NORTH AMERICA

Threat Landscape Report

SOCRadar®
Your Eyes Beyond

socradar.io

Executive Summary

Top Takeaways

- The Finance and Insurance sector experienced the highest volume of threat activity, accounting for 12.11% of all incidents across industries, making it the most frequently targeted sector.
- The United States was by far the most affected country, responsible for 82.15% of all recorded threats in North America, highlighting its high exposure to cyber risks.
- The most common threat category was the selling of stolen data, tools, or services, which made up 58.38% of all identified threat activity.
- Among ransomware groups, PLAY was the most active, linked to 9.19% of all reported ransomware attacks, slightly ahead of other top groups.
- The United States was the primary target for ransomware, with 88.5% of attacks directed at U.S.-based organizations.
- The Public Administration sector received the largest share of phishing attacks, accounting for 18.75%, likely due to the sensitive nature of government data.
- Phishing activity was heavily concentrated in the United States, which accounted for 61.63% of all such attacks, reinforcing its position as the top target in the region.

Technical Details

This report based on data collected between July 2024 and July 2025

In the following chapters, you will be reading about the various aspects of the cyber threat landscape around North America.

In the Dark Web Threats chapter, we will be covering the news and developments from Dark Web Forums, Telegram channels, Discord groups and so on. These are areas where threat actors with various skill sets come together, discuss, share tools and publish their alleged cyber attacks.

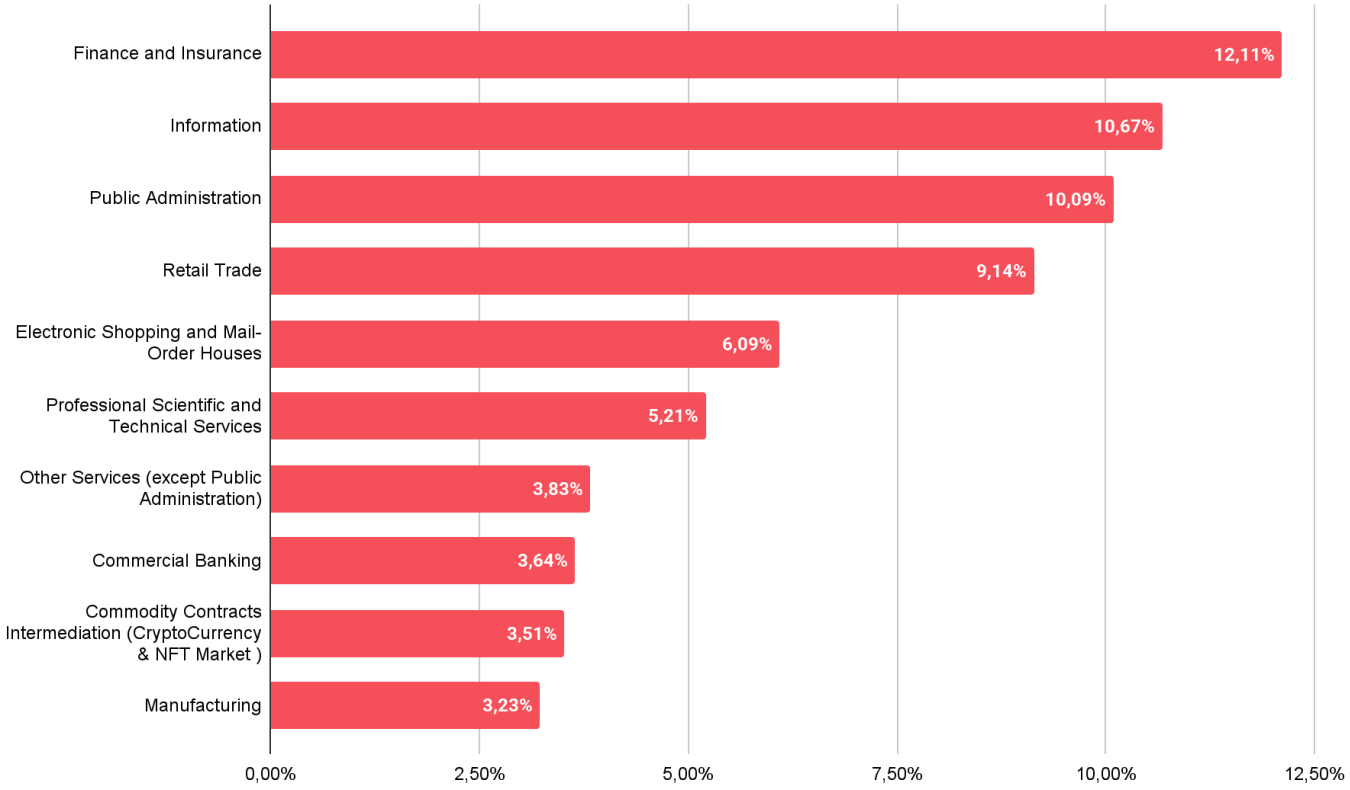
In the Ransomware Threats chapter you will find detailed information about ransomware actors targeting North America, their detailed profiles and the necessary data that summarizes the ransomware activities.

The Phishing Threats chapter will show you how threat actors target various organizations with fake websites. By examining the data here, you can take the necessary steps to prevent your employees from falling into threat actors' traps.

And lastly, the DDoS Attack Statistics shows you the latest information about the intensity of DDoS attacks and how threat actors target organizations to disrupt their operations.

Dark Web Threats Targeting North America

Industry Distribution of Dark Web Threats

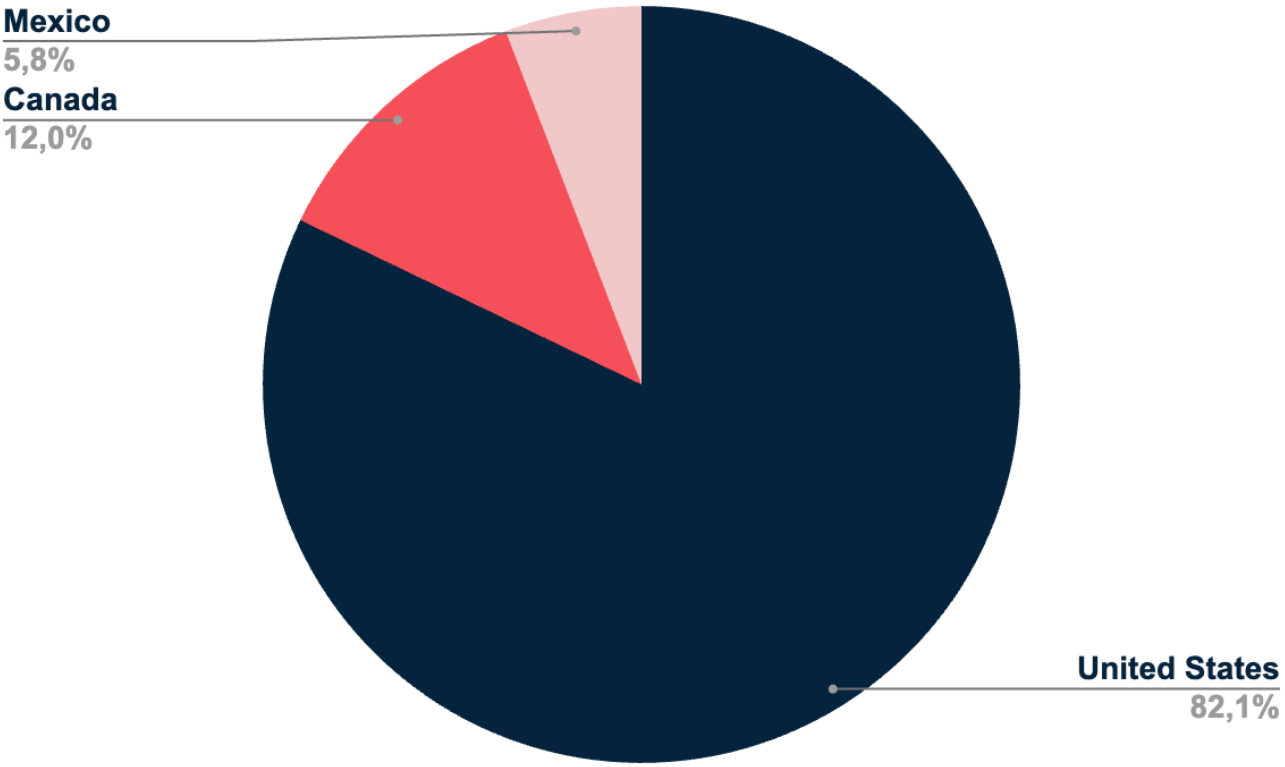


The Finance and Insurance sector has the highest number of threats at 12.11%, making it the most targeted. The Information industry follows closely with 10.67%, indicating significant attention from attackers. Public Administration comes third with 10.09%, suggesting government entities are also major targets.

Additionally, sectors related to cryptocurrencies, NFTs, and commercial banking show meaningful threat activity, each around 3.5%.

Overall, finance, information, and public administration sectors remain primary targets, indicating the need for stronger security measures in these industries.

Distribution of Dark Web Threats by Primary Target Country

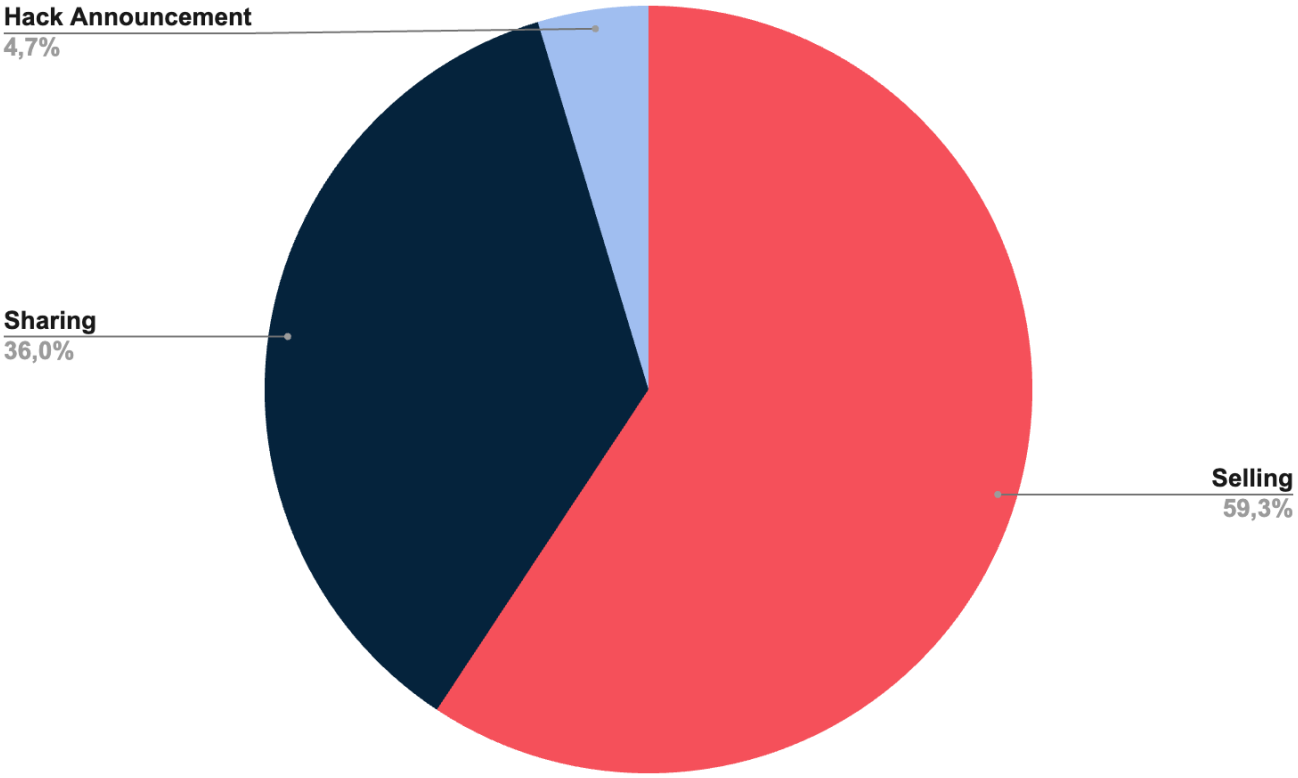


The United States leads significantly with 82.15%, indicating it is the primary target for threat actors in North America. Canada comes second with a considerably lower percentage of 12.01%, highlighting fewer cyber threats compared to the United States. Mexico is last, at 5.84%, showing it faces the least number of reported threats among the three countries.

The high percentage in the United States suggests a larger digital footprint and more attractive targets.

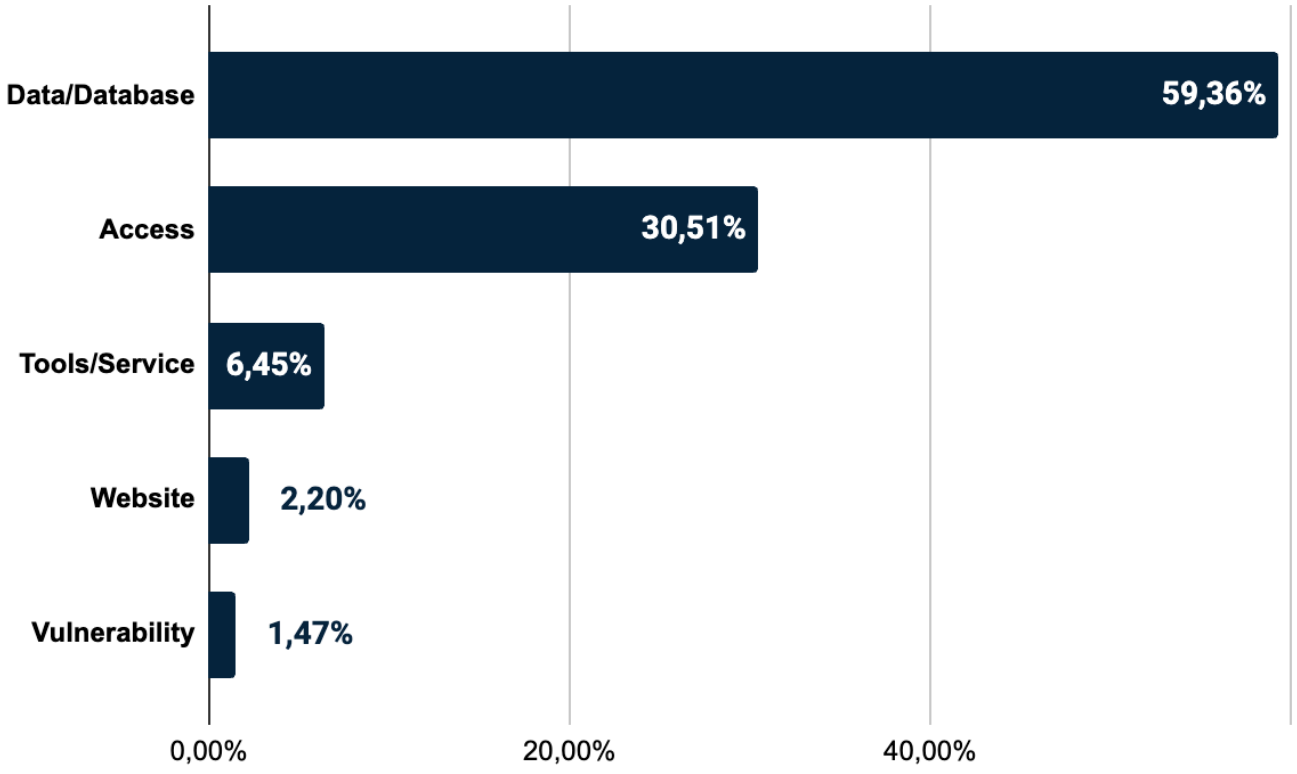
Companies operating in the United States or have a branch there should prioritize their cybersecurity resources and awareness due to their threat landscape.

Distribution of Dark Web Threats by Threat Categories



The largest category, Selling, makes up 59.3% of all threats. This shows attackers commonly sell stolen data or tools, making profit the main driver behind cyber incidents. Sharing is next, accounting for 36%. This indicates that attackers frequently distribute leaked or compromised information openly, increasing exposure risks for affected companies. Lastly, Hack Announcements represent 4.7%, which involve attackers publicly claiming responsibility for breaches. Although this number is much smaller, these threats can severely harm a company's reputation.

Distribution of Dark Web Threats by Threat Type

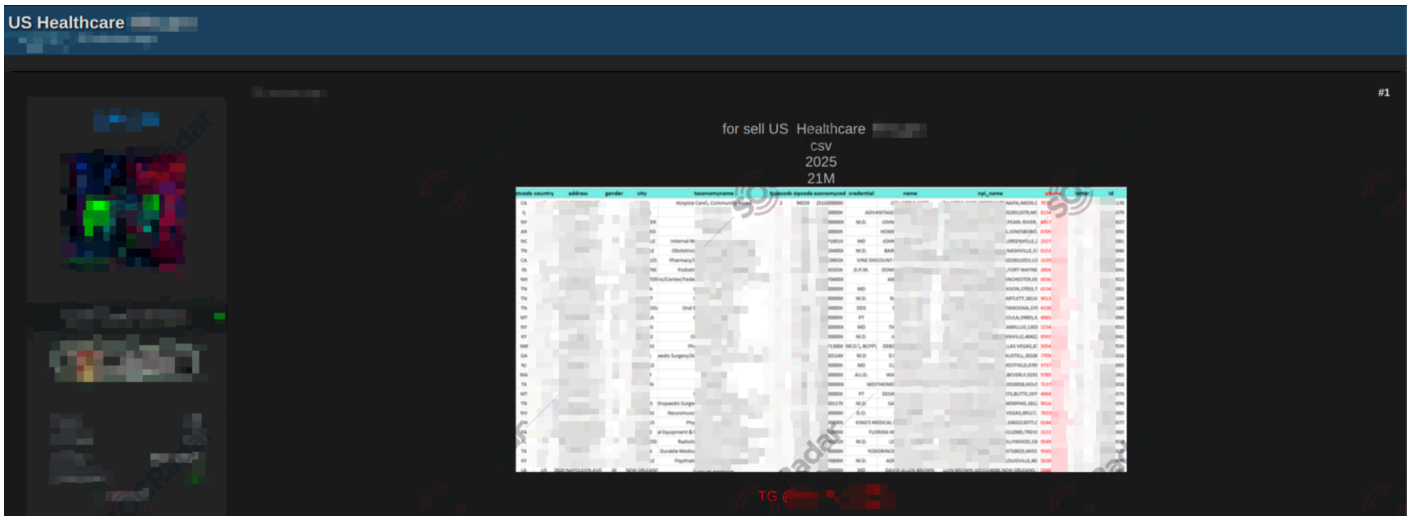


Data and Databases lead with 59.36%, meaning attackers often trade stolen personal or sensitive company information. Access credentials are also a major concern, representing 30.51% of posts. Threat actors regularly sell usernames, passwords, or entry points to compromise organizations. Tools and Services, at 6.45%, refer to malware or hacking software available to attackers.

Businesses should pay close attention to protecting data and securing login credentials since these are the most attractive items for attackers. Monitoring these dark web activities helps companies anticipate threats and strengthen their defenses.

Recent Dark Web Activities Targeting Entities in North America

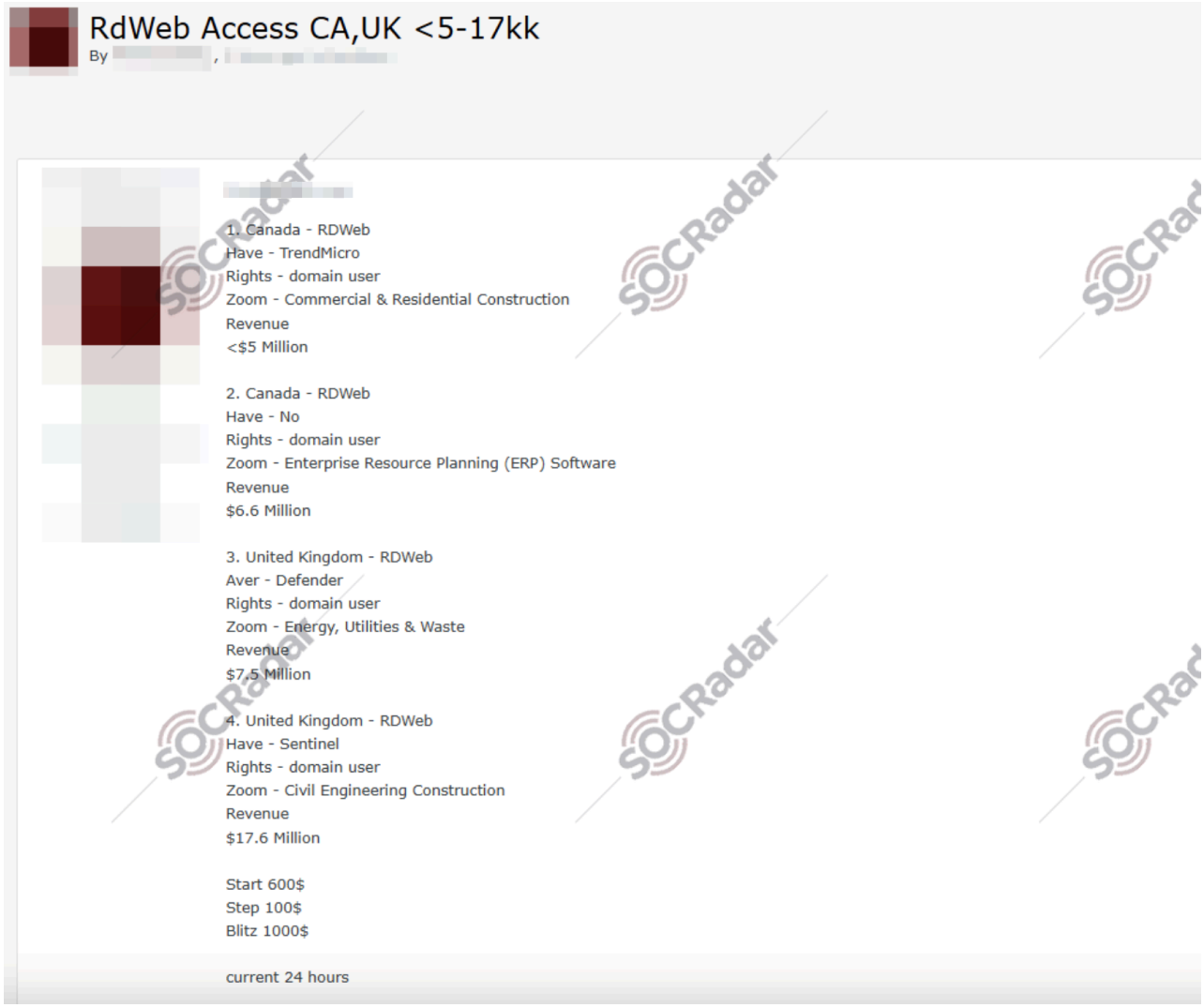
Alleged U.S. Government Health Agency Data Appears for Sale on a Dark Web Forum



A Dark Web forum post has surfaced offering what appears to be stolen data linked to a major U.S. government health agency. The listing advertises a CSV file claimed to contain healthcare-related records connected to a well-known U.S. domain.

The post, dated 2025, suggests that the dataset includes 21 million records and invites interested buyers to connect via Telegram. The seller describes the content simply as “US Healthcare” and references a prominent government health website.

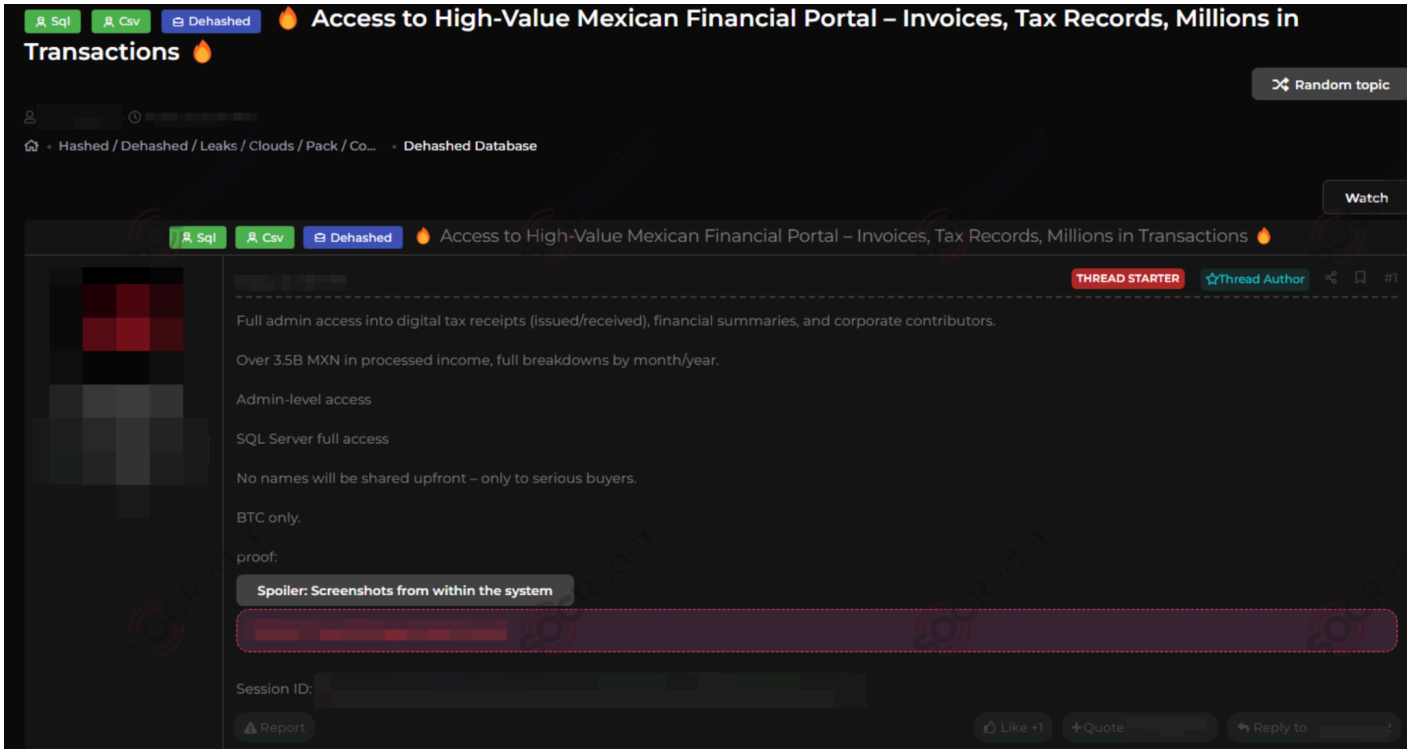
Unauthorized Access to Canadian and British Companies Advertised on a Dark Web Forum



A new listing on a Dark Web forum is offering unauthorized access allegedly tied to multiple companies based in Canada and the United Kingdom. The post includes specific details about systems and sectors involved, with prices starting at $600 and increasing in $100 increments, with a “blitz” price set at $1,000.

The access appears to involve RDWeb portals and domain user-level rights. In Canada, the targets include a commercial and residential construction firm with revenue under $5 million, and an enterprise resource planning (ERP) software company reporting $6.6 million in revenue.

Admin Access to Mexican Financial Platform Allegedly for Sale on a Dark Web Forum



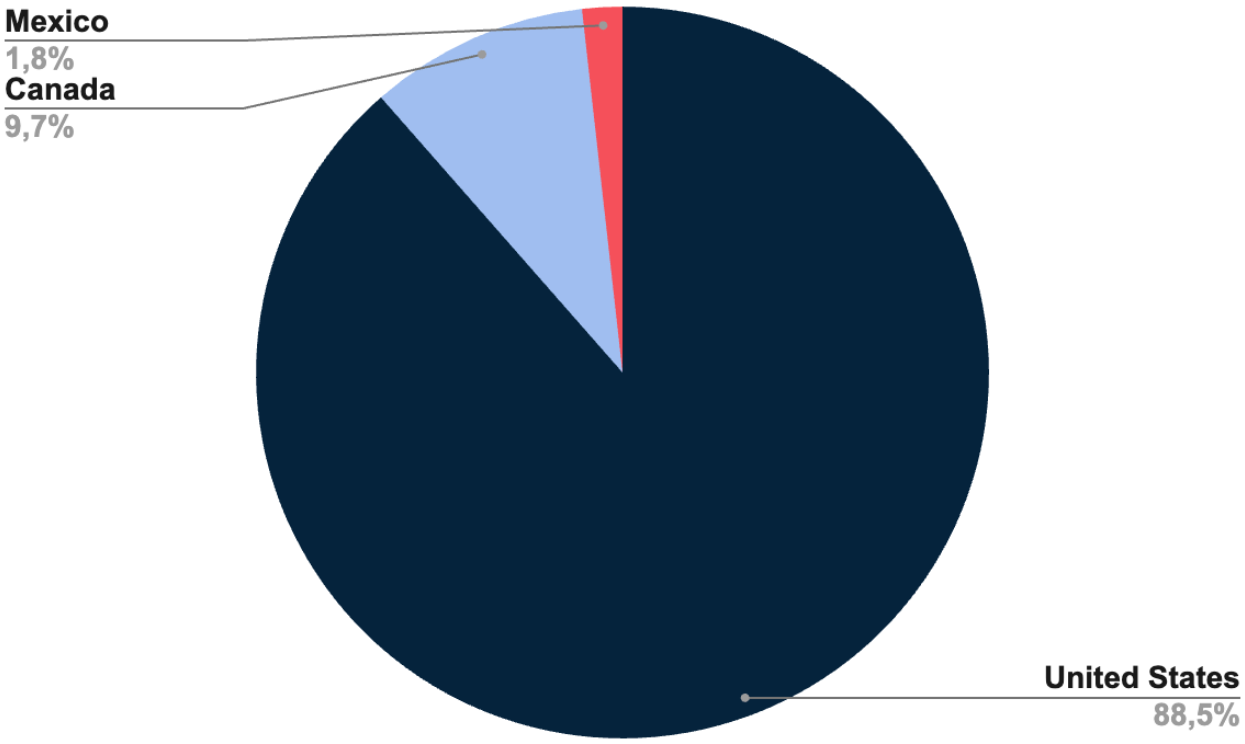
A threat actor has advertised unauthorized admin-level access to a financial portal based in Mexico on a Dark Web forum. The listing claims full control over the platform, including access to digital tax receipts, both issued and received, along with detailed financial summaries and information on corporate contributors.

According to the post, the platform has processed over 3.5 billion MXN in income, with full monthly and yearly breakdowns available. The access reportedly includes full control over the SQL Server, suggesting deep access into the backend infrastructure.

The seller notes that no identifying information will be shared upfront and that access details will be provided only to serious buyers. Transactions are accepted in Bitcoin (BTC) only.

Ransomware Threats Targeting North America

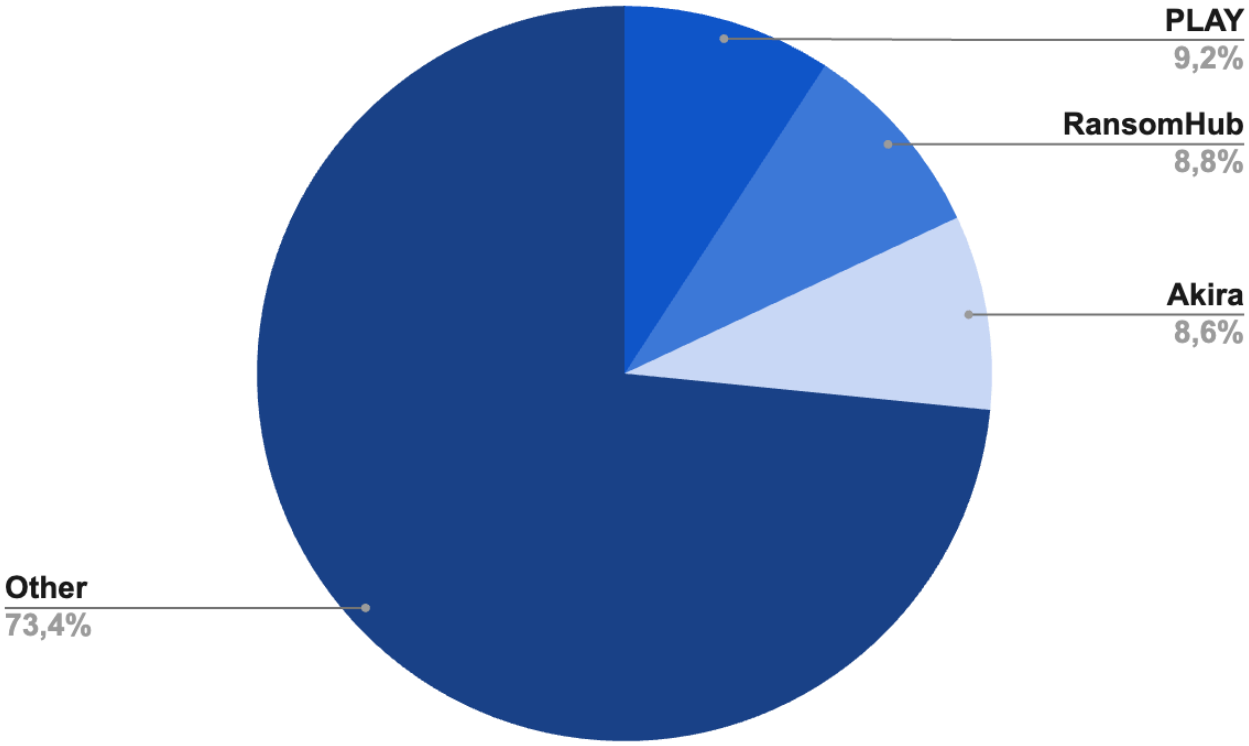
Distribution of Ransomware Attacks by Primary Target Country



The United States experiences the highest impact, with 88.5% of all ransomware incidents. Canada follows with 9.7%, showing fewer attacks compared to the U.S. Mexico has the smallest share, at just 1.8%. High-value businesses, extensive digital networks, and larger financial opportunities likely attract attackers to the U.S. market.

Canadian and Mexican companies, although targeted less, should not underestimate the risks. All countries must stay vigilant and actively strengthen cybersecurity defenses against ransomware threats. However, businesses in the United States, due to their high exposure, must especially focus on prevention, rapid response, and recovery strategies.

Top Ransomware Groups Targeting North America



The PLAY group is the most active, responsible for 9.19% of attacks. Closely behind is RansomHub, making up 8.84%, showing it is also a significant threat. Akira ranks third, causing 8.56% of incidents.

The small differences between these groups mean all three are major players in ransomware threats in North America.

Businesses should stay aware of these groups and track their methods to better defend against them. Companies can prioritize protection against these specific ransomware groups due to their activity.

A Closer Look into The Top 3 Ransomware Groups

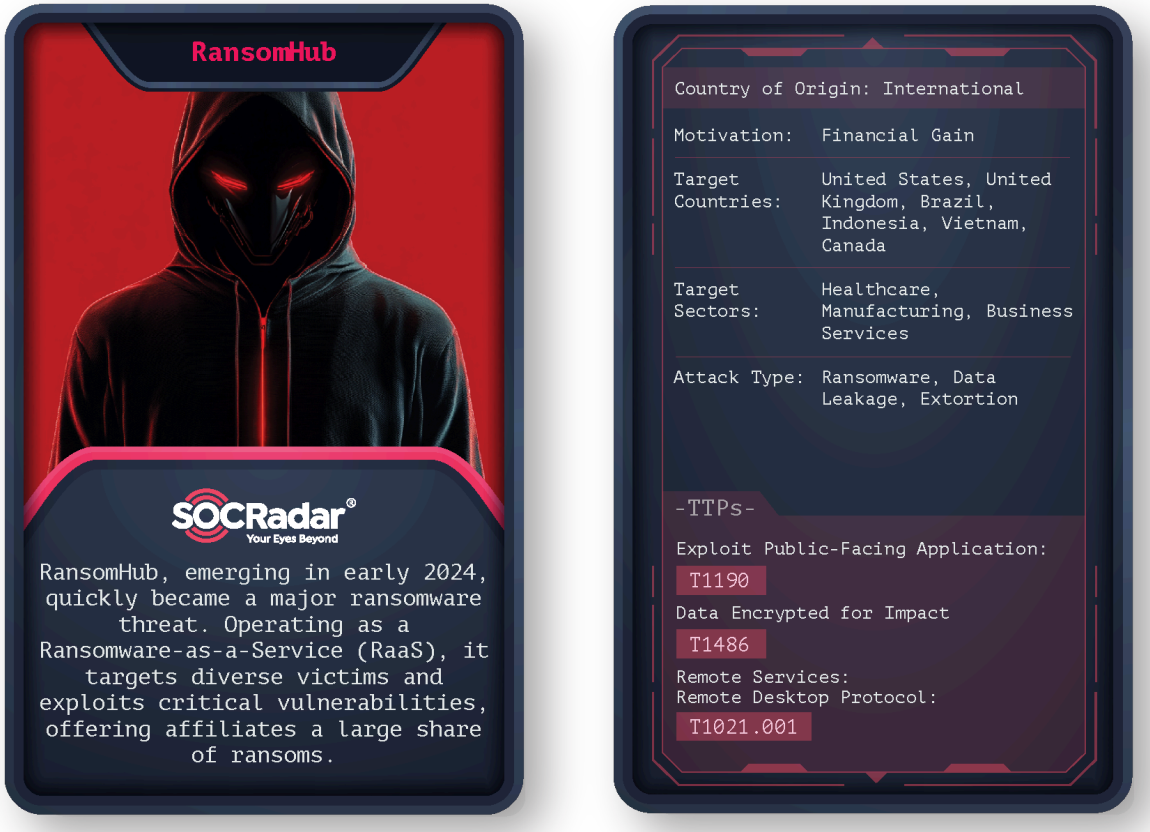
PLAY Ransomware

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.

RansomHub



As stated on the group's About page, RansomHub is comprised of hackers from various locations united by a common goal of financial gain. The gang explicitly mentions prohibiting attacks on specific countries and non-profit organizations. In February 2024, RansomHub posted its first victim, the Brazilian company YKP.

The gang's website states that they refrain from targeting CIS, Cuba, North Korea, and China. While they suggest a global hacker community, their operations notably resemble a traditional Russian ransomware setup. Their stance on Russian-affiliated nations and the overlap in targeted companies with other Russian ransomware groups are also worth noting.

You can visit our ***blog post*** for more detailed information about RansomHub.

Akira

Since its discovery in early 2023, Akira ransomware has evolved from a seemingly ordinary addition to the ransomware landscape to a significant threat affecting many businesses and critical infrastructure entities. This evolution and the unique aesthetic of its leak site and communications have drawn attention to its operations.

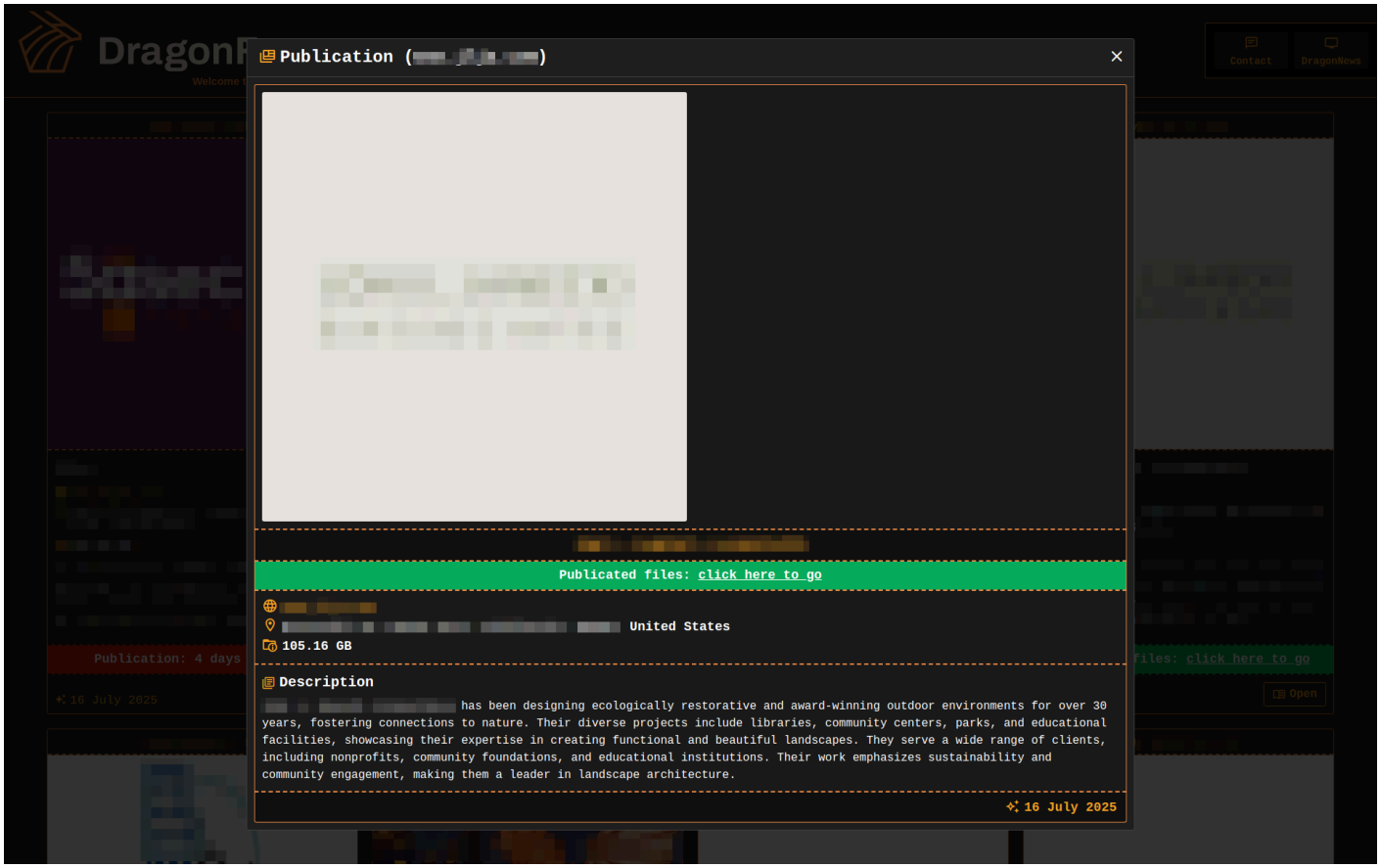
The ransom group employs a double extortion strategy, first exfiltrating data and then encrypting devices within the targeted network. Payment is then demanded not only for decrypting files but also for preventing the exposure of leaked data.

The Akira ransomware group frequently demands hefty ransoms, primarily targeting large enterprises across North America, Europe, and Australia. The malware typically spreads through targeted threat campaigns using phishing emails or exploiting software vulnerabilities, focusing on industries such as education, finance, manufacturing, and healthcare.

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

Recent Ransomware Attacks Targeting Entities in North America

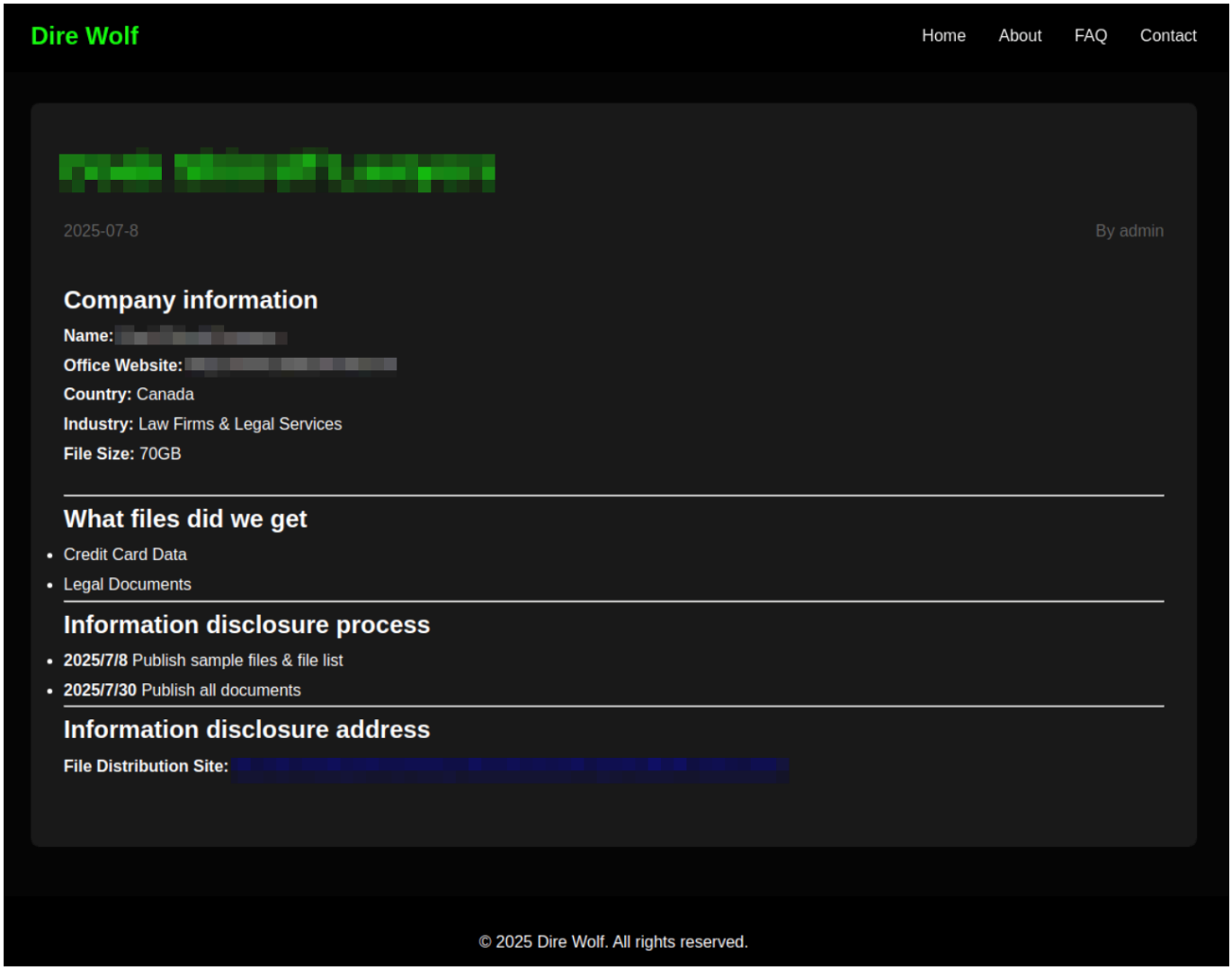
Ransomware Group DragonForce Claims New Victim in Architecture Sector



The ransomware group DragonForce has added a new alleged victim to its leak site. The target appears to be a well-established landscape architecture firm with over 30 years of experience in designing outdoor environments focused on ecological restoration and community impact.

According to the listing, the organization has worked on a variety of public-facing projects, including libraries, parks, community centers, and educational facilities. Their clients reportedly include nonprofits, community foundations, and educational institutions, with a strong focus on sustainability and public engagement.

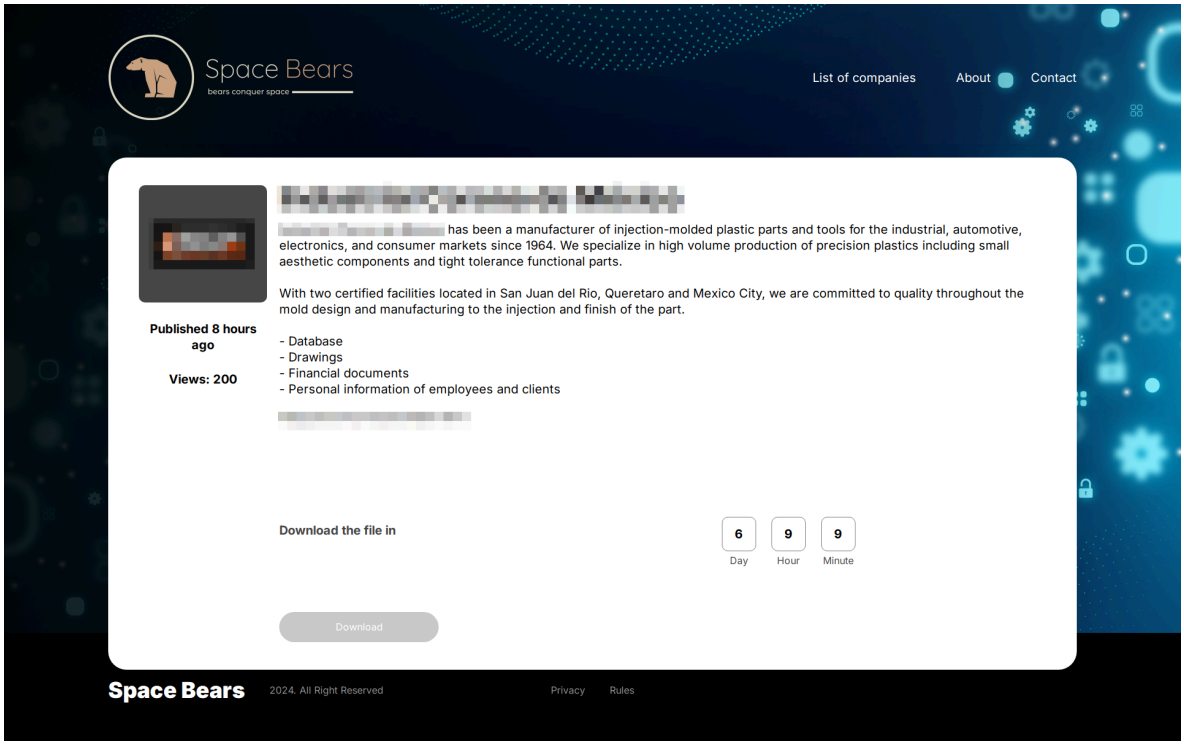
Dire Wolf Ransomware Group Claims Attack on Canadian Legal Services Firm



The ransomware group Dire Wolf has claimed responsibility for a cyberattack targeting a Canadian law firm, according to a post on their leak site. The threat actors allege they have exfiltrated 70GB of sensitive data, including credit card information and a large collection of legal documents.

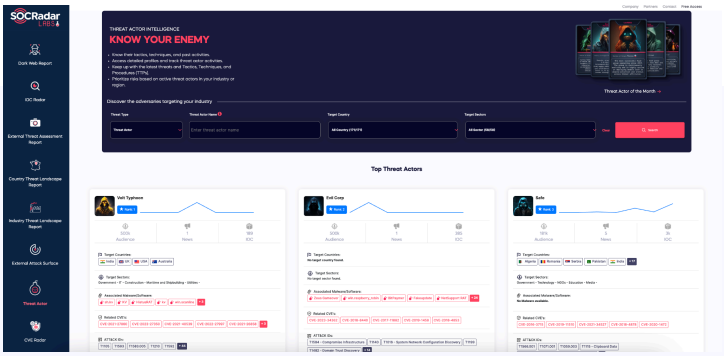
The victim operates in the legal services sector and is based in Canada. The firm is known for offering a range of legal support to individuals and businesses, suggesting the stolen data may involve both personal and corporate clients.

Space Bears Ransomware Group Claims Attack on Mexican Manufacturing Firm



The ransomware group Space Bears has allegedly targeted a manufacturing company in Mexico, according to a new post on their leak site. The victim operates in the plastics and tooling industry, producing high-volume, precision-molded parts for sectors such as automotive, electronics, and consumer goods.

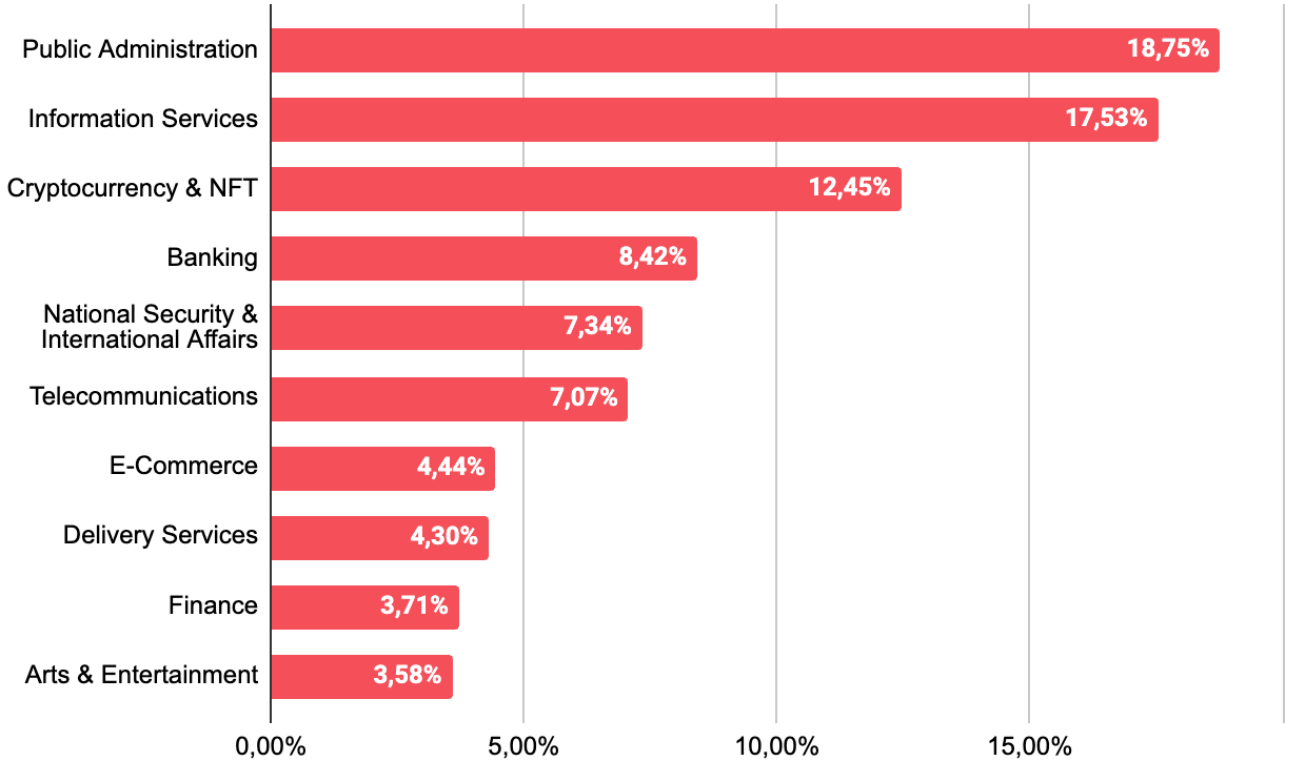
The threat actors claim to have stolen a range of sensitive data, including the company's database, technical drawings, financial documents, and personal information belonging to both employees and clients. The listing suggests that data was taken from operations across two certified facilities located in San Juan del Rio and Mexico City.



*SOCRadar enhances cybersecurity measures with its **Threat Actor Intelligence Module**, which features advanced Threat Actor Tracking capabilities for organizations that want to stay ahead of cyber threats in real time.*

Phishing Threats Targeting North America

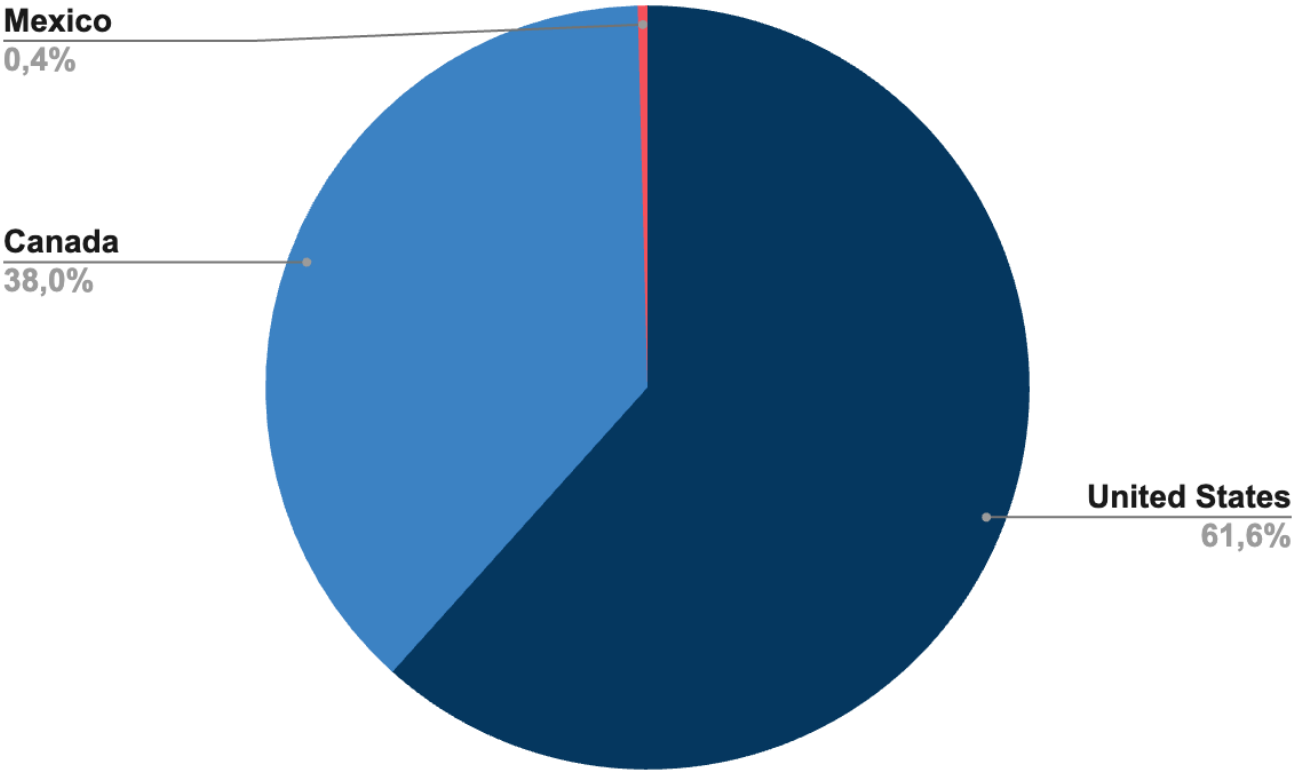
Phishing Attacks - Distribution by Industry



This graph highlights the sectors most affected by phishing attacks. Public Administration leads with 18.75%, showing that government bodies are a major target. Information Services follow at 17.53%, likely due to the high value of data they manage. The Cryptocurrency and NFT sector ranks third at 12.45%, reflecting attackers' interest in digital assets.

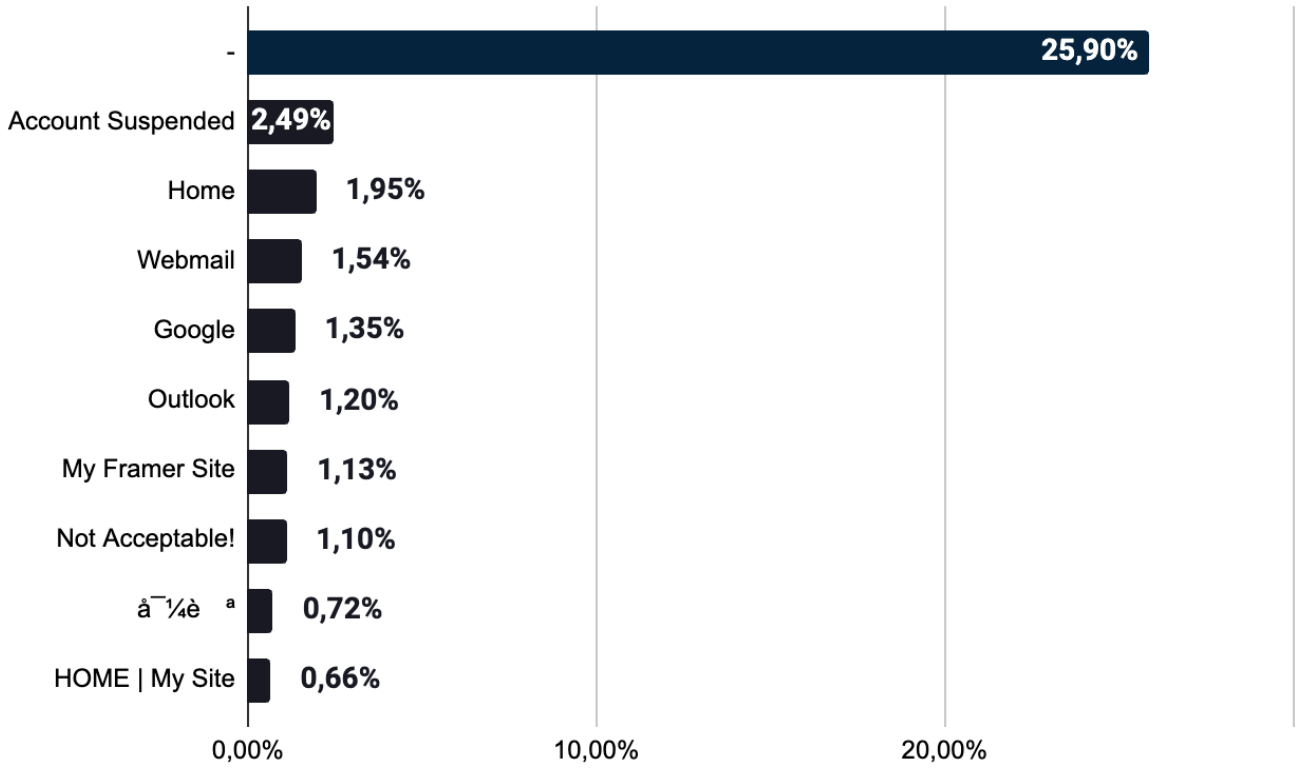
This spread shows that phishing affects both public and private sectors. Attackers aim for industries with valuable data or financial access.

Phishing Attacks - Distribution by Target Country



This graph shows the distribution of phishing attacks by country. The United States has the highest share at 61.63%, making it the top target for phishing campaigns. Canada follows with 37.96%, also facing a significant number of attacks. In contrast, Mexico accounts for only 0.41%, showing minimal phishing activity.

Phishing Attacks - Distribution by Phishing Page Title



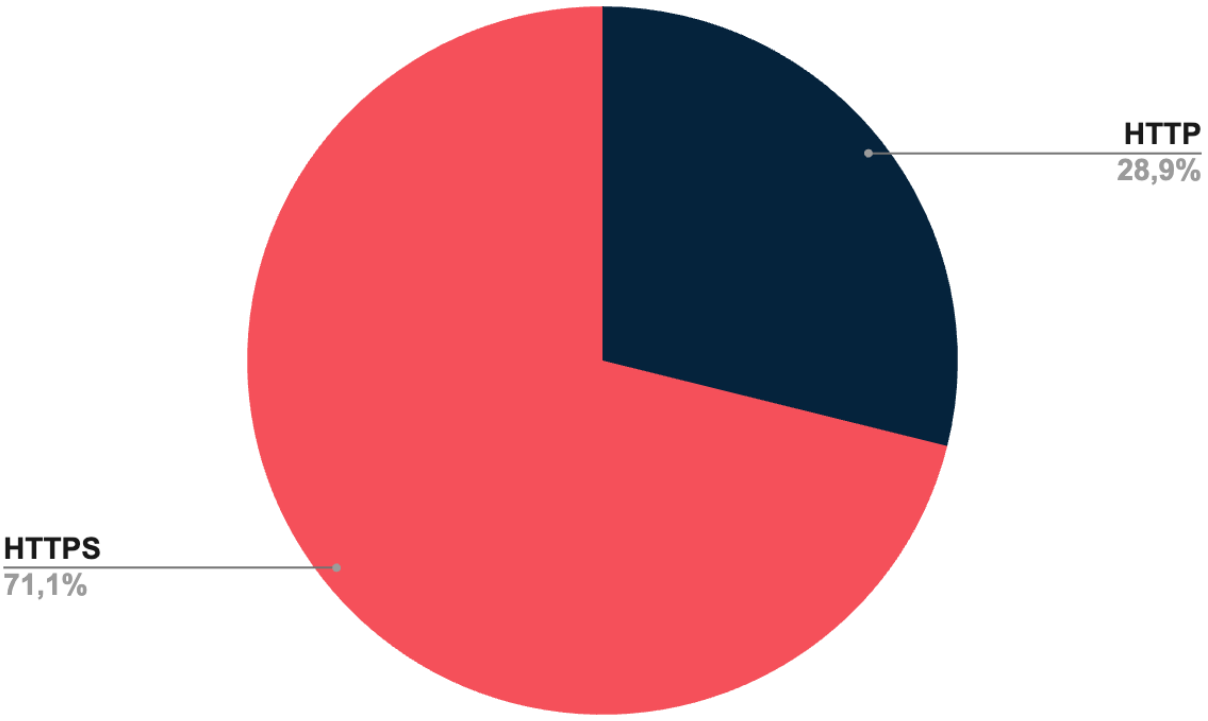
This graph shows the most common phishing page titles. A large portion, 25.90%, had no title (“-”), which suggests attackers try to avoid detection or use blank pages.

The rest of the titles mimic familiar or official terms to appear trustworthy. “Account Suspended” (2.49%) is the most used real title, likely chosen to create urgency and trick users into clicking.

Other common titles include “Home,” “Webmail,” “Google,” and “Outlook,” showing that attackers often copy well-known services to lure victims.

While each of these titles has a low individual percentage, together they show a clear pattern: attackers use fake pages that look like login portals or alerts.

Phishing Attacks - Distribution by SSL/TLS Protocol



Most phishing sites, 71.1%, use HTTPS, while only 28.9% use HTTP. This may seem surprising, as HTTPS is often linked with secure websites. However, attackers now use HTTPS to trick users into thinking a site is safe. The padlock icon in browsers can give a false sense of trust.

This trend shows that users should not rely only on HTTPS to judge a website's safety. Businesses should educate staff and customers to look beyond the padlock and check for signs of phishing.

DDoS Attack Statistics

The threat landscape was pretty active for North America.

- The **peak bandwidth** witnessed during a DDoS attack reached 1857,31 Gbps, highlighting a significant capacity from the cyber threats.
- The **highest recorded throughput** during these incidents was 653,51 Mpps.
- Most DDoS attacks lasted **49 minutes** on average.
- **1.485.121 DDoS attacks** were recorded, highlighting the high frequency of cyberattacks and illustrating the general threat landscape for North American targets.

The numbers above show that the North America faces a serious DDoS risk. The attacks don't take too long, but the amount of attacks and their size are considerable threats to organizations.

Top DDoS Attack Vectors

Attack Vector	Number of Attacks
TCP ACK	381,78
ICMP	316,61
DNS Amplification	251,199
TCP SYN	223,84
TCP RST	148,821

Strategic Recommendations

- **Enhance Endpoint Security:** Implement advanced anti-malware, regular device audits, and employee training on safe browsing practices.
- **Strengthen Phishing Defense:** Invest in phishing detection systems, web filtering tools, and employee training on recognizing phishing attempts.
- **Enforce Multi-Factor Authentication (MFA):** Apply MFA across critical systems to protect against stolen credentials.
- **Fortify Ransomware Defenses:** Regularly back up data, segment networks, and develop incident response plans for ransomware attacks.
- **Monitor Dark Web Activity:** Use dark web monitoring to detect exposed company data early and respond quickly to breaches.
- **Collaborate on Cyber Threat Intelligence:** Share insights with industry peers and stay informed about emerging threats and new attack vectors.
- **Secure Communications and Data:** Ensure encryption for sensitive communications and transactions, and train employees on secure data handling.
- **Proactive Vulnerability Management:** Regularly apply patches and conduct penetration testing to address potential system vulnerabilities.
- **Build a Cybersecurity Culture:** Foster ongoing employee training, phishing simulations, and establish clear security policies to ensure a security-first mindset across the organization.

Who is SOCRadar?

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.