SOCRadar®
Your Eyes Beyond

FROM BLACK FRIDAY TO CYBER MONDAY

2024 E-COMMERCE THREAT LANDSCAPE REPORT

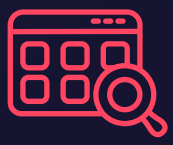
SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary

Top Takeaways

The E-Commerce industry was on the **5th spot**, among other industries, with **6,77%** of ransomware attacks targeting e-commerce companies worldwide.



The **USA** was the most targeted country in the E-Commerce Industry, with **17,16%** of all the Dark Web posts. **7,20%** of all the posts from those forums targeted the **UK**, putting it in second place. **India** was in third place, with **5,11%** of the posts targeting Indian organizations.

When we look at the type of information published on Dark Web forums, we see that **Access (sales/shares, etc.)** takes the first spot with **46,82%** of all the posts. The second most popular type of information threat actors share is **data-related content (sales/shares, etc.)** with **41,22%** of the posts. Lastly, we have posts associated with **Website attacks (defacements, DDoS attacks, etc.)**, which take **10,53%** of the posts.

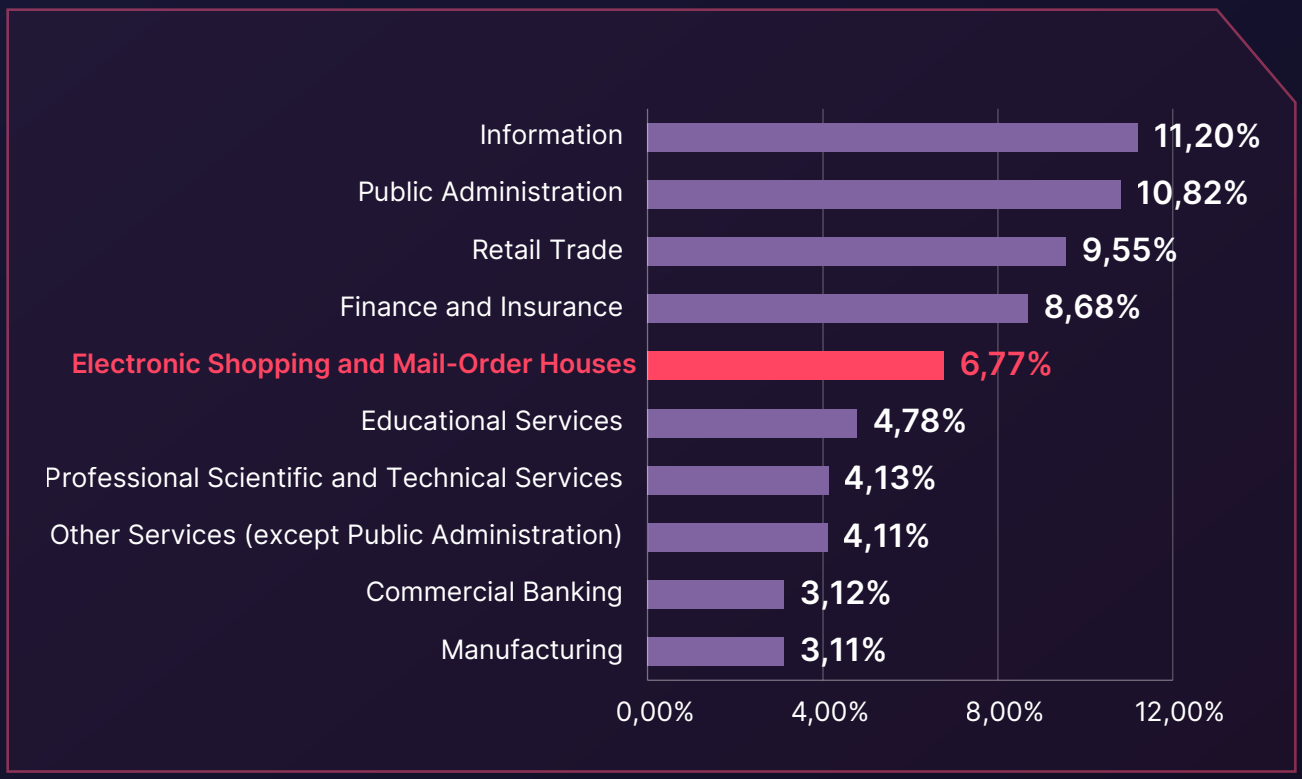
SOCRadar's stealer log data from the world's most frequented e-commerce platforms reveals sensitive information, including **686,644** email and password combinations, **131,756** unique victim IP addresses, **117,068** password hashes, and **29,925** credit card details.

According to SOCRadar, the majority of stealer malware victims are from **India, with 14,16% of the credentials belonging to victims from there. The USA comes second, with 8,33%** of the credentials exposed in stealer logs. In the third spot, **Brazil comes with 4,60%.**

Technical Details

Dark Web Threats Targeting the E-Commerce Industry

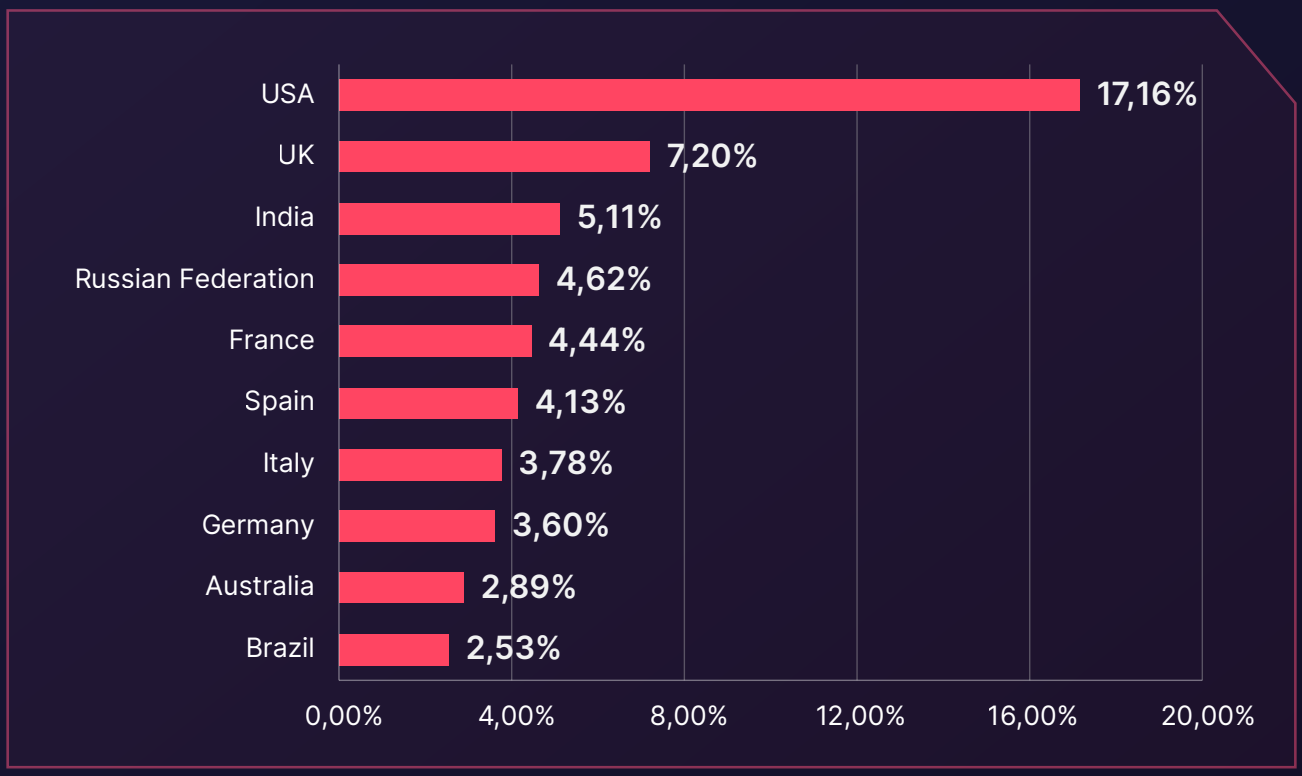
Distribution of Dark Web Threats by Industry



When we look at the industry distribution of Dark Web posts published last year, the **Information industry emerged as the most widely discussed sector, with 11,20% of the posts. The Public Administration** industry took second place, with **10,82%** of the attacks, and **Retail Trade** was the third industry, with **9,55%.**

The **E-Commerce industry** was on the **5th spot**, with **6,77%** of ransomware attacks targeting e-commerce companies worldwide.

Distribution of Dark Web Threats by Primary Target Country



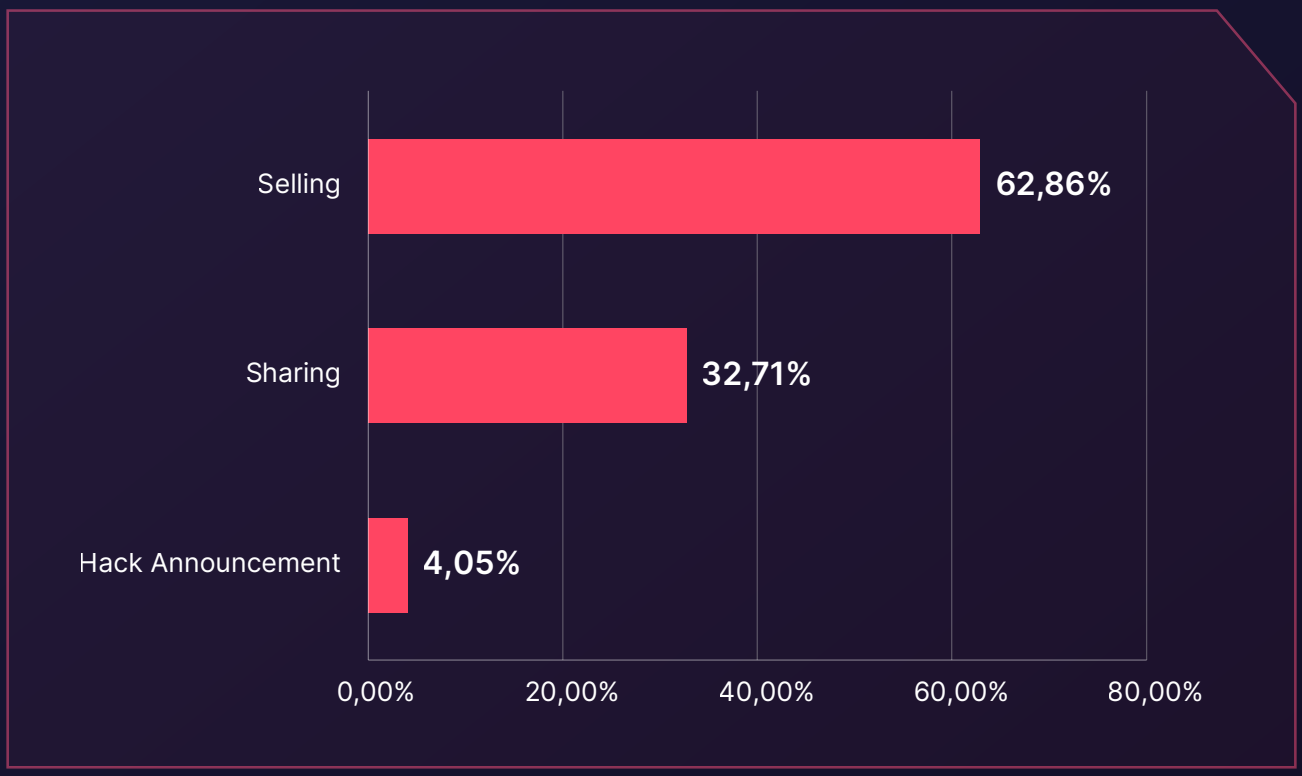
> The **USA** was the most targeted country in the E-Commerce Industry, with **17,16%** of all the Dark Web posts. **7,20%** of all the posts from those forums targeted the **UK**, putting it in second place. **India** was in third place, with **5,11%** of the posts targeting Indian organizations.

SOCRadar's Advanced Dark Web Monitoring provides e-commerce companies with critical insights into hidden threats targeting Retail Trade, 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.

Protect Your Business from the Shadows—Uncover Dark Web Threats with Premium Intelligence at an Affordable Price

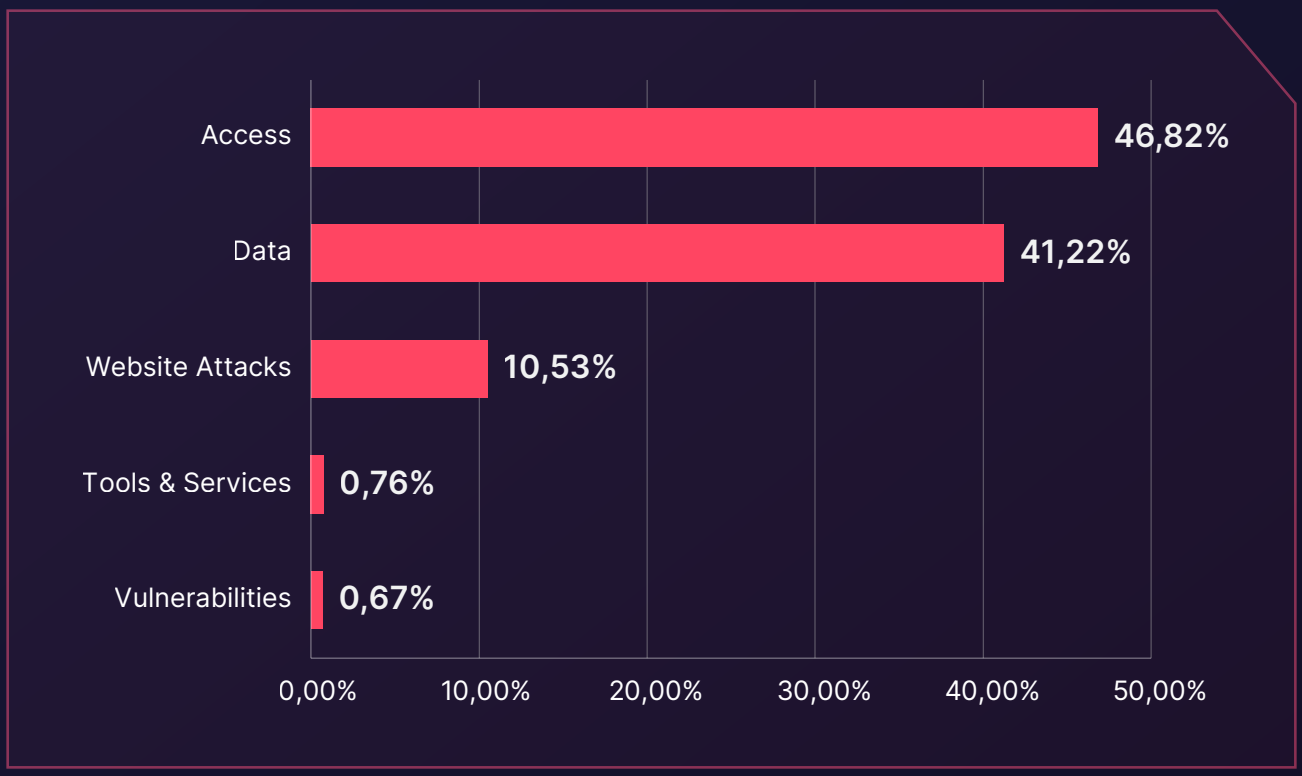
Stay tuned this Black Friday week for exclusive access to high-quality dark web intelligence tailored for e-commerce and SMBs. Secure your edge in cyber defense—without breaking the bank.

Distribution of Dark Web Threats by Threat Categories



Threat actors targeting the E-Commerce industry mainly sell their content. The **Selling** category is in first place with **62,86%** of all the posts from Dark Web forums, followed by **Sharing**, which comprises **32,71%** of the posts from Dark Web forums. **Hack Announcements are in third place**, with **4,05%** of the posts.

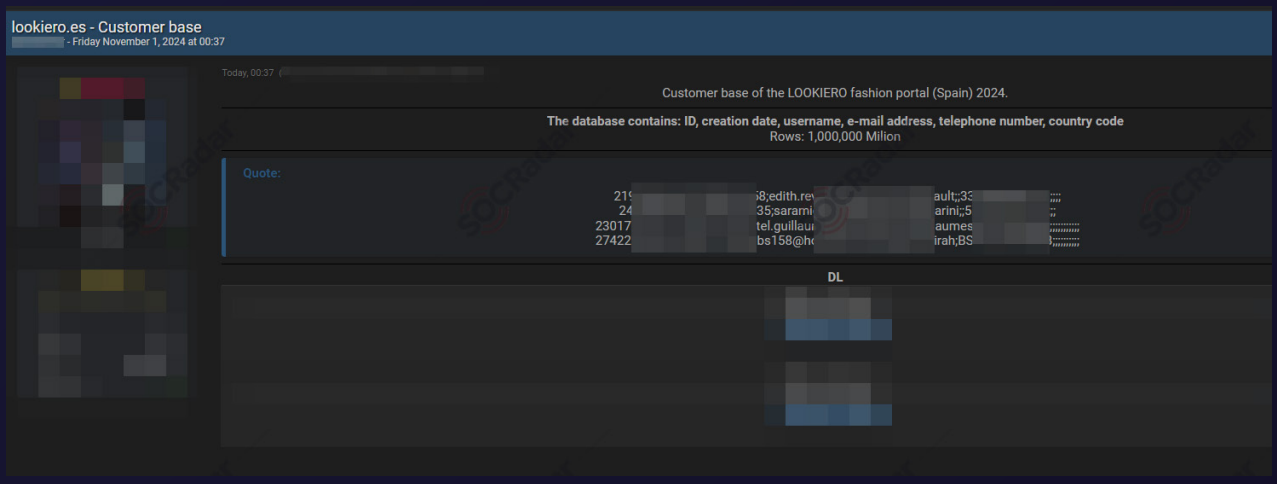
Distribution of Dark Web Threats by Threat Type



When we look at the type of information published on Dark Web forums, we see that **Access (sales/shares, etc.)** takes the first spot with **46,82%** of all the posts. The second most popular type of information threat actors share is **data-related content (sales/shares, etc.)** with **41,22%** of the posts. Lastly, we have posts associated with **Website attacks (defacements, DDoS attacks, etc.)**, which take **10,53%** of the posts.

Recent Dark Web Activities Targeting the E-Commerce Industry

The Alleged Customer Database of Lookiero Spain is Leaked

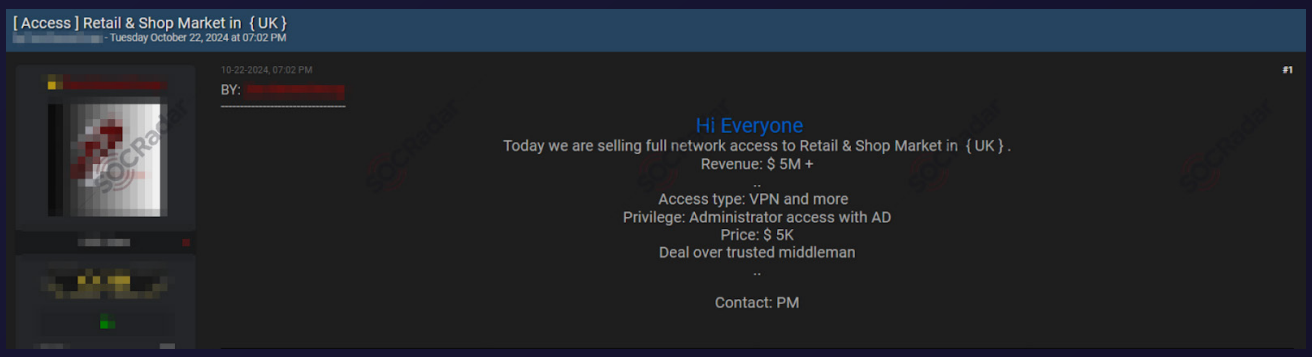


A post on a Dark Web Forum monitored by SOCRadar

In a recent incident observed by SOCRadar, a claim of a data breach affecting Lookiero Spain, a prominent fashion and styling portal, has surfaced on a Dark Web forum. The post alleges that the breach compromised the personal data of Lookiero's customers in Spain, exposing sensitive information.

According to the forum post, the leaked database purportedly includes critical customer details such as user IDs, account creation dates, usernames, email addresses, phone numbers, and country codes. The database reportedly contains around 1 million entries, representing a substantial portion of Lookiero's Spanish customer base.

The Alleged Unauthorized Network Access Sale is Detected for a British Retail Company



A post on a Dark Web Forum monitored by SOCRadar

In a recent discovery on a monitored hacker forum, SOCRadar analysts identified a listing advertising unauthorized network access allegedly belonging to a retail company operating in the United Kingdom. According to the forum post, the seller claims full administrator-level access, including Active Directory privileges, with VPN and additional access methods available.

The retail entity is reported to have annual revenue exceeding $5 million. The seller offers access at a starting price of $5,000, promising secure transactions through a trusted middleman.

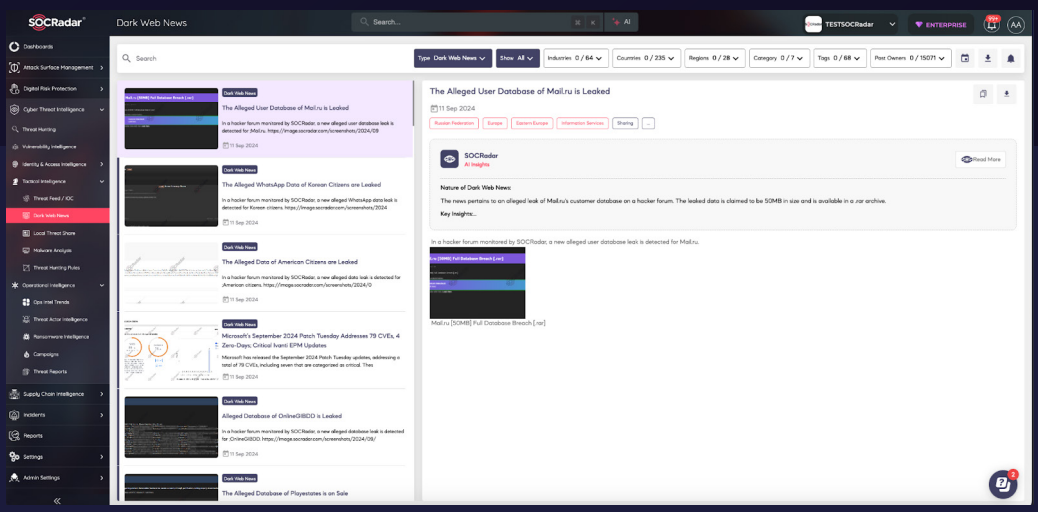
This listing underscores a concerning trend of illicit access sales in the cybercrime landscape. These sales pose significant threats to businesses with high-value network infrastructures.

The Alleged Customer Database of Temu is on Sale

A post on a Dark Web Forum monitored by SOCRadar

In a recent development on a hacker forum monitored by SOCRadar, a threat actor has allegedly put up a database for sale belonging to the e-commerce platform Temu. The post indicates that over 87 million records are allegedly exposed.

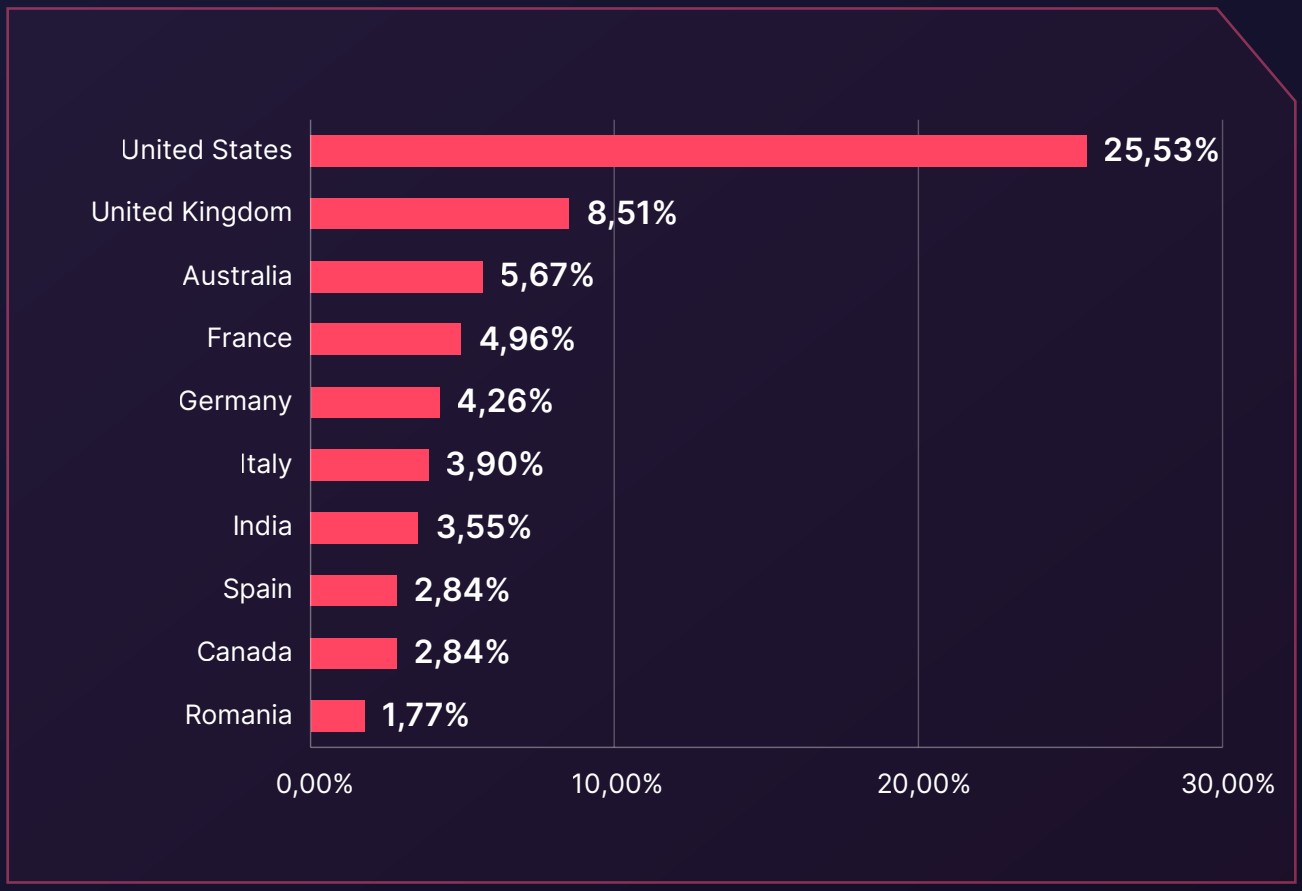
The seller describes the data as previously unsold, emphasizing that only a single copy will be available for purchase, and provides an offer for samples to verify authenticity.



You can learn about the latest Dark Web developments with SOCRadar's Dark Web News Module. SOCRadar's Dark Web News page revolutionizes how you stay informed. It's not just an information aggregator; it's a sophisticated filter, meticulously separating the signal from the noise.

Ransomware Threats Targeting the E-Commerce Industry

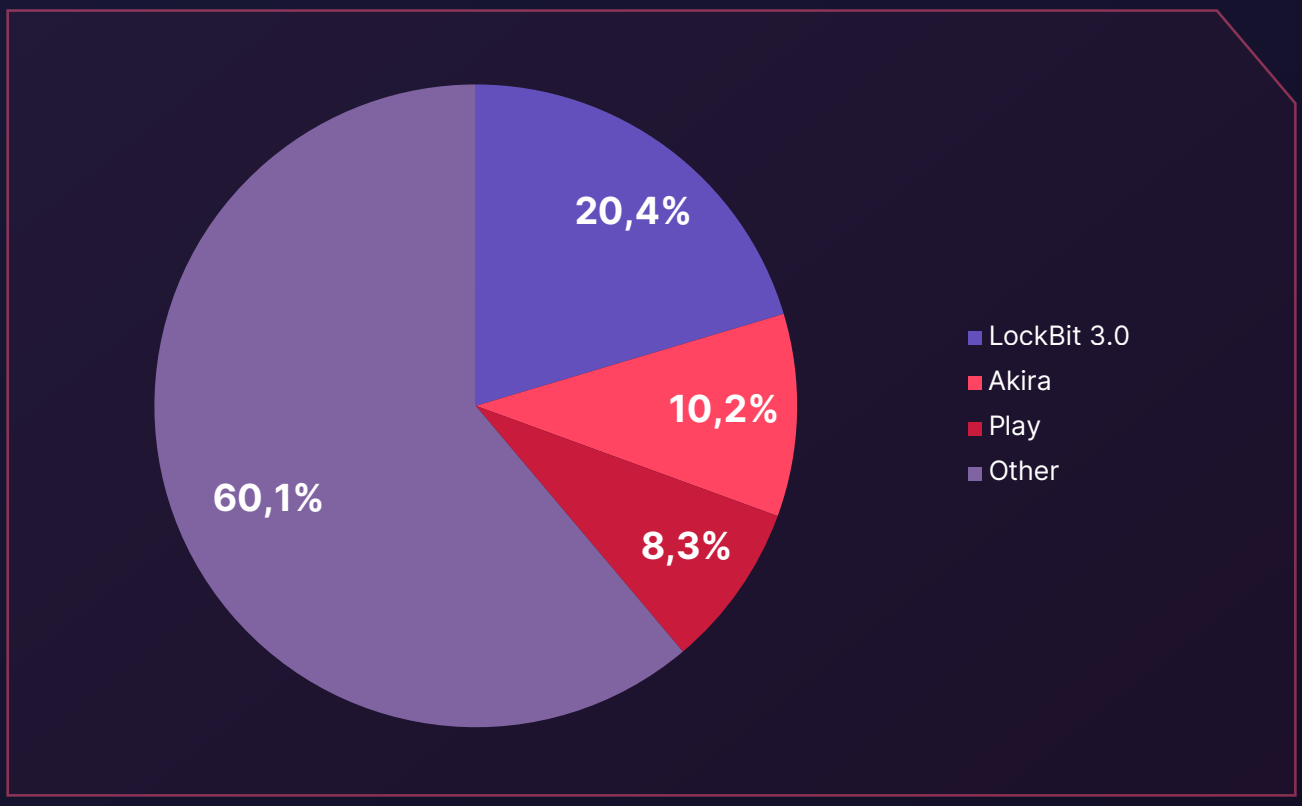
Distribution of Ransomware Attacks by Primary Target Country



Ransomware groups most targeted the **United States** in the e-commerce industry, with **25,53%** of the attacks targeting the organizations there. The **United Kingdom** was in second place, suffering from **8,51%** ransomware attacks. In third place, **Australia** was targeted with **5,67%** ransomware attacks.

Top Ransomware Groups Targeting the E-Commerce Industry

Top Ransomware Groups Targeting the E-Commerce Industry



Our analysis shows that **LockBit 3.0** was the most active ransomware group targeting the E-Commerce Industry last year, responsible for **20.4%** of all the attacks. **Akira** was the second most active group, with **10.2%** of all the attacks. In third place, we have **Play Ransomware**, with **8.3%** of all the ransomware attacks targeting the E-Commerce Industry.

A Closer Look into The Top 3 Ransomware Groups

LockBit 3.0

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Canada, Europe, Thailand, Taiwan
Target Sectors:	Manufacturing, Professional Services, IT, Healthcare, Finance, Education, Legal Services
Attack Type:	Phishing, RDP and VPN access Exploitation, Ransomware, Data Exfiltration, Double-extortion

-TTPs-

Exploit Public-Facing Application:	T1190
Remote Desktop Protocol:	T1021.001
Data Encrypted for Impact:	T1486

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.

You can visit our **blog post** for more detailed Lockbit 3.0 Ransomware Group information.

Akira

-Ransomware Group-

Motivation: Financial Gain

Target Countries: US, Canada, Australia, United Kingdom, France, Germany, Italy, Spain

Target Sectors: Education, Finance, Manufacturing, Healthcare

Attack Type: Data Exfiltration, Ransomware, Data Leakage

-TTPs-

Valid Accounts: T1078

Exploit Public-Facing Application: T1190

External Remote Services: T1133

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.

Play

-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

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.

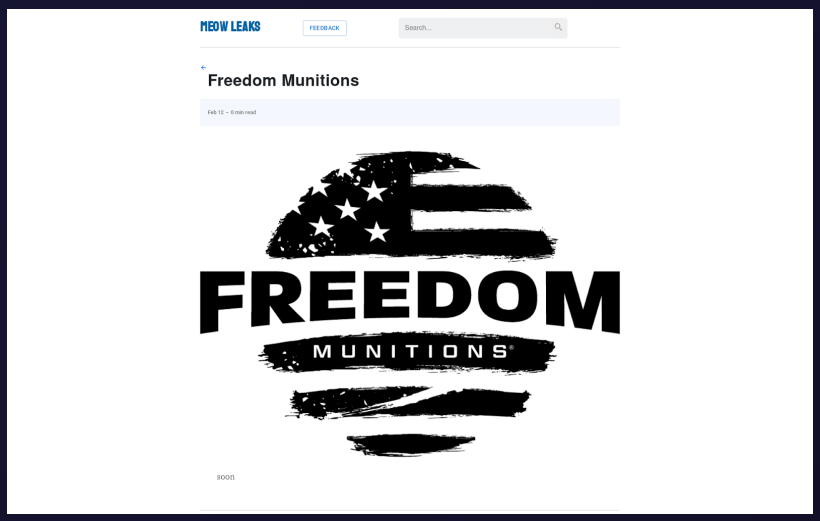
You can visit our **blog post** to read the rest of the threat actor profile.

Recent Ransomware Attacks Targeted the E-Commerce Industry

Freedom Munitions Allegedly Targeted by Meow

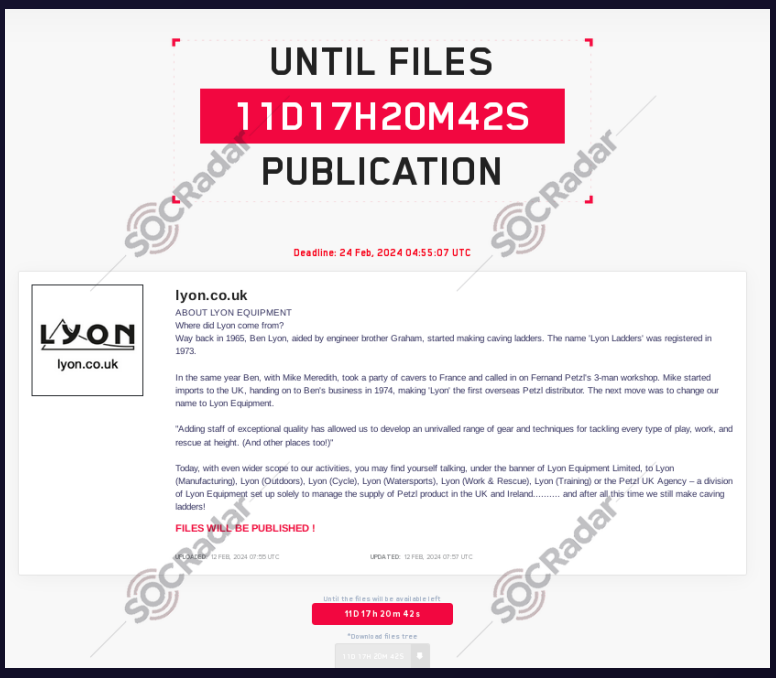
In the Meow ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Freedom Munitions.

Freedom Munitions is known for producing ammunition with premium components sourced from trusted manufacturers.



The threat actor website monitored by SOCRadar

Another Ransomware Victim of LockBit 3.0: Lyon Equipment



In the LockBit 3.0 ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Lyon Equipment.

Lyon Equipment, founded in 1965 by Ben Lyon and his brother Graham, is renowned for its specialized gear for caving, climbing, and outdoor activities. Over the years, the company expanded significantly, adding various divisions.

Lush Targeted by Akira Ransomware

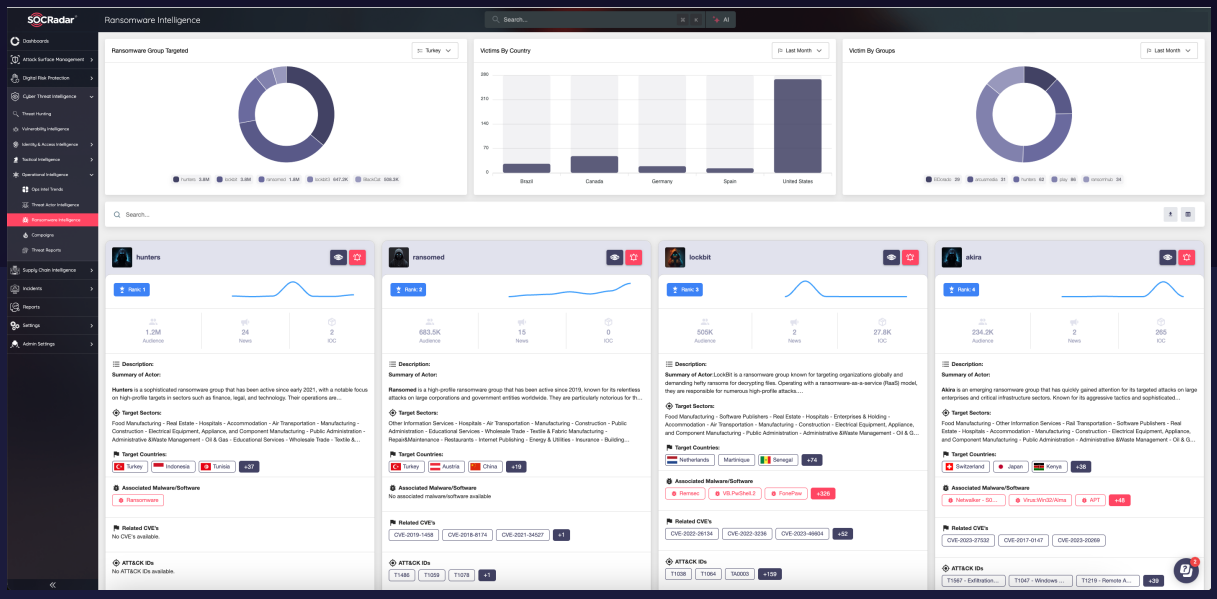
A new ransomware victim was allegedly announced as Lush in the Akira ransomware group website monitored by SOCRadar.

Lush was founded in 1995 and is headquartered in Poole, United Kingdom. It is a cosmetic store specializing in bath bombs, hair products, and makeup.

According to the alleged post on the website, the threat actor group had 110 GB of their files, including personal documents, passports, information related to accounting, finance, tax, projects, client information, and much more.

date	title	content
2024-01-25	Lush	Founded in 1995 and headquartered in Poole, United Kingdom, Lush is a cosmetic store specializing in the retail of bath bombs, hair products, makeup and more. 110 Gb of their files are prepared for uploading. There are a lot of personal documents especially passports. Accounting, finance, tax, projects, clients information and much more could be found in the archives we are going to share.

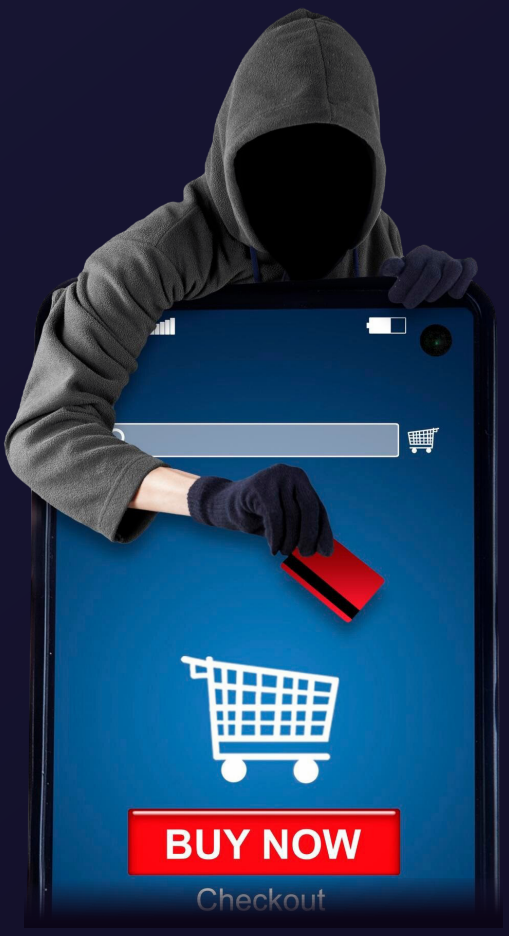
The threat actor website monitored by SOCRadar



Explore our newly renovated 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.

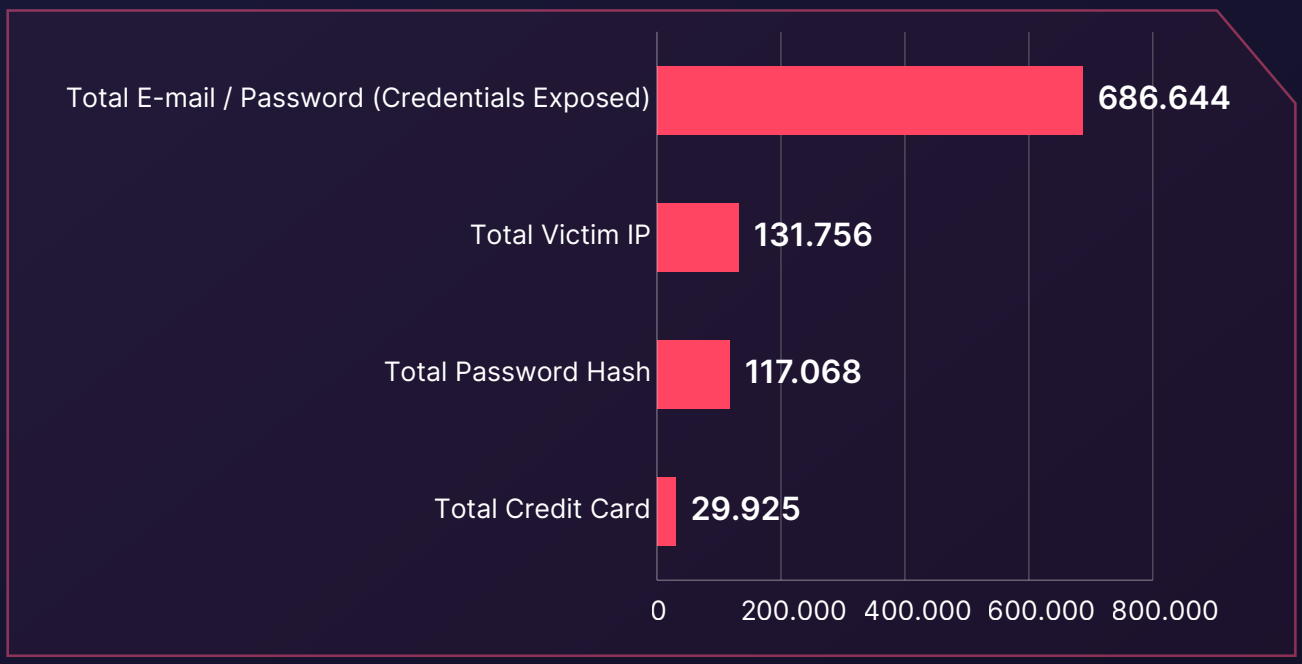
Stealer Log Statistics

E-commerce companies hold the data of thousands of individuals, processing their email addresses, passwords, credit card data, and more. Since most of this data belongs to people from every part of life, stealer logs can be problematic for their lives and the organizations they work for when threat actors exploit the information. In this chapter, you will see the most popular domains in the E-Commerce industry and the country-based analysis of our data.



amazon.com
temu.com
ebay.com
aliexpress.com
walmart.com
rakuten.co.jp
wildberries.ru
ozon.ru
flipkart.com
etsy.com

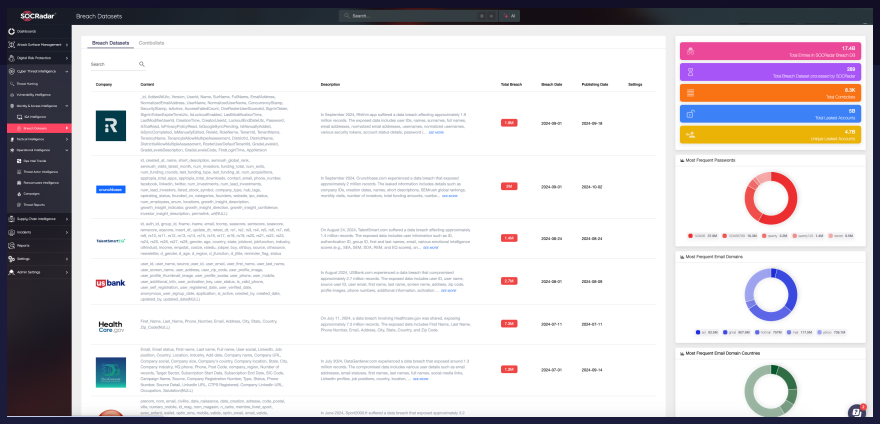
Stealer Logs- Compromise Data



SOCRadar's stealer log data from the world's most visited e-commerce platforms reveals sensitive information, including 686,644 email and password combinations, 131,756 unique victim IP addresses, 117,068 password hashes, and 29,925 credit card details.

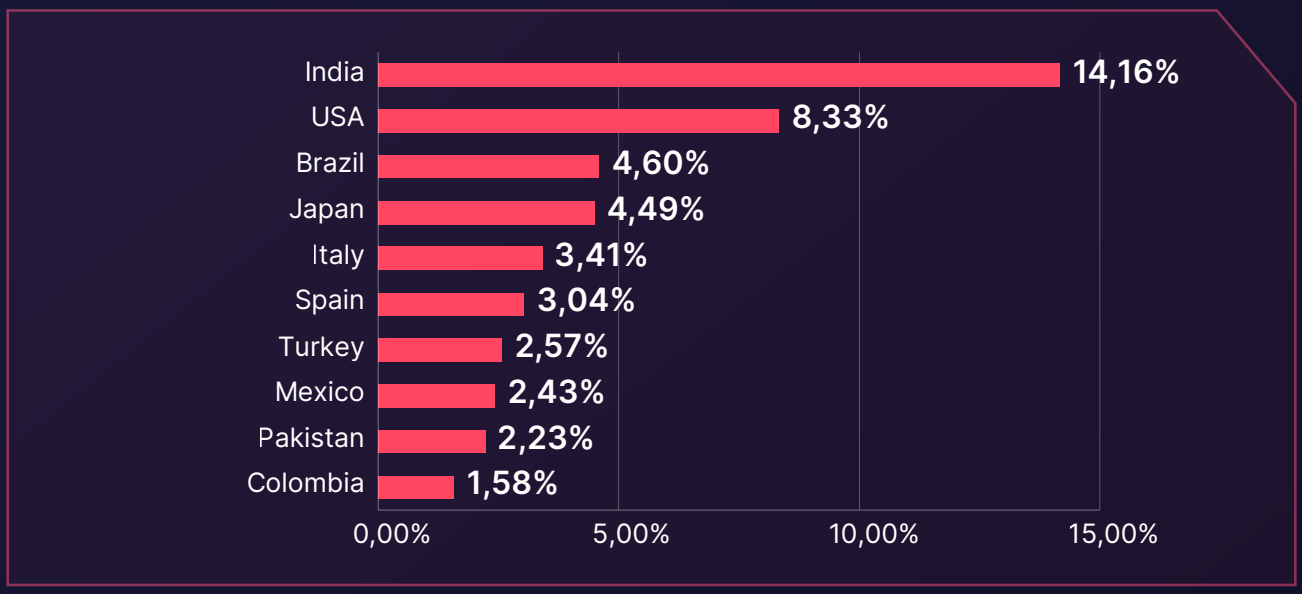
Organizations should implement strict password policies and ensure appropriate Identity & Access intelligence solutions are used.

While the amount of credit card data is smaller, its presence indicates a serious financial risk, showing that stealer malware effectively intercepts sensitive information across various devices.



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.

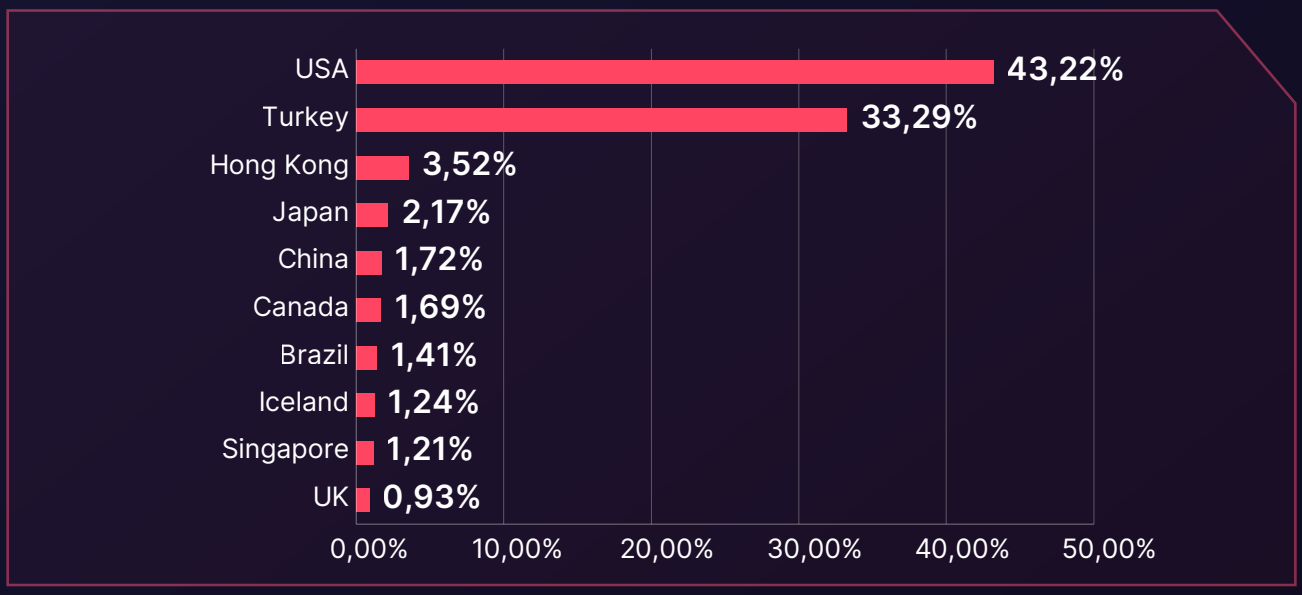
Stealer Logs - Distribution of the Victims' Countries



According to SOCRadar, most stealer malware victims are from **India, with 14,16% of the credentials belonging to victims from there. The USA comes second**, with **8,33%** of the credentials exposed in stealer logs. In the third spot, **Brazil comes with 4,60%.**

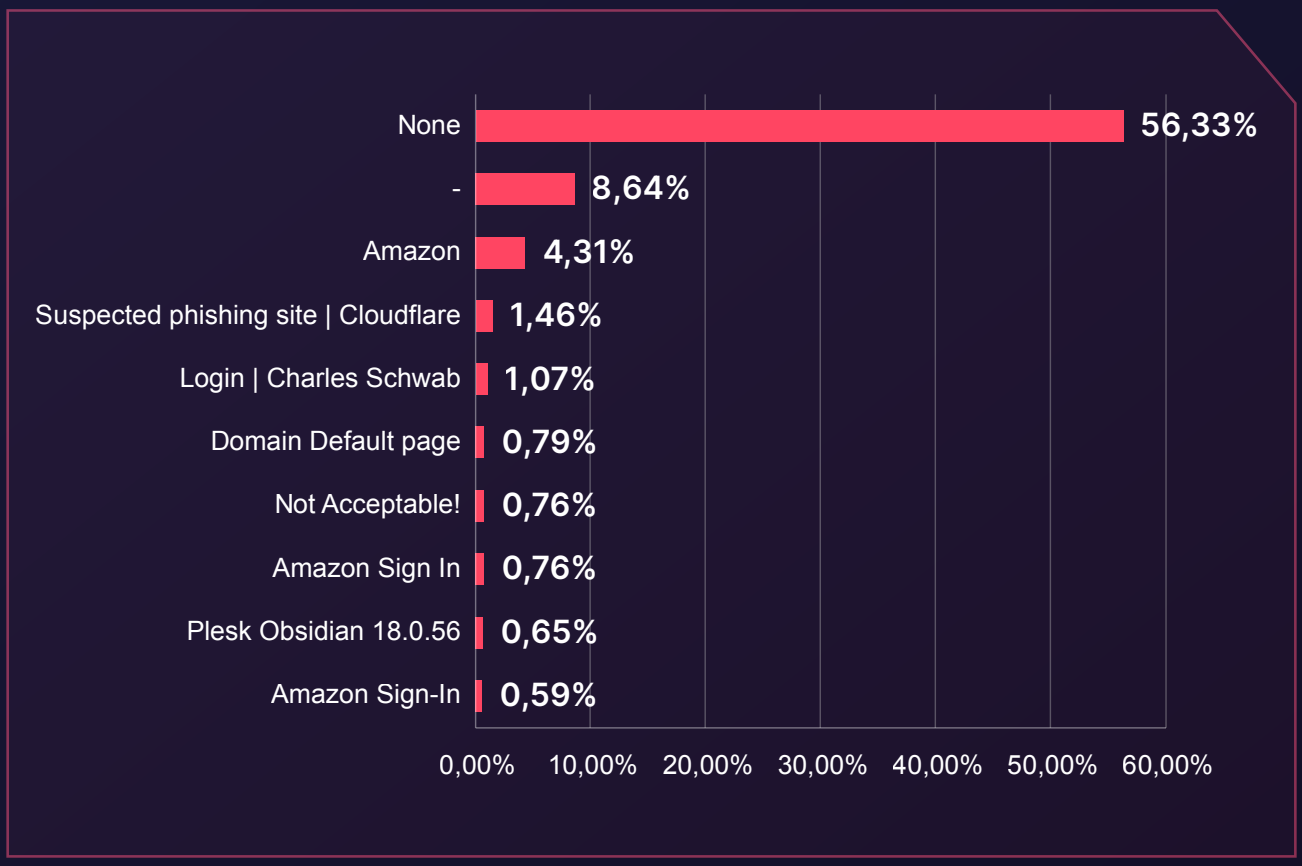
Phishing Threats Targeting the E-Commerce Industry

Phishing Attacks - Distribution by Country



Phishing attack statistics reveal that victims from the **USA** were predominantly targeted with phishing activities, accounting for **43.22%** of all attacks. **Turkey** ranked second, facing **33.29%** of the phishing attacks, followed by **Hong Kong** in third place, targeted by **3.52%** of the attacks.

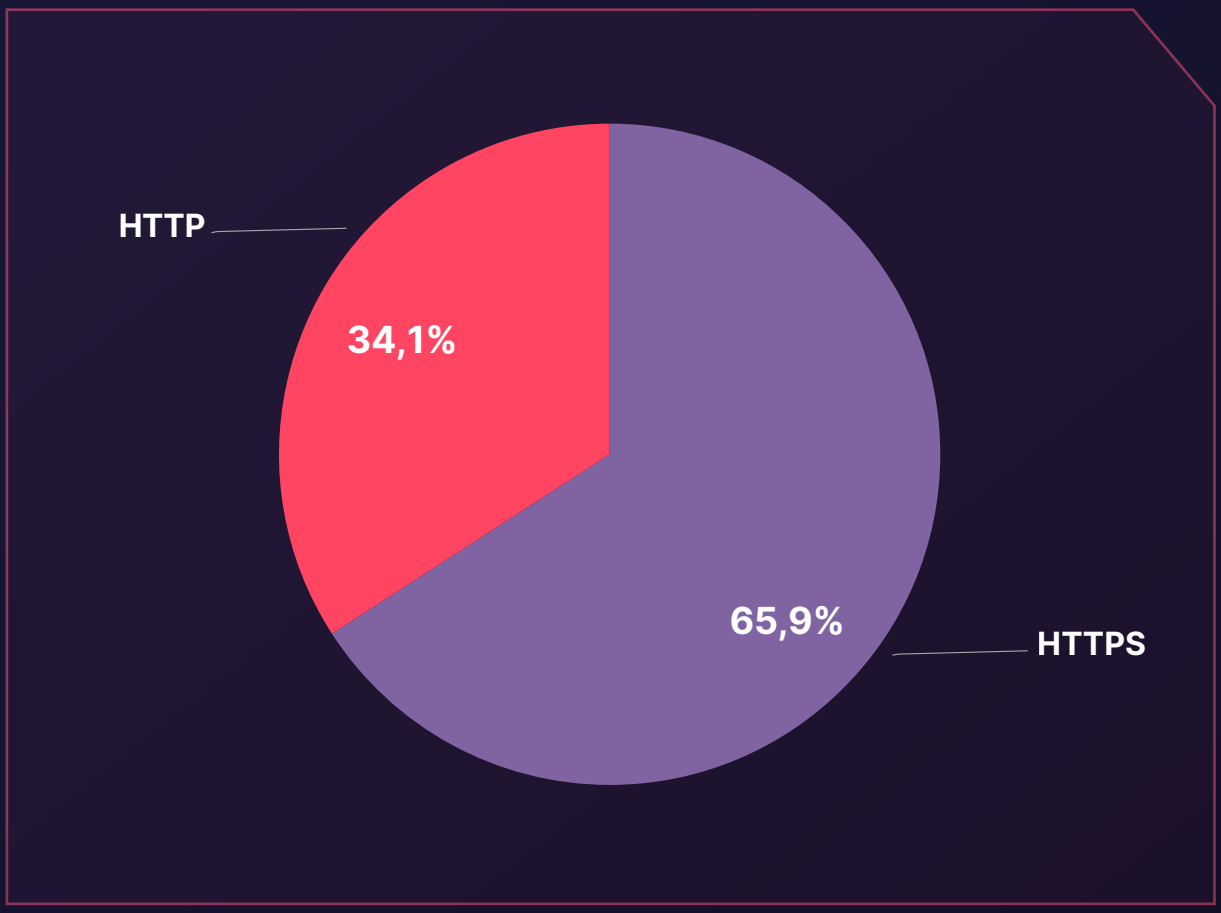
Phishing Attacks - Distribution by Phishing Page Title



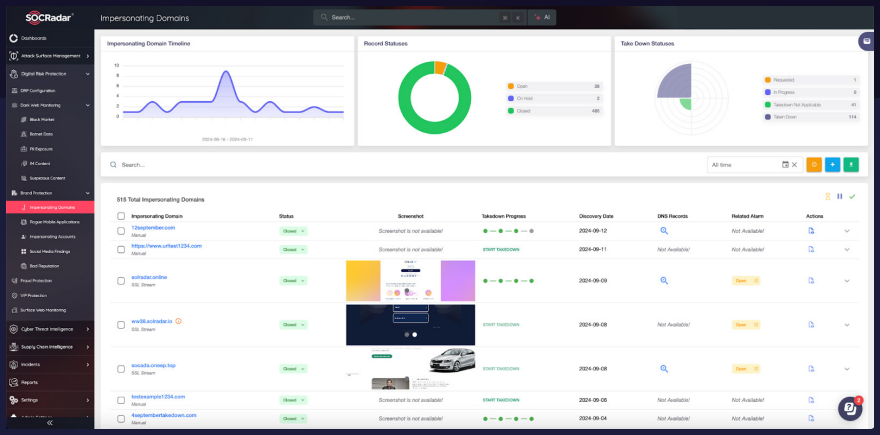
Our analysis shows the most used pages in phishing attacks. The data reveals a predominant usage of empty page titles such as “None” or “-.” This is generally related to the threat actor’s operational strategy. Threat actors prioritize speed over presentation, aiming to complete tasks quickly with minimal detection risk, and creating sophisticated pages takes time.

Additionally, in some cases, they know their target will access the page via a direct link or a closed platform (e.g., phishing emails), so page titles are irrelevant to the end goal.

Phishing Attacks- Distribution by SSL/TLS Protocol



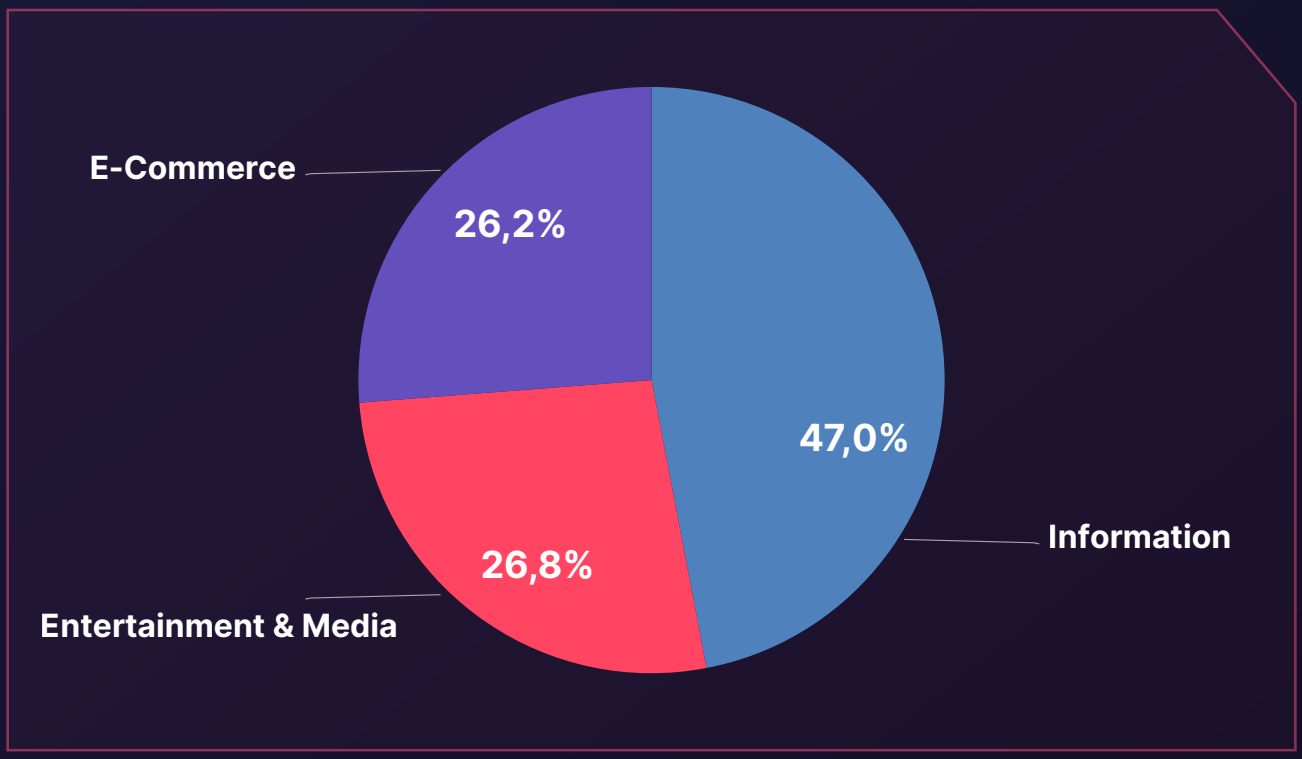
When we analyze the protocols used by phishing websites, we see a predominant use of HTTPS protocols. This is generally done to improve the websites' genuineness.



SOCRadar Labs provides free services such as **Phishing Radar**, which helps identify phishing attacks swiftly.
Our **AI-powered Brand Protection** scans millions of domain registrations to detect malicious domains and alerts on suspicious activity.

DDoS Attack Statistics

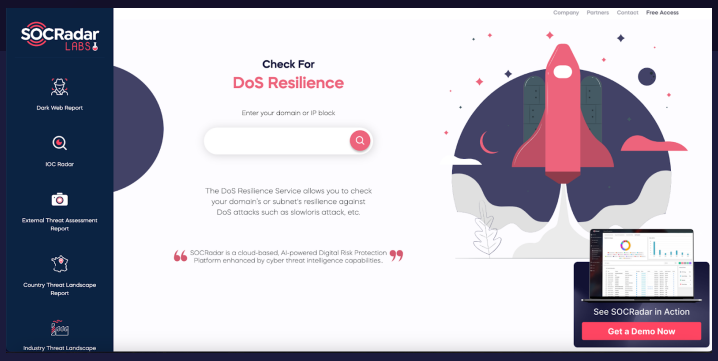
Top 3 Most Targeted Industries by DDoS Attack in 2024



In 2024, the most targeted industries with DDoS attacks are led by the information sector, which accounts for nearly half of all attacks at 47%.

Close behind, the entertainment and media sector represents 26.8% of attacks, likely due to its heavy reliance on continuous online access and high-profile events that attract considerable attention.

E-commerce follows at 26.2%, driven by its dependence on digital transactions and the significant financial implications of service disruptions.



Enhance your DDoS defense with SOCRadar's DoS Resilience Free Tool. Our Free DoS Resilience Service allows you to check your domain's or subnet's resilience against DoS attacks, such as slow loris attacks.

Lessons Learned: Key Insights and Strategic Recommendations

Upon reflection of the cyber threat landscape impacting organizations in E-Commerce, 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 E-Commerce 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 for E-Commerce Sites

The diverse range of cyber threats underscores the necessity for multi-layered security for E-Commerce Sites. As demonstrated, threat actors do not discriminate based on industry, necessitating a comprehensive security approach across all industries, 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 training is 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. Adopting a proactive, informed, and comprehensive approach to cybersecurity is paramount. By partnering with solutions such as SOCRadar, organizations in E-Commerce can fortify their defenses and effectively navigate the evolving cyber threat landscape.

SOCRadar®
Your Eyes Beyond

Defend Your Business with High-Quality Dark Web Intelligence Now More Affordable Than Ever

Get Ahead of the Game with SOCRadar
Delivering Powerful Threat Intelligence Without the High Price Tag

Exciting Savings Await This Black Friday Week!
Look for a limited-time offer designed to help you secure your business

Get Notified About Exclusive Discounts

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 PERSONALIZED DEMO

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.