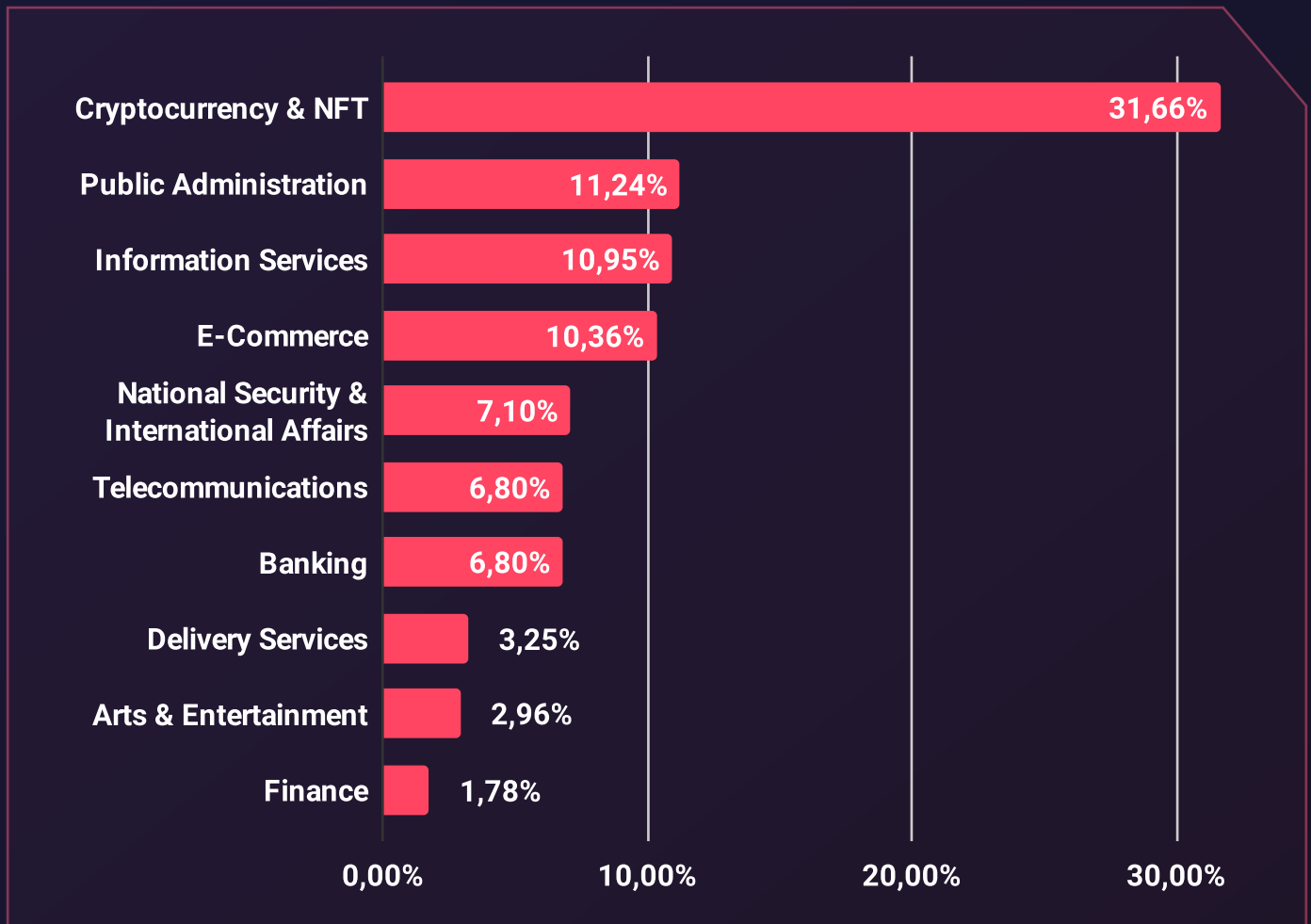
Organizations should implement strict password policies and ensure appropriate Identity & Access intelligence solutions are used.



SOCRadar's Identity & Access Intelligence Module can detect stealers on your devices and identify their location, facilitating a secure working environment. Changing passwords without eliminating stealers is insufficient to secure your organization, as it will only provide new passwords to threat actors.

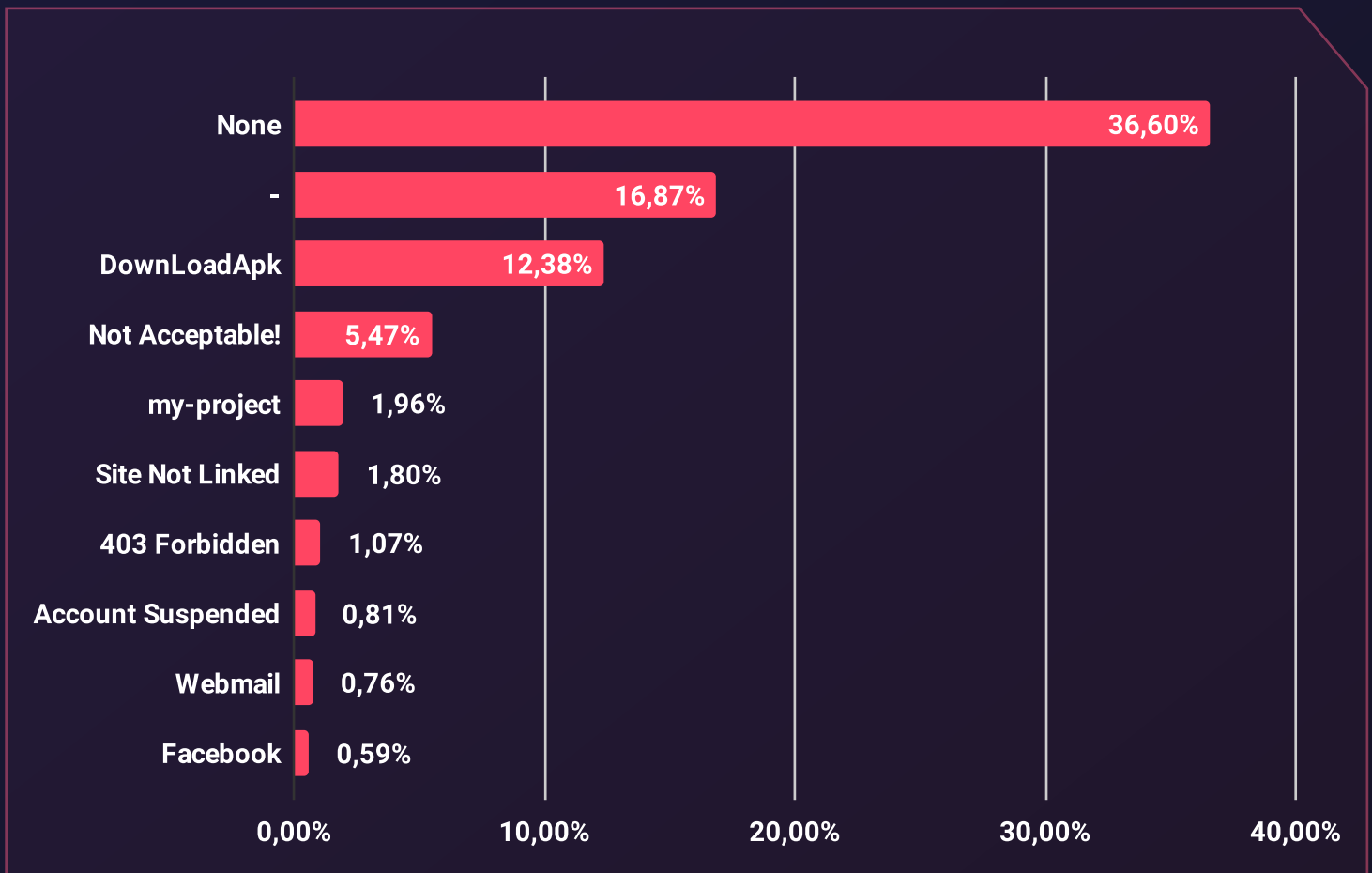
Phishing Threats

Phishing Attacks - Distribution by Industry



The **cryptocurrency** industry in Canada faced the most phishing attacks, with **31,66%** of the total attempts. The **public administration** industry was in the second spot, with **11,24%** of the attacks, and **information services** were targeted at **10,95%**.

Phishing Attacks - Distribution by Phishing Page Title

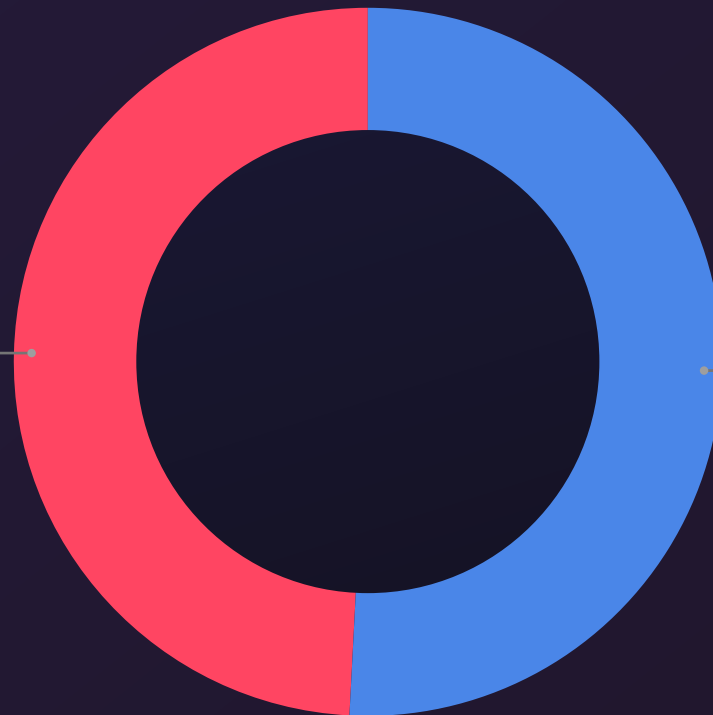


Our analysis shows the most used page titles in phishing attacks.

The data reveals that 36,60% of phishing pages use the “None” title. In second place, we detected “-” on **16,87%** of the pages. Lastly, “**DownLoadApk**” was the third most used title for phishing attempts, with **12,38%**.

Phishing Attacks - Distribution by SSL/TLS Protocol

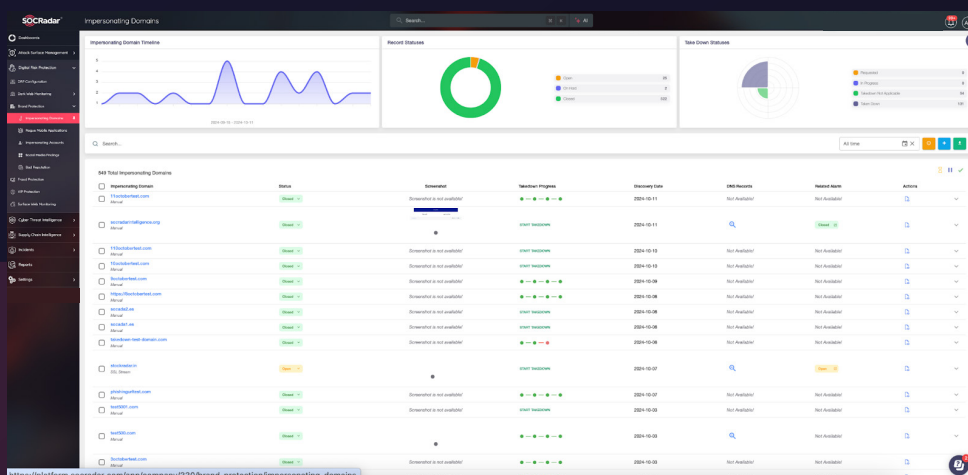
HTTPS
49,2%



HTTP
50,8%

When we analyze the protocols used by phishing websites, we mostly detect HTTP protocols.

In our previous reports, we detected a predominant use of the HTTPS protocol, but threat actors mostly used the HTTP protocol for the pages used in phishing attacks targeting Canada.



With SOCRadar's AI-powered Phishing Domain Detection module, you can swiftly identify malicious domains and protect your brand from phishing threats. Start safeguarding your digital presence today with **SOCRadar—request a free trial and see the platform in action.**

DDoS Attack Statistics

- The peak bandwidth witnessed during a DDoS attack reached 377.34 Gbps, highlighting a significant capacity from the cyber threats.
- The highest recorded throughput during these incidents was 253.56 Mpps.
- Most DDoS attacks lasted between 24.05 Minutes on average.
- 110,722 DDoS attacks were recorded, highlighting the high frequency of cyberattacks and illustrating the general threat landscape for Canadian targets.

The numbers above show that Canada is facing a severe DDoS risk. The attacks don't take too long, but their number and size pose considerable threats to organizations.

Top DDoS Attack Vectors

Attack Vector	Number of Attacks
TCP ACK	54,202
TCP SYN	8,902
DNS Amplification	26,314
ICMP	7,811
TCP SYN/ACK Amp	14,467

Lessons Learned: Key Insights and Strategic Recommendations

Upon reflection of the cyber threat landscape impacting organizations in Canada, several pivotal lessons and recommendations emerge. These insights, coupled with the capabilities of SOCRadar, offer a roadmap for enhancing cyber resilience and preserving operational integrity. The following are the top 5 takeaways from our analysis:

- **Maintain vigilance regarding the evolving cyber threat landscape:**

The cyber threat landscape is dynamically evolving, as evidenced by the surge in Dark Web activity related to Canada and the proliferation of ransomware incidents.

Organizations must stay abreast of these developments and adapt their security strategies accordingly. Leveraging SOCRadar's Cyber Threat Intelligence provides businesses with real-time insights into emerging threats, enabling them to stay ahead of cyber adversaries.

- **Emphasize multi-layered security measures:**

The diverse range of industries targeted by cyber threats underscores the necessity for multi-layered security measures. As demonstrated, threat actors do not discriminate based on industry, necessitating a comprehensive security approach across all sectors, from Information Technology to Public Administration. SOCRadar can support this effort through proactive threat intelligence and monitoring services.

- **Maintain vigilance against ransomware:**

Ransomware remains a significant threat, highlighting the importance of robust defenses and response plans. SOCRadar's threat intelligence capabilities enable businesses to identify potential ransomware threats and develop effective response strategies.

- **Educate and train employees:**

Given the persistent threat of phishing attacks, continuous employee education and training are essential. Familiarity with phishing tactics and detection methods is critical. SOCRadar's solutions can assist by identifying potential phishing domains and raising awareness of the latest phishing techniques.

- **Ensure defense against Stealers:**

Organizations must enhance their defenses against these malicious software. [**SOCRadar's advanced threat intelligence**](#) aids in detecting and mitigating Stealer threats, bolstering the organization's overall security posture.

In conclusion, adopting a proactive, informed, and comprehensive approach to cybersecurity is paramount. By partnering with solutions such as SOCRadar, organizations in Canada can fortify their defenses and effectively navigate the evolving cyber threat landscape.

Who is SOCRadar®?

Your Eyes Beyond

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by
21.000+ companies
in **150+ countries**

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

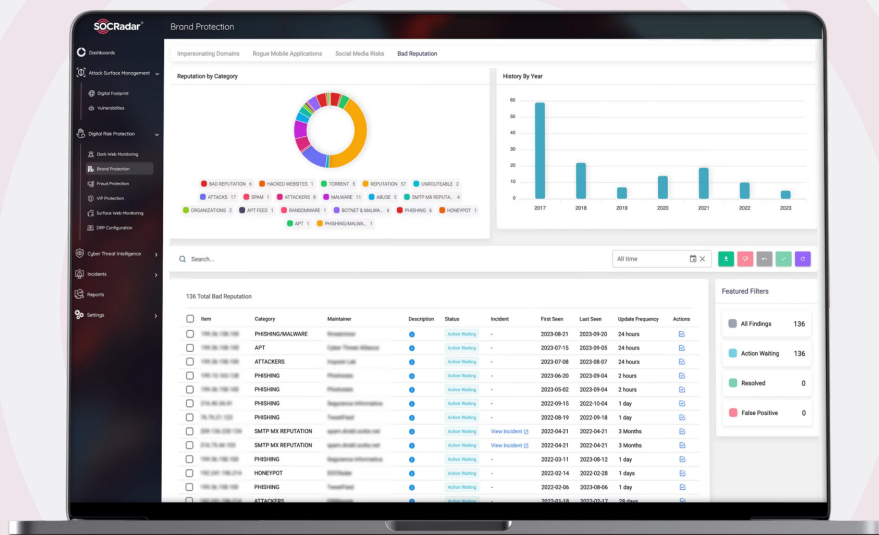
Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.



Start Your Free Trial

**SOCRadar HQ**

HQ Office: 254 Chapman Rd, Ste
208 Newark, Delaware 19702 USA

Call

+1 (571) 249-4598

Email

info@socradar.io

socradar.io

Virtual Addresses**London, UK**

167 City Road Old Street,
London EC1V 1AW

Dubai, UAE

8W building 5th Floor,
DAFZA, Dubai

São Paulo, Brasil

7th & 8th Floors Torre
Joao Salem, Av. Paulista
1079 São Paulo

Bangalore, India

The Estate, 8th Floor
Dickenson Road 560042
Bangalore Karnataka

