GLOBAL LOGISTICS & TRANSPORTATION INDUSTRY

Threat Landscape Report

SOCRadar®
Your Eyes Beyond

socradar.io

Table of Contents

Executive Summary

Top Takeaways

- The majority of stealer logs are related to the **Transportation and Warehousing** sector (64.33%), with **FedEx, UPS, and DHL** leading the list of domains. These global giants face the brunt of cyber threats due to their central role in global trade and logistics.

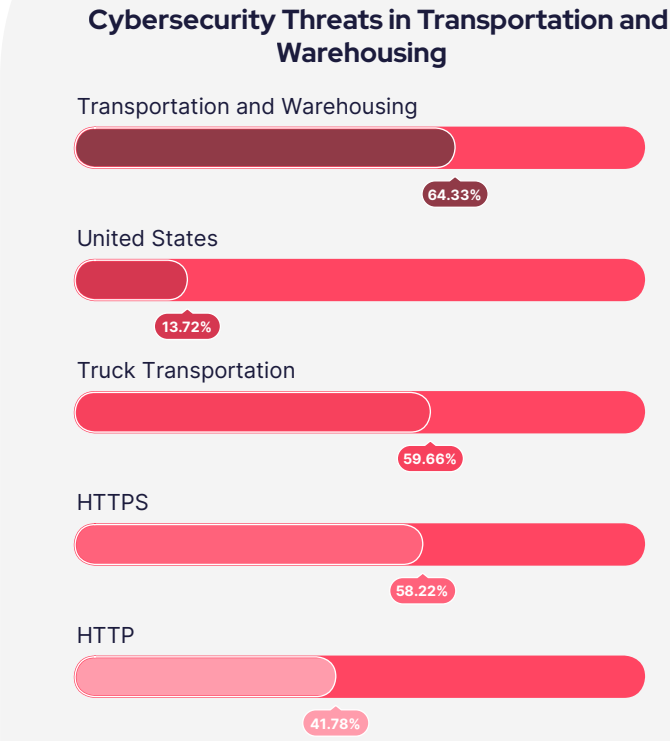
- The **United States (13.72%)** stands out as the top target by threat actors, followed by **Ukraine and the United Kingdom**. The U.S. is a prime focus for attackers due to its vast logistics network, while Ukraine's geopolitical situation has made it a target for state-sponsored cyberattacks.

- **Truck Transportation (59.66%)** is the most targeted sub-sector for ransomware attacks, highlighting the vulnerability of fleet management and logistics coordination systems. **Water and Air Transportation** are also heavily targeted, indicating a broad attack strategy aimed at halting global trade.

- Over **2.28 million credentials** and **117K victim IPs** have been exposed through stealer malware, indicating widespread compromises of logistics employees' personal or corporate devices. **Password hashes** and **credit card details** are also at risk, underscoring the need for enhanced endpoint security and credential management.

- **DHL** is a frequent target of phishing campaigns, with attackers leveraging **tracking and delivery status pages** to steal sensitive information.

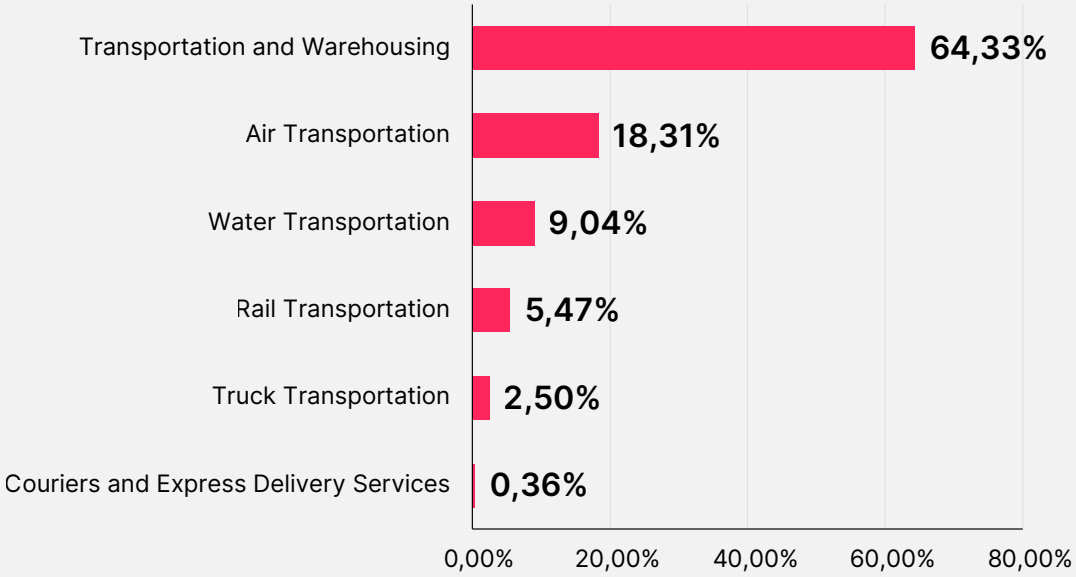
- While **HTTPS (58.22%)** is more commonly used in phishing attempts, the use of **HTTP (41.78%)** remains a significant concern. This underscores the importance of web filtering and **user education on secure browsing practices**.



Technical Details

Dark Web Threats

Distribution of Dark Web Threats by Industry



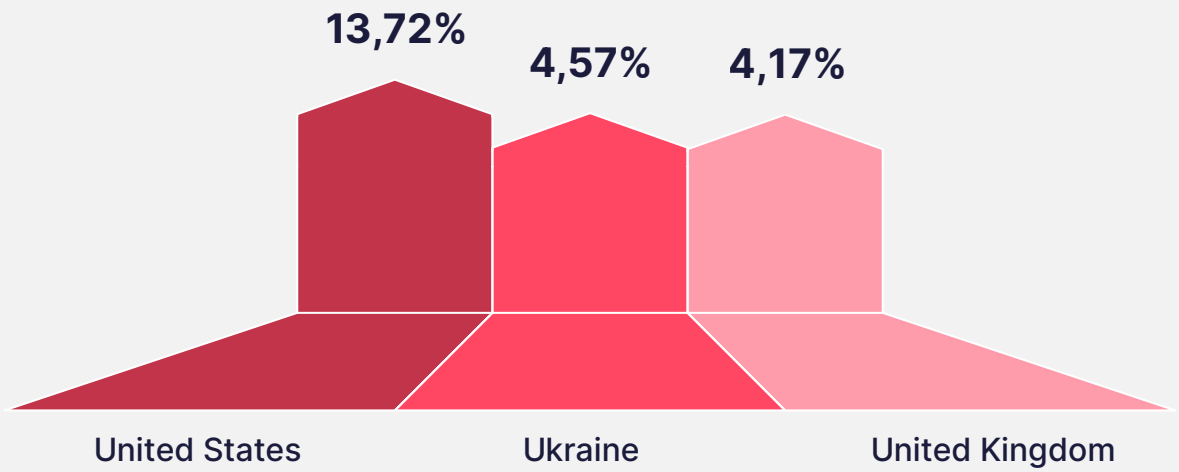
The Transportation and Warehousing sector is the most targeted (64.33%), indicating that cybercriminals prioritize broad supply chain disruptions, likely aiming at third-party logistics providers and warehouse management systems.

Air Transportation (18.31%) follows, likely due to the critical nature of airline operations and valuable passenger/cargo data. Water (9.04%) and Rail Transportation (5.47%) are less targeted but still significant, possibly due to their role in global trade and freight movement.

Truck Transportation (2.50%) and Couriers & Express Delivery (0.36%) face minimal exposure, suggesting lower digital attack surfaces or less financially lucrative data for threat actors.

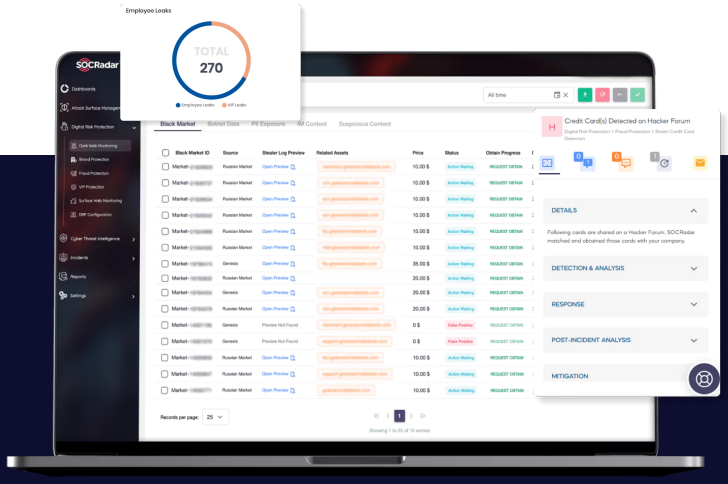
This distribution highlights the need for enhanced cybersecurity in logistics hubs and supply chain networks, particularly for warehousing and large-scale transport providers.

Distribution of Dark Web Threats by Country



The United States (13.72%) is the most targeted, likely due to its vast logistics infrastructure and the presence of major global supply chain hubs. Ukraine (4.57%) stands out, potentially linked to geopolitical cyber warfare and disruptions in critical transport networks.

This data suggests attackers prioritize major economies and geopolitical hotspots, emphasizing the need for regional cybersecurity collaboration and industry-wide threat intelligence sharing.

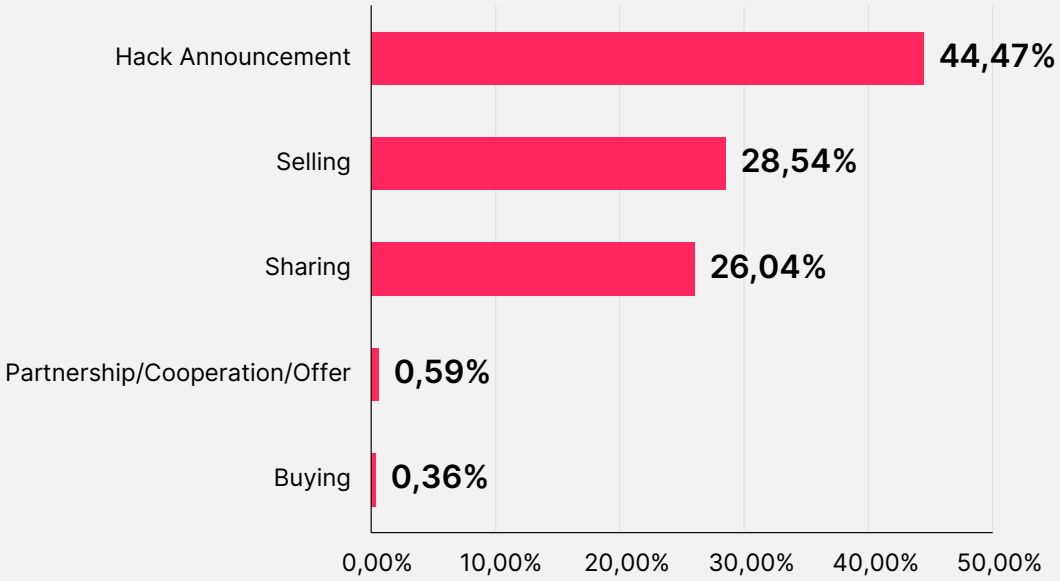


SOCRadar's Advanced Dark Web Monitoring

SOCRadar's Advanced Dark Web Monitoring provides Spanish organizations with critical insights into hidden threats targeting their sectors, including Retail Trade, finance, and Insurance, which have faced significant risks over the past year. With real-time tracking of underground chatter and sensitive data exposure, SOCRadar enables proactive defense against Dark Web threats.

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

Distribution of Dark Web Threats by Threat Categories



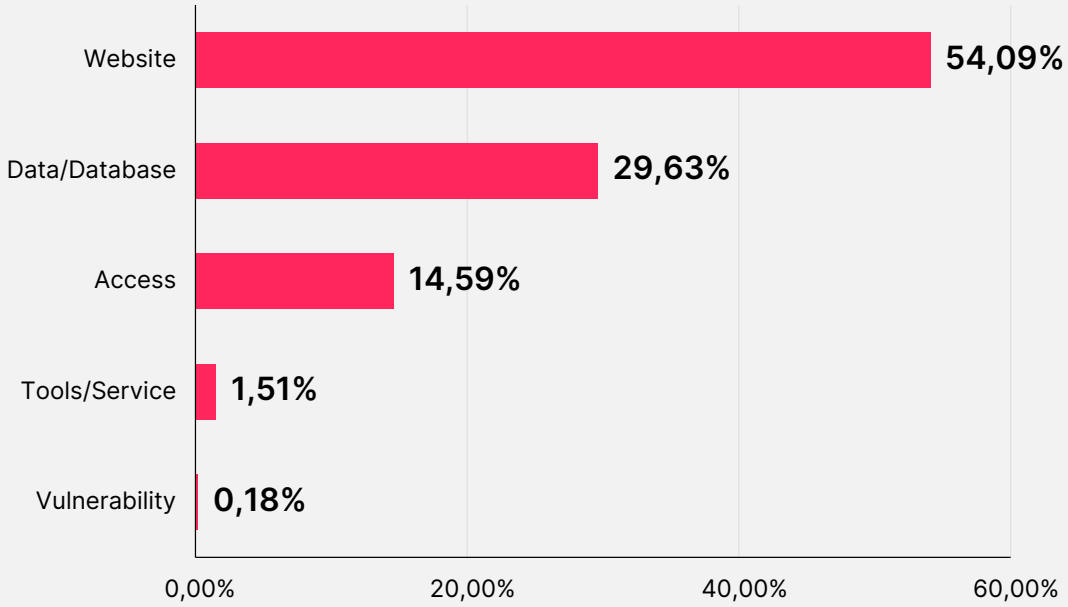
The high percentage of Hack Announcements (44.47%) suggests that cybercriminals prioritize publicizing breaches, likely to enhance their reputation, intimidate victims, or attract buyers for stolen data.

Selling (28.54%) and Sharing (26.04%) indicate that logistics-related breaches often lead to data monetization or free distribution of stolen assets, posing risks of credential stuffing, fraud, and supply chain disruptions.

Partnership/Cooperation/Offer (0.59%) and Buying (0.36%) are minimal, implying that direct purchases or collaboration among criminals are secondary compared to selling and exposure strategies.

This trend highlights the need for proactive cyber defense, breach monitoring, and dark web surveillance to mitigate risks before stolen data is exploited.

Distribution of Dark Web Threats by Threat Types



The dominance of Website-related posts (54.09%) suggests that cybercriminals frequently target or discuss compromised logistics websites, possibly for defacement, phishing, or credential leaks.

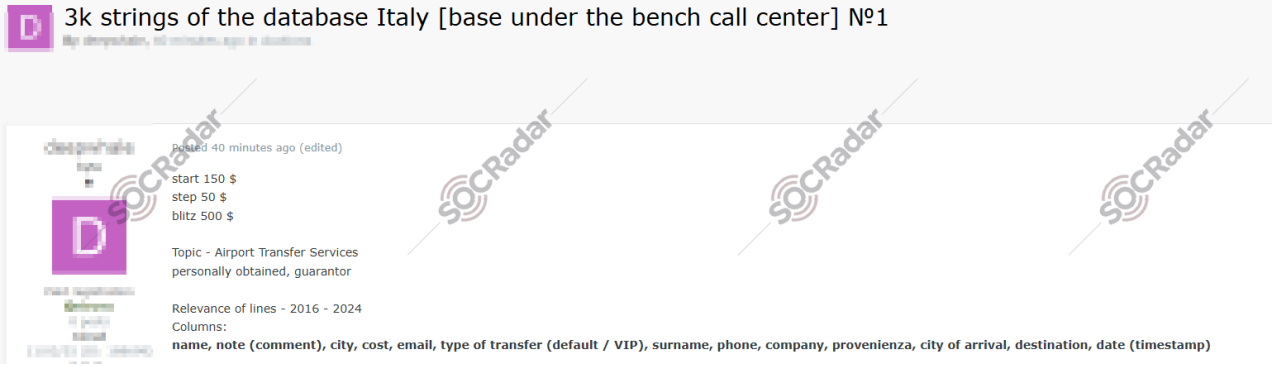
Data/Database (29.63%) postings indicate a significant focus on stolen sensitive records, such as customer information, shipment details, or internal logistics systems data.

Access (14.59%) implies that threat actors are actively selling or distributing unauthorized entry points, likely involving compromised credentials, RDP, VPN access, or initial footholds into company networks.

This emphasizes the need for strong website security, data encryption, and access controls to mitigate exposure on dark web forums.

Recent Dark Web Activities Targeting the Logistics Industry

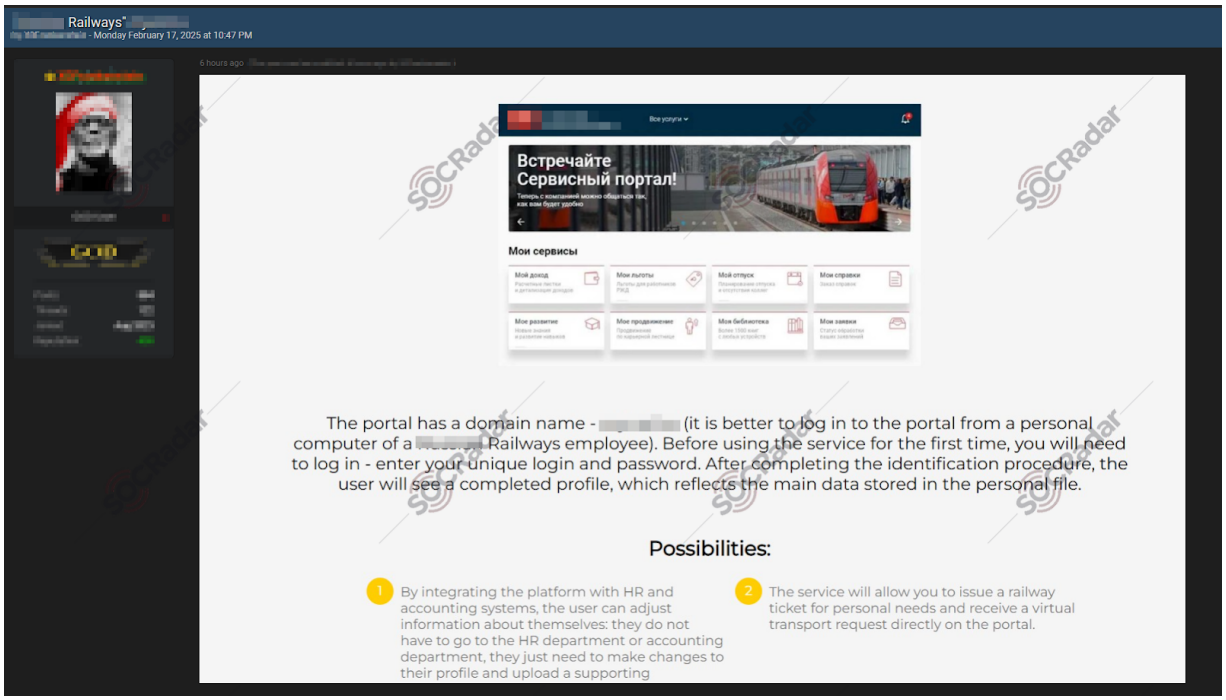
The Alleged Database of a European Airport Transfer Service is Leaked



A threat actor has reportedly claimed responsibility for leaking a substantial database containing sensitive information about an airport transfer service based in a European country. The post, which surfaced on a dark web forum monitored by SOCRadar, allegedly reveals details of customers who utilized the service between 2016 and 2024.

According to the threat actor, the database includes various types of information such as names, surnames, email addresses, phone numbers, the type of transfer (default or VIP), and even timestamps of the bookings. In addition, other details like the origin city, destination, and company names are reportedly included in the data.

The Alleged Database of a Railway Company is Leaked

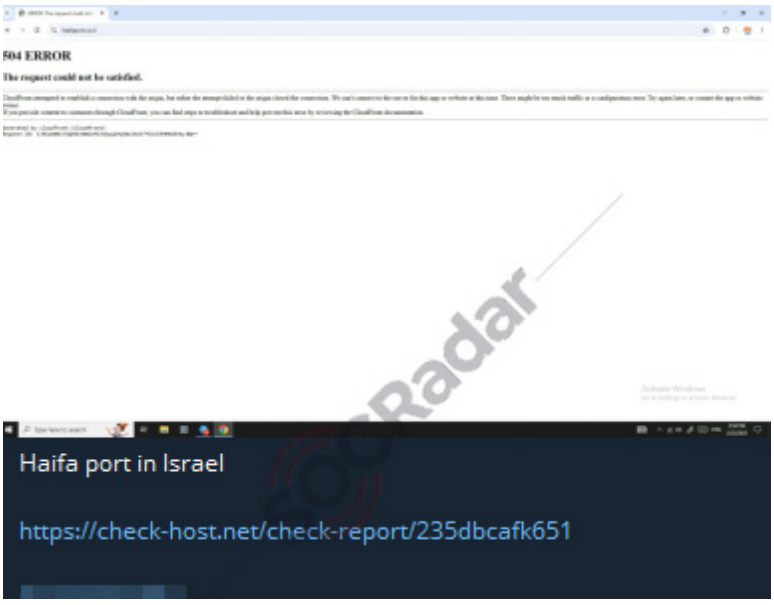


A threat actor claiming to have obtained sensitive data from a railway company located in Eastern Europe. The alleged leak reportedly involves 570,000 records, which are said to be in JSON format. According to the post, the file is 753MB in size and has been compressed to 35MB.

Dark Storm Team Conducted DDoS Attack on a Port-Shipping & Cargo Company

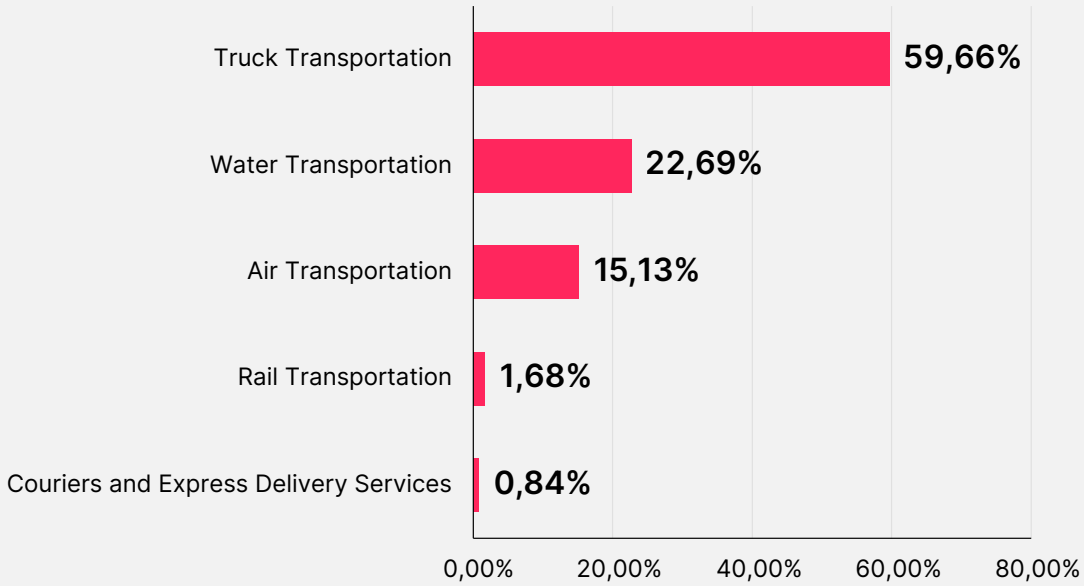
The post, published on a Telegram channel, purportedly details the group's intention to launch a Distributed Denial of Service (DDoS) attack against the port's digital infrastructure.

The allegations made by the purported hacker, who remains unidentified, suggest that the attack could disrupt operations at the port, which is a key entry point for goods entering into the country.



Ransomware Threats

Distribution of Ransomware Attacks by Industry



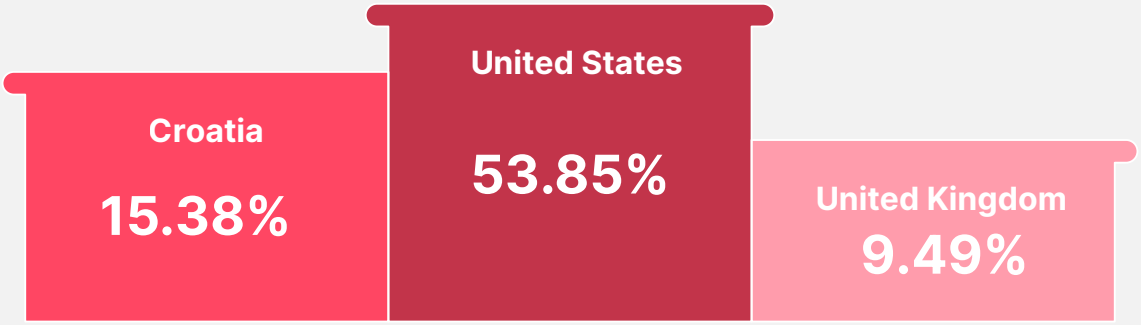
Truck Transportation (59.66%) is the primary target, likely due to high dependency on digital fleet management, GPS tracking, and logistics coordination systems. Disrupting these operations can cause severe supply chain delays, making companies more likely to pay ransoms.

Water Transportation (22.69%) and Air Transportation (15.13%) also face significant ransomware threats, reflecting their critical role in global trade and passenger movement. Attacks on these sectors can lead to port shutdowns, flight disruptions, and cargo delays.

Rail Transportation (1.68%) and Couriers & Express Delivery (0.84%) see minimal targeting, possibly due to lower digital integration or stronger resilience measures in these industries.

This distribution suggests that ransomware groups focus on high-impact, high-disruption targets, reinforcing the need for network segmentation, regular backups, and ransomware-specific threat detection in logistics cybersecurity strategies.

Distribution of Ransomware Attacks by Country



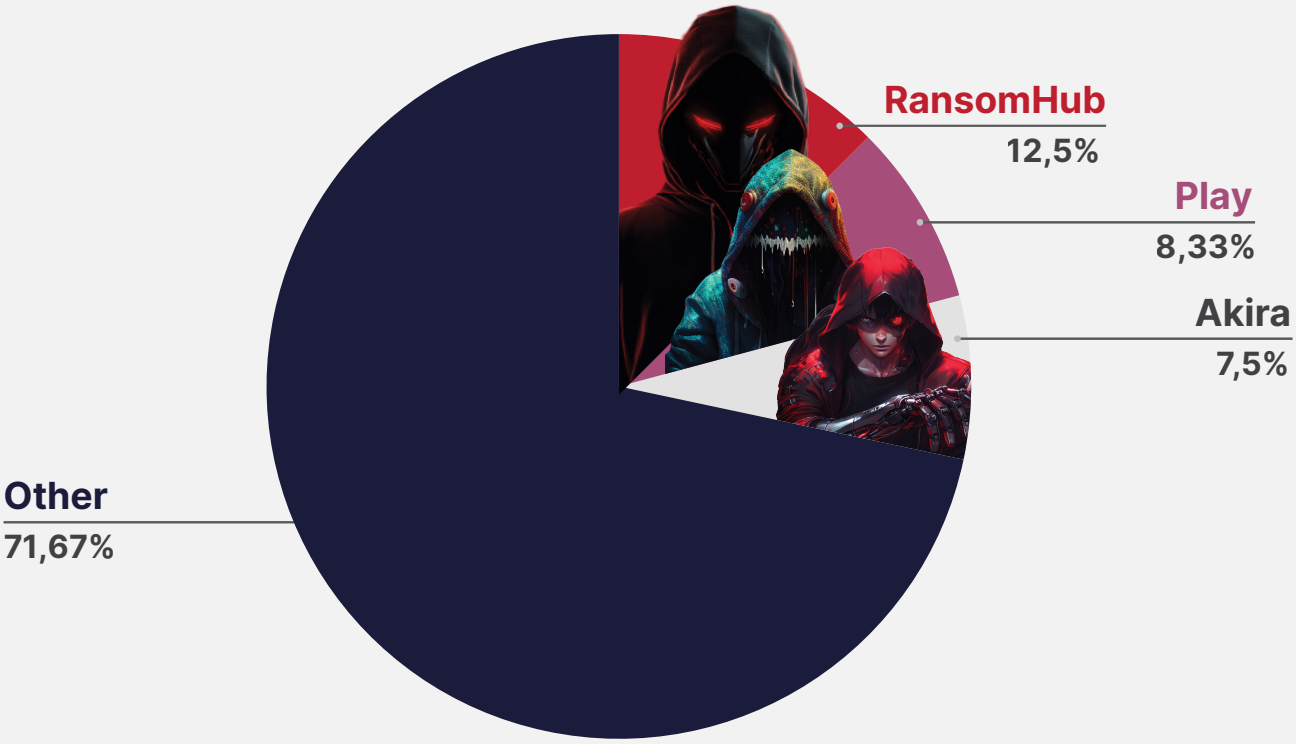
The United States (53.85%) dominates ransomware incidents in logistics, likely due to its vast supply chain network, reliance on digital logistics platforms, and high-value targets. The U.S. is a prime focus for ransomware groups seeking large payouts and operational disruption.

Croatia (15.38%) is a surprising second, possibly indicating targeted attacks on critical maritime infrastructure or regional logistics hubs essential for European trade.

The United Kingdom (9.49%) faces steady ransomware threats, reflecting its major role in global shipping, air freight, and supply chain operations.

The heavy U.S. concentration suggests that ransomware groups prioritize wealthier economies with high digital dependency, emphasizing the need for stronger cyber resilience, rapid incident response, and industry-wide collaboration to counter these attacks.

Top Ransomware Groups Targeting the Logistics Industry



The RansomHub (12.5%) group leads in logistics attacks, likely due to its focus on high-value targets and double extortion tactics (data theft + encryption).

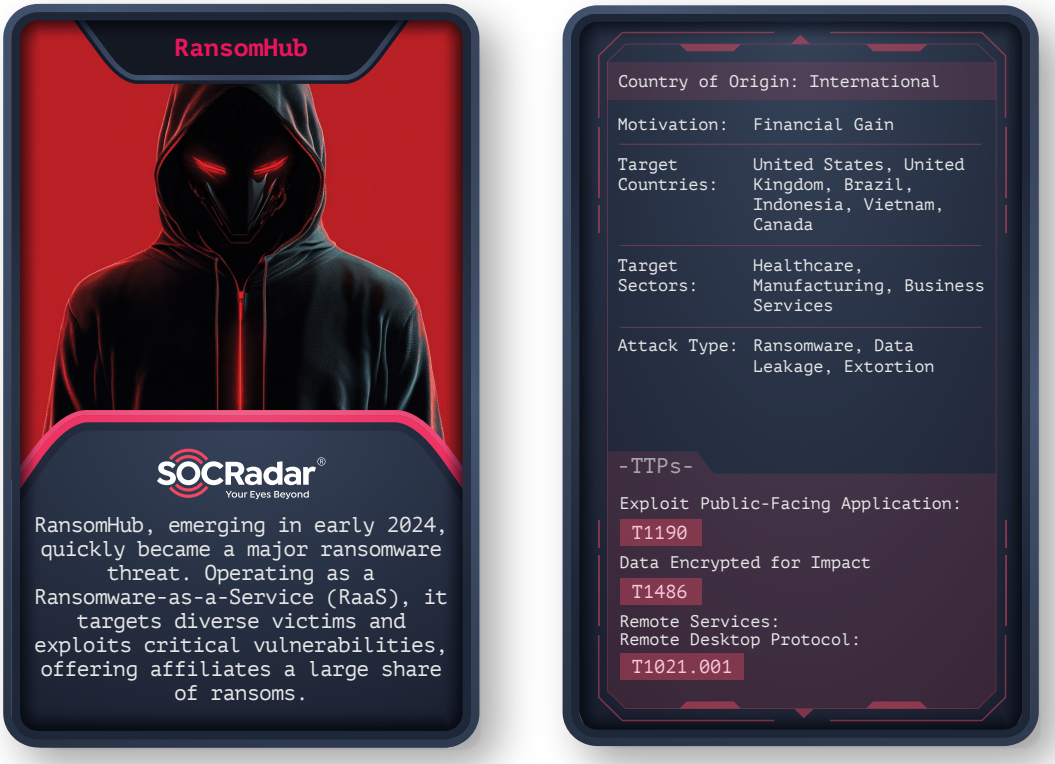
Play (8.33%) and Akira (7.5%) follow, both known for aggressive targeting of critical industries and leveraging customized ransomware payloads to maximize disruption.

The "Other" category (71.67%) suggests a diverse threat landscape with many smaller or emerging ransomware groups attacking logistics firms, making detection and mitigation more complex.

This data highlights the need for proactive ransomware defense strategies, including zero-trust security models, network segmentation, and robust incident response planning to counter evolving threats.

A Closer Look into The Top 3 Ransomware Groups

RansomHub



As stated on the group's About page, RansomHub is comprised of hackers from various global 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.

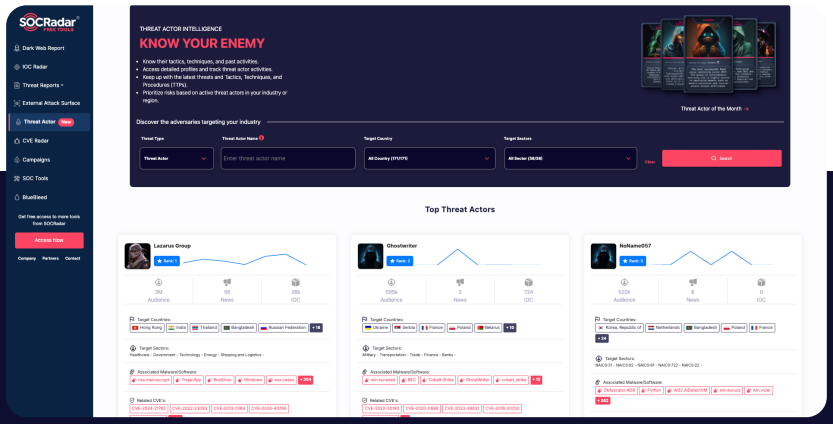
You can visit our *blog post* for more detailed information about RansomHub.

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.



Threat Actor Intelligence Module

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.

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.

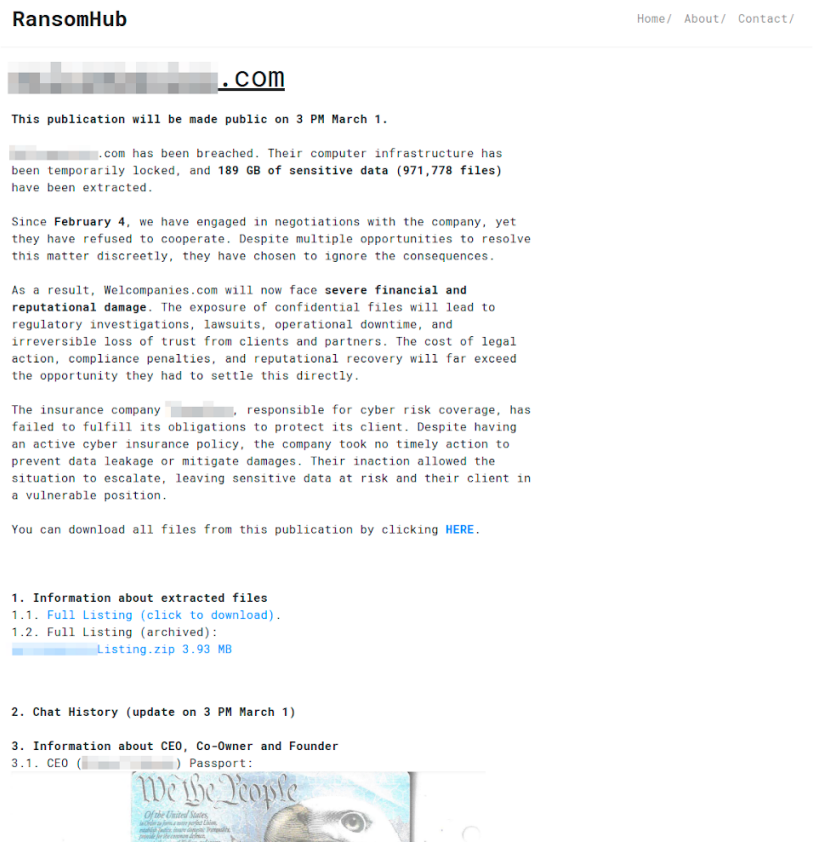
The ransom group employs a double extortion strategy, first exfiltrating data and then encrypting devices within the targeted network. Payment is then demanded not only for decrypting files but also for preventing the exposure of leaked data.

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 Targeted the Logistics Industry

RansomHub Targeted a Refrigerated Freight and Logistics Company


RansomHub

Home/ About/ Contact/

[redacted].com

This publication will be made public on 3 PM March 1.

[redacted].com has been breached. Their computer infrastructure has been temporarily locked, and **189 GB of sensitive data (971,778 files)** have been extracted.

Since **February 4**, we have engaged in negotiations with the company, yet they have refused to cooperate. Despite multiple opportunities to resolve this matter discreetly, they have chosen to ignore the consequences.

As a result, Welcompanies.com will now face **severe financial and reputational damage**. The exposure of confidential files will lead to regulatory investigations, lawsuits, operational downtime, and irreversible loss of trust from clients and partners. The cost of legal action, compliance penalties, and reputational recovery will far exceed the opportunity they had to settle this directly.

The insurance company [redacted], responsible for cyber risk coverage, has failed to fulfill its obligations to protect its client. Despite having an active cyber insurance policy, the company took no timely action to prevent data leakage or mitigate damages. Their inaction allowed the situation to escalate, leaving sensitive data at risk and their client in a vulnerable position.

You can download all files from this publication by clicking HERE.

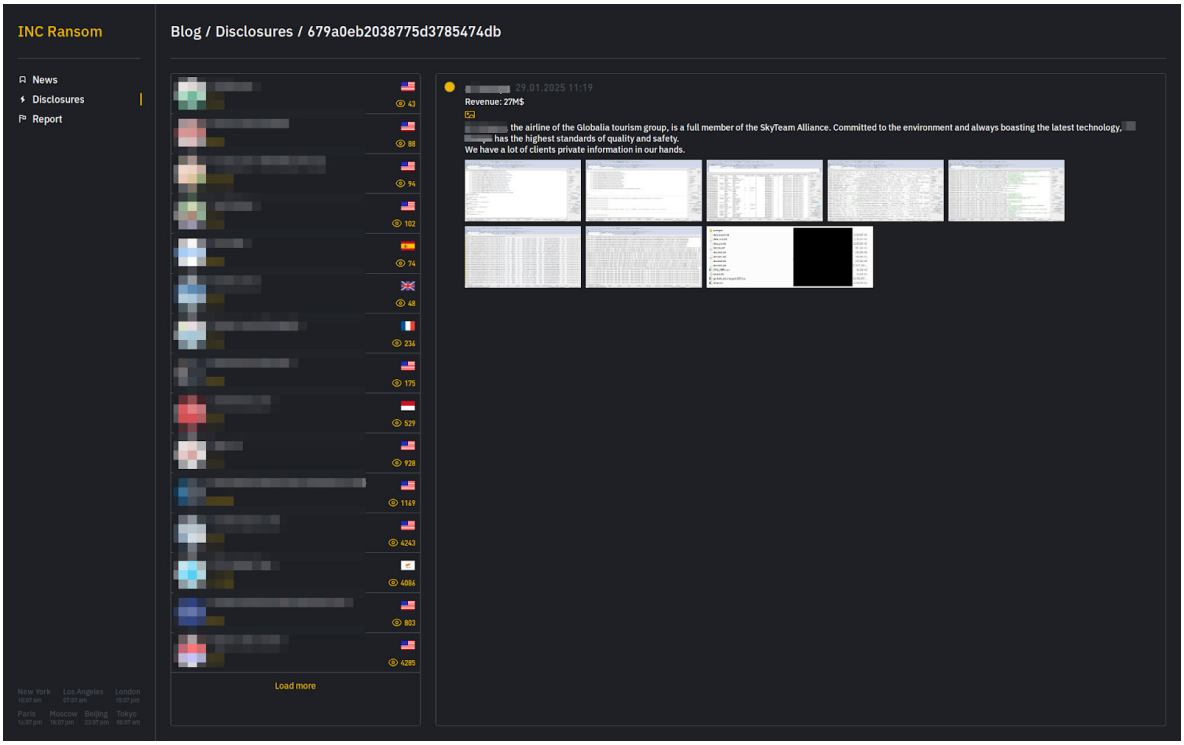
1. Information about extracted files
1.1. Full Listing (click to download).
1.2. Full Listing (archived):
[redacted]Listing.zip 3.93 MB

2. Chat History (update on 3 PM March 1)

3. Information about CEO, Co-Owner and Founder
3.1. CEO ([redacted]) Passport:

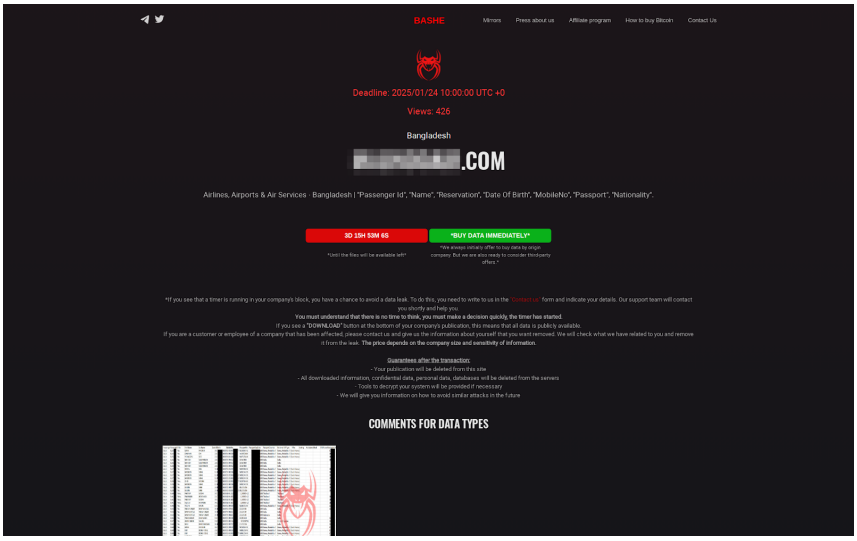
In the ransomhub ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as a refrigerated freight and logistics company based in De Pere, Wisconsin. They specialize in providing temperature-controlled truckload and logistics services across North America.

INCRansom Targets European Airline Companies



In the incransom ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as an airline from Europe.

APT73 Targets APAC Airline Companies



In the APT73 ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as an airline from the APAC region.

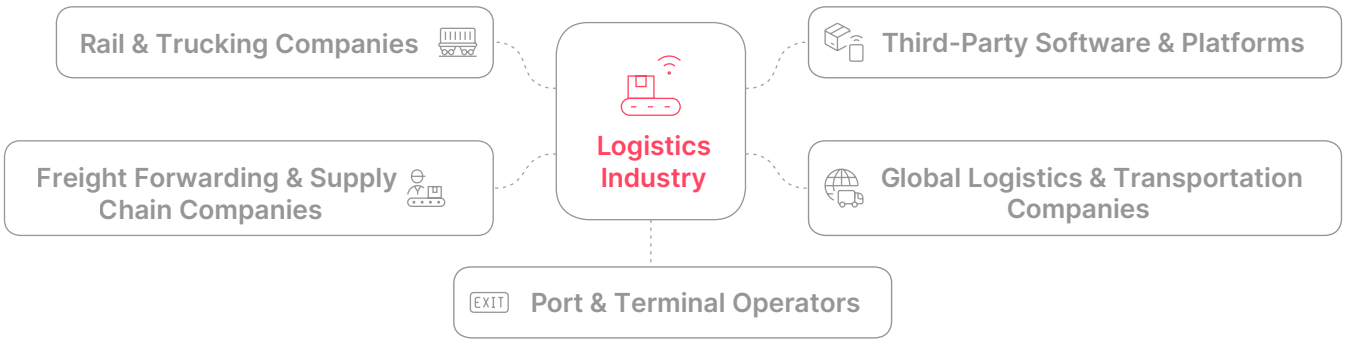
Stealer Log Statistics

Stealer Log Statistics: Top Domains in the Logistics Industry

Rail & Trucking Companies	Third-Party Software & Platforms
up.com	wisetechglobal.com
csx.com	descartes.com
cn.ca	cargowise.com
jbhunt.com	fourkites.com
knight-swift.com	project44.com

Global Logistics & Transportation Companies	Freight Forwarding & Supply Chain Companies	Port & Terminal Operators
dhl.com	flexport.com	dpworld.com
fedex.com	expeditors.com	globalpsa.com
ups.com	cevalogistics.com	portofrotterdam.com
maersk.com	dsv.com	
kuehne-nagel.com	xpo.com	
cma-cgm.com		
hapag-lloyd.com		

Top Domains in the Logistics Industry



Stealer Logs - Distribution of the Compromised Data

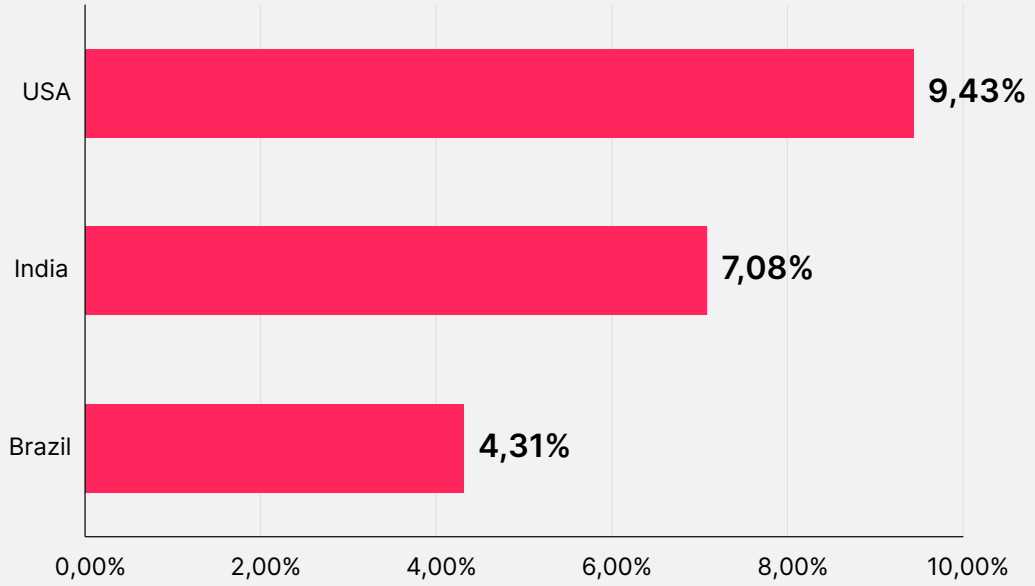
The high volume of exposed credentials (2.28M) suggests that many logistics employees or contractors have compromised devices, likely due to phishing, weak security hygiene, or lack of endpoint protection.

The exposure of 117.2K victim IPs highlights a significant risk of targeted attacks, as threat actors can geolocate users, exploit vulnerabilities, or conduct follow-up intrusions into corporate networks.

39.8K exposed credit cards reveal financial fraud risks, possibly linked to logistics e-commerce platforms, corporate payment systems, or fuel card usage.

This data underscores the urgent need for multi-factor authentication (MFA), endpoint security, and employee cybersecurity awareness training to mitigate stealer malware threats in the logistics industry.

Stealer Logs - Distribution of the Compromised Data by Victim Country

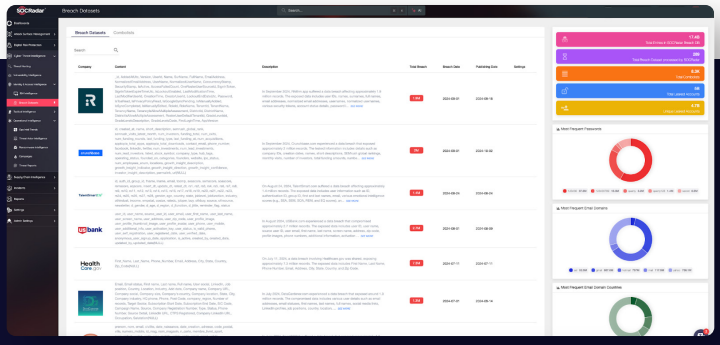


The United States (9.43%) has the highest number of stealer malware infections, likely due to its large logistics workforce and high digital integration in supply chain operations. Employees using infected personal or corporate devices pose a serious risk to enterprise security.

India (7.08%) follows, reflecting its growing logistics sector and large workforce, where cyber hygiene gaps and reliance on personal devices for work could contribute to infections.

Brazil (4.31%) indicates a regional cybercrime concern in Latin America's logistics infrastructure, possibly tied to increasing digital transformation and inadequate endpoint protections.

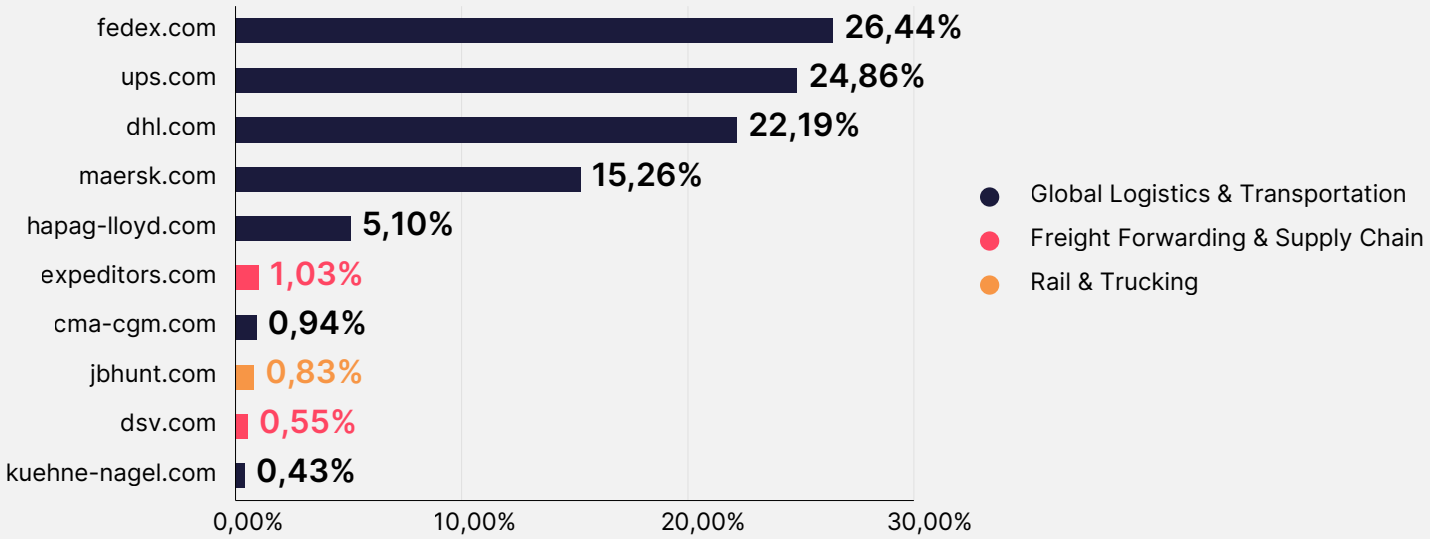
This distribution suggests that logistics employees across key global markets are frequently compromised, reinforcing the need for strong endpoint protection, network access controls, and phishing-resistant authentication to prevent further data leaks.



SOCRadar's Identity & Access Intelligence Module

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.

Stealer Logs - Distribution of the Compromised Data by Domains and Sub-Sectors



The top three most searched domains are fedex.com (26.44%), ups.com (24.86%), and dhl.com (22.19%), probably due their global presence and central role in logistics. These companies and their employees likely represent the highest-value targets for stealer malware due to their extensive customer and employee databases.

maersk.com (15.26%) follows, with a notable portion of global container shipping under its belt, making it a valuable target for attackers looking to exploit sensitive shipping or freight data.

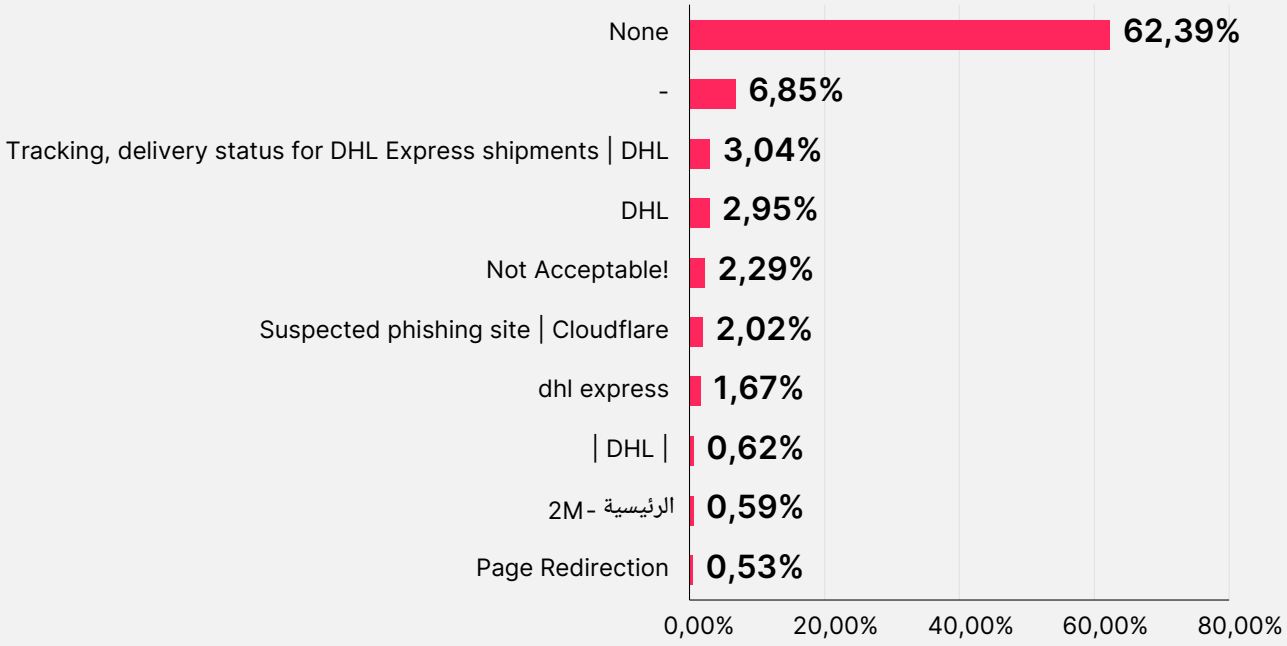
hapag-lloyd.com (5.10%) and expeditors.com (1.03%) also attract significant attention, indicating a focus on major international shipping and logistics companies.

The lower percentage for companies like cma-cgm.com (0.94%) and jbhunt.com (0.83%) suggests less exposure.

This data highlights the importance of securing high-profile logistics platforms, particularly in the top global shipping and courier services, to prevent data theft and enhance cybersecurity measures.

Phishing Threats

Phishing Attacks - Distribution by Phishing Page Title

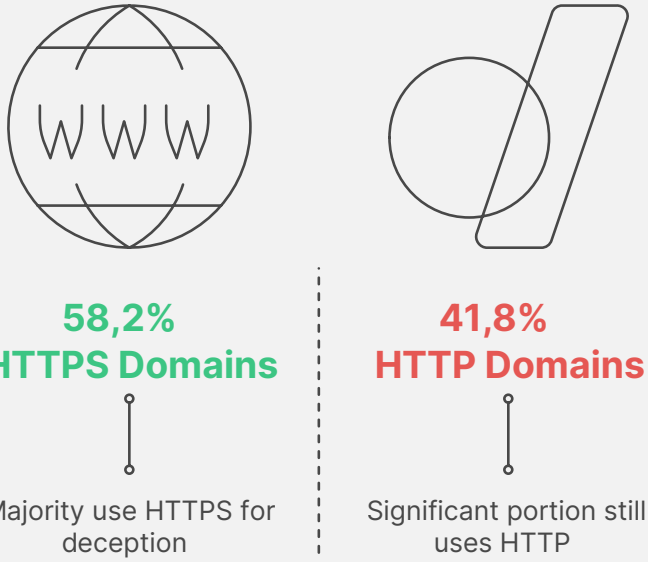


The overwhelming majority of phishing attempts show a "None" (62.39%) or "-" (6.85%) designation for page titles, likely indicating generic phishing pages or attempts to hide the identity of the phishing target. This suggests a high volume of unsophisticated or low-targeted phishing campaigns.

The presence of legitimate tracking and delivery status pages for DHL (3.04%) and general DHL references (2.95%) indicates that attackers are leveraging brand impersonation, with DHL being a key target for phishing campaigns, likely to exploit user trust and gain access to sensitive information such as shipping or customer data.

This data underscores the importance of phishing awareness, verification processes, and protective web filtering systems to safeguard logistics employees and customers from social engineering and credential theft.

Phishing Attacks - Distribution by SSL/TLS Protocol



The data shows that HTTPS (58.22%) is slightly more prevalent than HTTP (41.78%) in phishing attempts, which aligns with the fact that many phishing sites are now using HTTPS to appear legitimate and bypass browser security warnings. This tactic increases the credibility of the phishing pages, making them harder to detect for users.

However, the HTTP prevalence still represents a significant portion, as non-encrypted HTTP pages can easily be identified by security filters and browsers, which may flag them as insecure.

Overall, this highlights that while HTTPS phishing sites are more sophisticated, traditional HTTP-based phishing pages still remain a concern, particularly for organizations lacking web filtering solutions. The trend emphasizes the need for advanced phishing detection systems and education on verifying URLs and secure connections.

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.s to safeguard sensitive information from cybercriminal exploitation.

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.