SOCRadar®
Your Eyes Beyond

2024 End of the Year Report

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary

The year 2024 has been marked by an unprecedented surge in cyber threats, with attackers employing increasingly sophisticated tactics. The evolving threat landscape has presented formidable challenges, from ransomware campaigns targeting critical sectors like manufacturing to the widespread use of Stealer Logs compromising millions of sensitive records.

SOCRadar's Extended Threat Intelligence (XTI) platform has been instrumental in equipping security operations teams with actionable insights, enabling proactive threat mitigation. The rise in phishing incidents, particularly in regions such as the United States and Singapore, highlights cybercriminals' adaptability. The Dark Web remains a hub for illicit activity, driving the need for continuous monitoring.

Ransomware groups such as RansomHub and LockBit have dominated the landscape, emphasizing the need for robust defenses. Meanwhile, targeted industries like cryptocurrency and information services have faced heightened risks, showcasing the critical importance of multi-layered cybersecurity strategies.

As 2024 concludes, the reliance on AI-driven solutions and real-time intelligence has proven indispensable. With SOCRadar's XTI platform at the forefront, organizations are better positioned to navigate the evolving threat environment and protect their critical assets against cyber adversaries' sophisticated tactics.

Top Takeaways

Dark Web Activity: In 2024, 2,126 threat actors were active on the Dark Web, collectively making 18,537 posts. These activities primarily centered on selling compromised data and unauthorized access credentials, underlining the growing threat landscape in underground forums.

Targeted Industries: The United States faced the highest volume of Dark Web targeting, making up 19.24% of the total posts. Meanwhile, the Information industry emerged as the most targeted industry on the Dark Web, accounting for 12% of all activity.

Ransomware Trends: The United States was also the top target for ransomware attacks, experiencing 54.12% of all reported incidents globally. Meanwhile, Manufacturing was the most impacted industry, representing 18.26% of ransomware activity.

Prominent Ransomware Groups: Key ransomware groups dominated the 2024 landscape, with RansomHub (9.45%), LockBit 3.0 (6.91%), and LockBit (5.96%) being the most active. These groups exploited vulnerabilities across critical sectors, causing widespread damage.

Stealer Logs: The use of Stealth Logs compromised vast amounts of sensitive information, including 5,876,049 email/password combinations, 768,328 password hashes, 736,112 credit card details, and 148,962 victim IP addresses. This highlights the severity of credential-based attacks in 2024.

Phishing Trends by Region: The United States experienced the highest share of phishing attacks globally, accounting for 34.89%, followed by Singapore (15.89%) and the United Kingdom (3.06%). These statistics reveal the regional concentration of phishing campaigns.

Phishing by Industry: The Cryptocurrency and NFT sectors led the list of industries targeted by phishing attacks, with 19.11% of incidents. They were closely followed by Information Services (18.95%) and National Security and international Affairs (12.63%), underscoring the adaptive nature of phishing campaigns.

SOCRADAR WITH NUMBERS 2024

37.772 Users

200M+ IP Search

40B+ Port Search

2.904.391
Domains Discovered

3.229.833
IP Address

576.100
Web Sites

9.968.633
Ports

31.746
Login Pages

30.000
Rogue Mobile Apps

1.166.217
SSL Certificate

21K
Dark Web

18K
Cyber Attack

14K
Ransomware

4K
Defacement

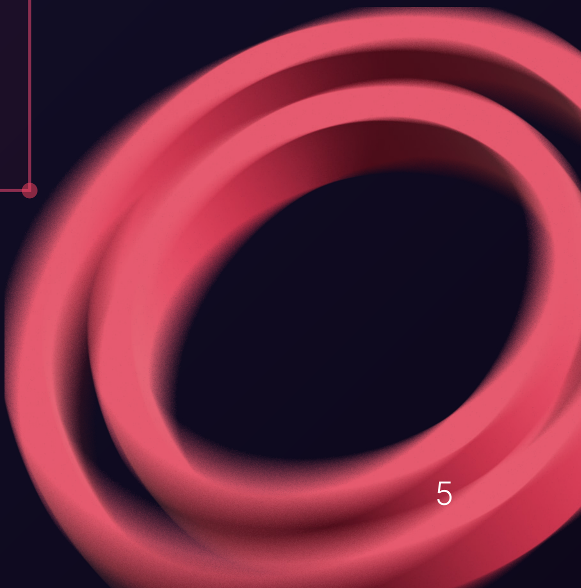
500K
DarkWeb
Notification

18.638.535
Generated Alarms

59.058
ThreatShare

5.000
Scanned Mobile App

13.019.773
PII Stealer

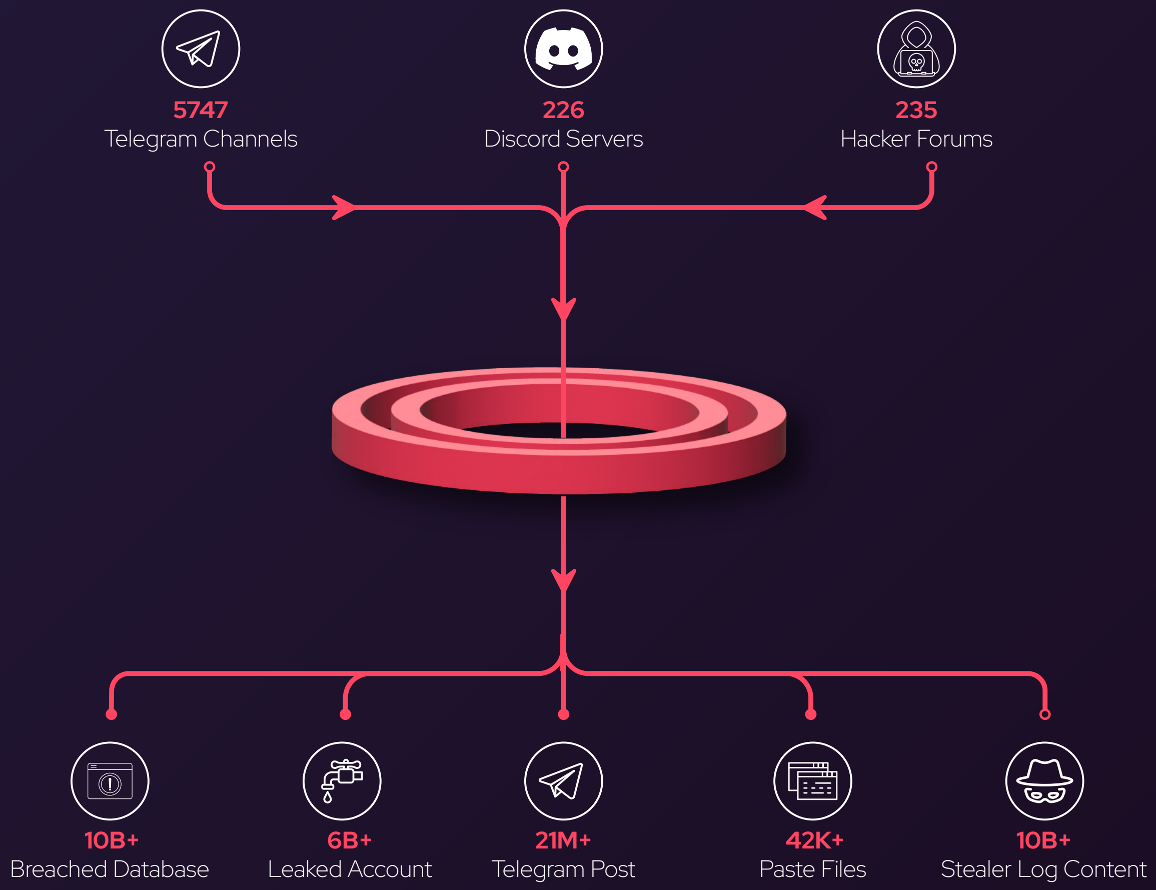


DARK WEB WITH NUMBERS

See behind the shadows:

Wherever threat actors are, **so are we.**

SOCRadar XTI continuously monitors Telegram Channels, Discord Servers, Hacker Forums along with numerous TOR sites and paste sites ;



5747
Telegram Channels

226
Discord Servers

235
Hacker Forums

10B+
Breached Database

6B+
Leaked Account

21M+
Telegram Post

42K+
Paste Files

10B+
Stealer Log Content

Top Data Breaches of 2024

UnitedHealth Ransomware Attack:
In January 2024, UnitedHealth, a leading healthcare provider, faced a ransomware attack that disrupted services and compromised sensitive patient records. This breach underscored the growing threat of ransomware in the healthcare sector and the critical need for robust cybersecurity measures.

Change Healthcare Ransomware Attack:
In February 2024, a major healthcare technology company, Change Healthcare, was targeted by a ransomware attack. The breach affected over 100 million customer records, potentially making it the most significant healthcare breach. The attackers demanded a substantial ransom, which the company paid to swiftly restore essential services and limit disruptions to patient care.

Pandabuy Data Breach:
In March 2024, Pandabuy, a prominent Chinese e-commerce platform, suffered a breach exposing 1.3 million user records, including personal and order information. The incident raised concerns about data protection practices in e-commerce platforms and the potential risks to user privacy.

National Public Data Breach:
In April 2024, National Public Data, a data broker, suffered a massive breach impacting approximately 1.3 billion individuals. The exposed data included personal information such as Social Security numbers, addresses, and dates of birth. This incident is considered one of the largest data breaches in history, highlighting significant vulnerabilities in data brokerage firms.

Acuity Data Breach:
In April 2024, Acuity, a U.S. government technology contractor, was breached, exposing confidential information from the Five Eyes intelligence alliance and the U.S. military. The data, stored in a GitHub repository, included sensitive communications and contact details of government officials. This breach emphasized the risks associated with inadequate data security practices among government contractors.

Snowflake Inc. Data Breach:
Between April and June 2024, cloud data company Snowflake Inc. experienced a significant breach affecting over 100 customers. Hackers accessed sensitive data from clients, including major corporations, by exploiting stolen login credentials. The breach led to the theft of billions of records, raising serious concerns about the security of cloud-based data storage solutions.

Europol Data Breach:
In May 2024, hackers infiltrated the European Union's law enforcement agency, Europol, obtaining over 9,000 confidential records. The compromised data included employee information, source code, and guideline documents. Europol confirmed the breach but stated that no operational information was compromised. This incident highlighted the need for enhanced cybersecurity measures within international law enforcement agencies.

AMD Data Breach:
In June 2024, semiconductor giant AMD was targeted by hackers who claimed to have accessed data on future products, employee information, customer details, source code, and financial records. AMD acknowledged the breach and collaborated with law enforcement, stating that the incident was limited in scope and would not materially impact the business. The breach underscored the importance of protecting intellectual property in the tech industry.

Internet Archive Data Breach:
In October 2024, the Internet Archive, including its Wayback Machine, suffered a cyberattack that exposed the data of 31 million users. The breach involved email addresses, usernames, and bcrypt password hashes. A hacktivist group linked to pro-Palestinian movements claimed responsibility, leading to concerns over the security of digital archives and the potential misuse of user data.

Chinese Hackers Infiltrate U.S. Telecoms:
In November 2024, it was revealed that Chinese hackers had infiltrated major U.S. telecommunications providers, including Verizon and AT&T. They accessed sensitive cellular logs, enabling millions of Americans to track their geolocation and record their calls. The breach, which began at least eight months prior, raised significant national security concerns and highlighted the vulnerabilities in critical infrastructure.

Top Cybersecurity Incidents of 2024

Midnight Blizzard Targets Microsoft Executives

In January 2024, the Russian threat actor Midnight Blizzard breached Microsoft's corporate email systems, focusing on high-ranking executives in cybersecurity and legal departments. The espionage operation, which started in late 2023 and was uncovered in January, included data theft as part of a more considerable effort to compromise private organizations.

Change Healthcare Ransomware Attack

The Alphv/BlackCat ransomware group orchestrated an attack on Change Healthcare in February 2024, severely disrupting healthcare services across the United States. The breach exposed the sensitive medical information of over 100 million individuals, making it one of the most significant healthcare-related data breaches. The organization reportedly paid a $22 million ransom to restore operations.

XZ Utils Supply Chain Attack

In March 2024, the XZ Utils compression utility discovered a backdoor vulnerability (CVE-2024-3094). This supply chain compromise seriously threatened thousands of downstream systems worldwide before it was successfully identified and neutralized.

Snowflake Data Breach

In April 2024, the Scattered Spider group exploited weak security configurations in Snowflake's cloud platform, exposing massive datasets. High-profile organizations like AT&T and Santander Bank were affected, and terabytes of sensitive information were stolen during the breach.

National Public Data Breach

Hackers infiltrated National Public Data's systems in April 2024, exposing 2.9 billion records containing personal details such as Social Security numbers and phone numbers. The stolen database, reportedly sold for $3.5 million on the dark web, highlighted vulnerabilities in data broker practices.

Dell Data Breach

A breach at Dell Technologies in May 2024 compromised 49 million customer records, including names, addresses, and order histories. Although no financial details were exposed, the leaked data could be misused in phishing or scams.

CrowdStrike Falcon Update Outage

In July 2024, a problematic update for CrowdStrike’s Falcon platform caused a widespread IT outage that disrupted 8.5 million devices across critical sectors such as healthcare and aviation. The incident is estimated to have caused $5.4 billion in damages for Fortune 500 companies.

Internet Archive Attack

In September 2024, pro-Palestinian hackers targeted the Internet Archive, exposing over 31 million files. The attack also included distributed denial-of-service (DDoS) incidents, which significantly interrupted the non-profit's operations.

OpenAI’s Generative AI Exploitation Attempts

In October 2024, OpenAI reported thwarting more than 20 attempts by state-sponsored groups from countries like Russia, China, and Iran to misuse its large language models (LLMs). These malicious activities ranged from phishing campaigns to reconnaissance and malware development.

China's Salt Typhoon Campaign

Throughout 2024, the Chinese state-backed group Salt Typhoon infiltrated major U.S. telecom networks, stealing metadata and communications involving political figures and corporations. This campaign demonstrated China's strategic reliance on cyber espionage to achieve geopolitical goals.

Most Exploited Vulnerabilities of 2024

In 2024, several vulnerabilities have been notably exploited, posing significant risks to organizations and systems. Here are the most exploited vulnerabilities identified this year, along with their CVSS scores:

CVE-2024-9680
(Mozilla Firefox Use-After-Free Vulnerability)
CVSS Score: 9.8
Details: A critical "Use-After-Free" vulnerability in Mozilla Firefox's developer tools allows attackers to remotely execute arbitrary code by exploiting memory corruption when users visit malicious websites. This vulnerability poses a severe risk for users who frequently interact with developer tools, and Mozilla has released patches to address it.

CVE-2024-20424
(Cisco Firewall Management Command Injection)
CVSS Score: 9.9
Details: This command injection vulnerability in Cisco's Firewall Management Center allows authenticated attackers to gain root-level control of the underlying operating system by executing specially crafted commands. The issue affects several platform versions, and a timely patch has been released to prevent potential exploitation.

CVE-2024-7589
(VMware vCenter Server Heap Overflow)
CVSS Score: 9.8
Details: A heap overflow vulnerability in the VMware vCenter Server allows attackers to exploit a flaw in the DCERPC protocol to execute remote code. This vulnerability can be exploited over the network, posing a significant risk to enterprises relying on vCenter for virtualized infrastructure management. VMware issued a comprehensive patch after an earlier incomplete fix.

CVE-2024-38018
(Microsoft SharePoint Remote Code Execution)
CVSS Score: 8.8
Details: A vulnerability in Microsoft SharePoint Server enables attackers with Site Owner permissions to execute arbitrary code by exploiting a flaw in the server's handling of permissions and user inputs. This can result in complete control of the affected SharePoint site and its data.

CVE-2024-38194
(Microsoft Azure Web Apps Authorization Flaw)
CVSS Score: 8.4
Details: This vulnerability in Microsoft Azure Web Apps allows authenticated attackers to exploit an authorization flaw, enabling unauthorized actions such as data exfiltration or privilege escalation. Organizations using Azure-hosted applications are advised to review and apply security updates promptly.

CVE-2024-29824
(Ivanti Endpoint Manager SQL Injection)
CVSS Score: 8.8
Details: An SQL injection vulnerability in Ivanti Endpoint Manager allows unauthenticated attackers to manipulate backend databases and compromise sensitive information. Exploitation can lead to system takeover or operational disruption, making this an actively exploited vulnerability in 2024.

CVE-2024-21762
(Fortinet FortiOS and FortiProxy Arbitrary Code Execution)
CVSS Score: 9.8
Details: An arbitrary code execution vulnerability in Fortinet FortiOS and FortiProxy allows attackers to exploit a specially crafted HTTP request to run arbitrary commands on the device. Threat actors have actively targeted this issue, putting unpatched systems at immediate risk.

CVE-2024-37341

(Microsoft SQL Server Privilege Escalation)

CVSS Score: 8.8

Details: A privilege escalation vulnerability in Microsoft SQL Server lets attackers with limited access escalate their permissions to gain administrative control over the database. This vulnerability could result in unauthorized modifications to critical data or system configurations.

CVE-2024-21416

(Windows TCP/IP Remote Code Execution)

CVSS Score: 9.8

Details: A Windows TCP/IP stack flaw enables attackers to send specially crafted packets, allowing remote code execution on affected systems. If exploited, this vulnerability can lead to complete system compromise, affecting all devices running unpatched versions of Windows.

CVE-2024-3400

(Palo Alto Networks PAN-OS Command Execution)

CVSS Score: 9.0

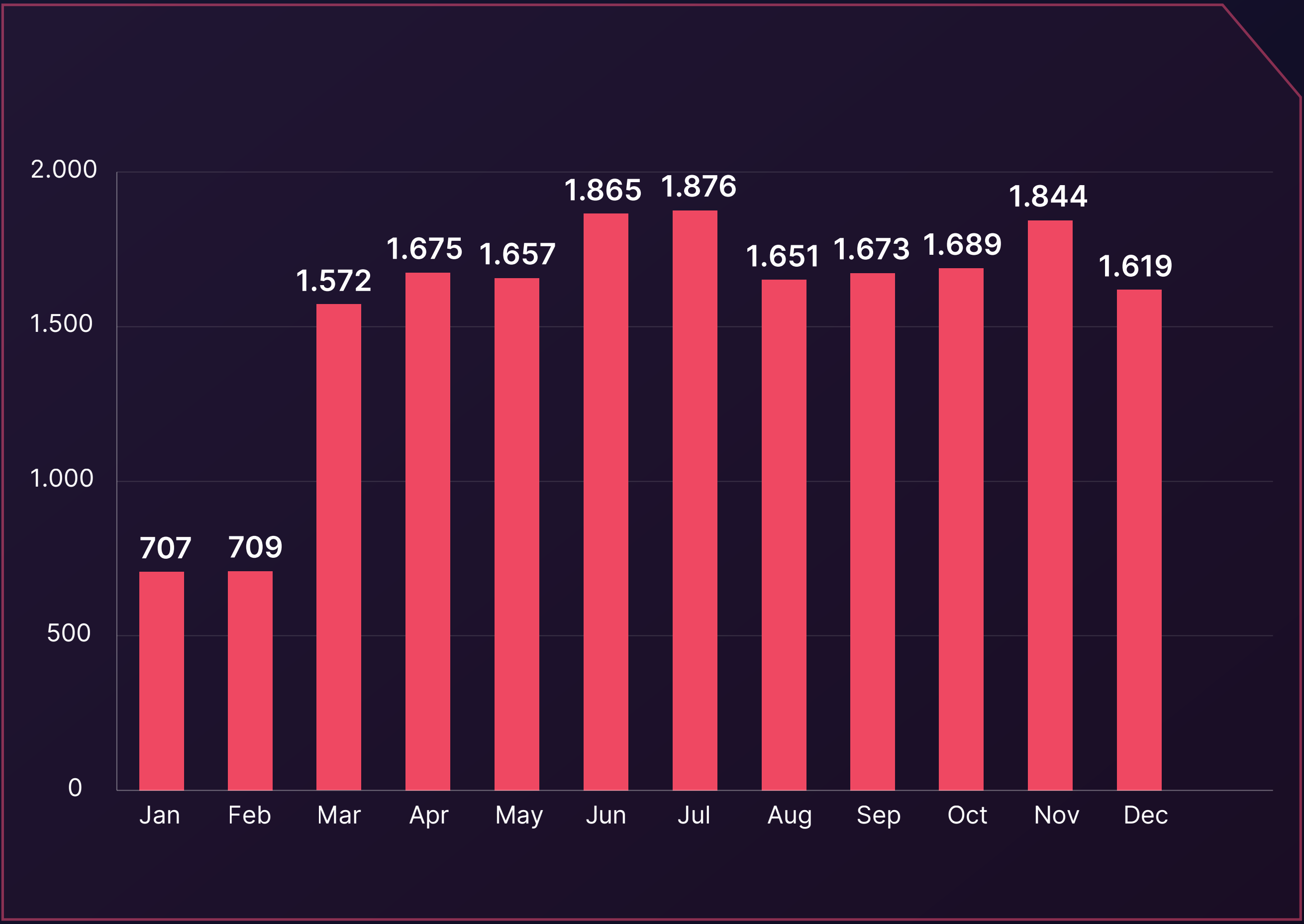
Details: A command injection vulnerability in Palo Alto Networks PAN-OS enables attackers to execute unauthorized commands on affected devices. Exploiting this flaw could allow attackers to gain complete control of the device, disrupt operations, or access sensitive data.

Dark Web Statistics of 2024

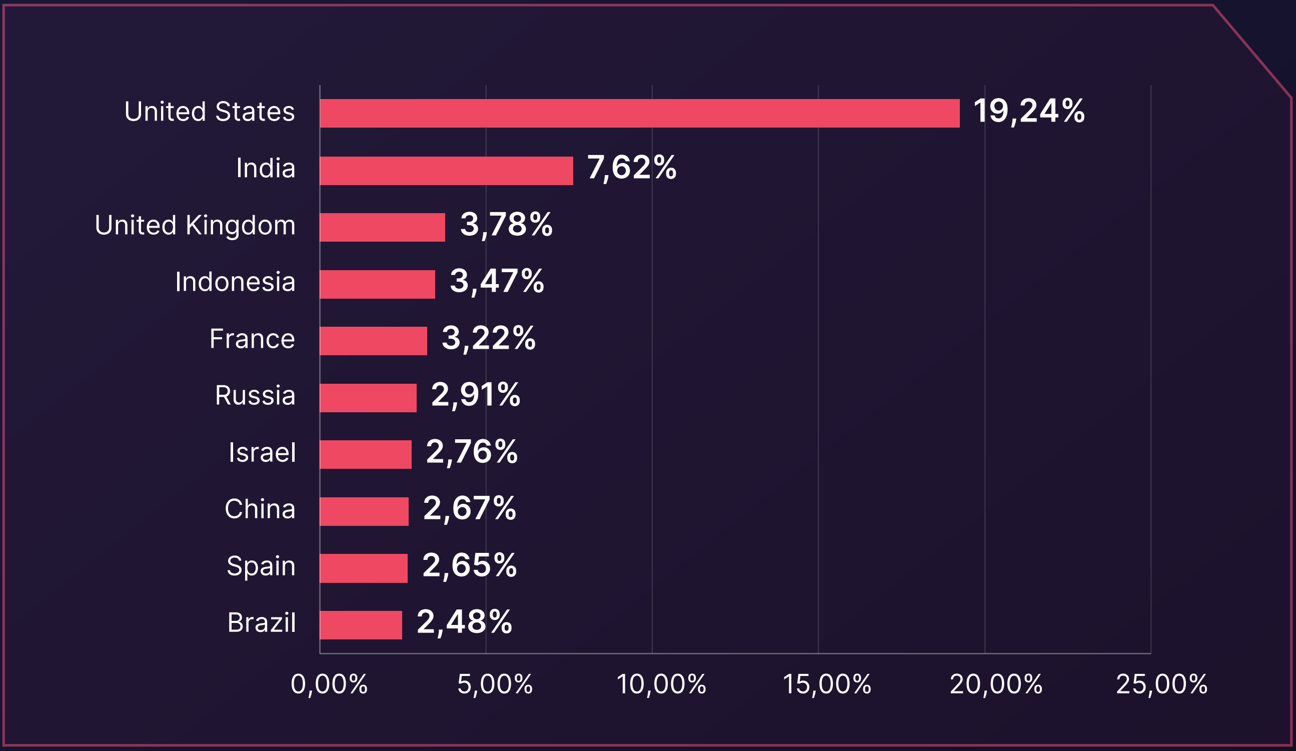
This section provides insights into the data gathered by SOCRadar in 2024. This data was collected through the SOCRadar XTI Platform, which utilizes Machine Learning, Artificial Intelligence, and expert analysts to monitor threat actor activities across various sources, including Dark Web forums and markets, Telegram groups, and ransomware group blog pages.

The total number of posts published on the platform's Dark Web News channel during this period was 18,537, with a daily average of 50.7 posts.

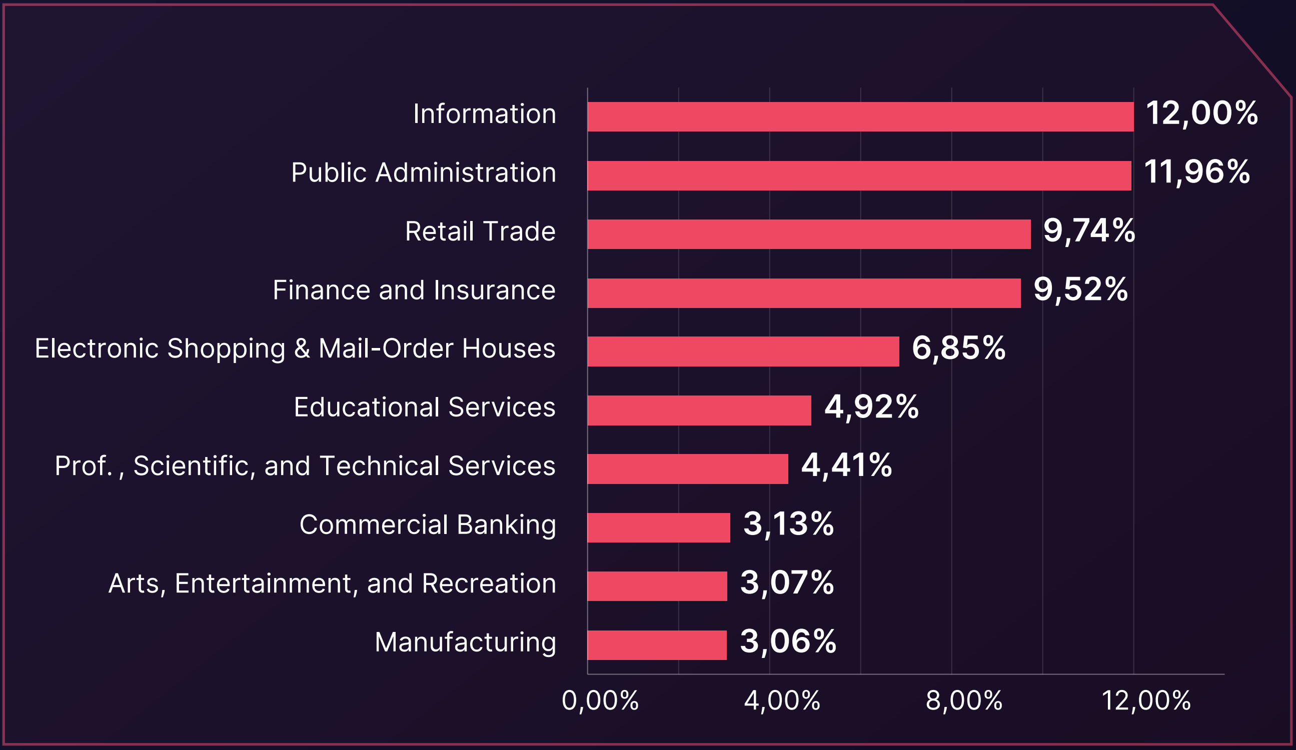
Dark Web Threats - Monthly Distrubution



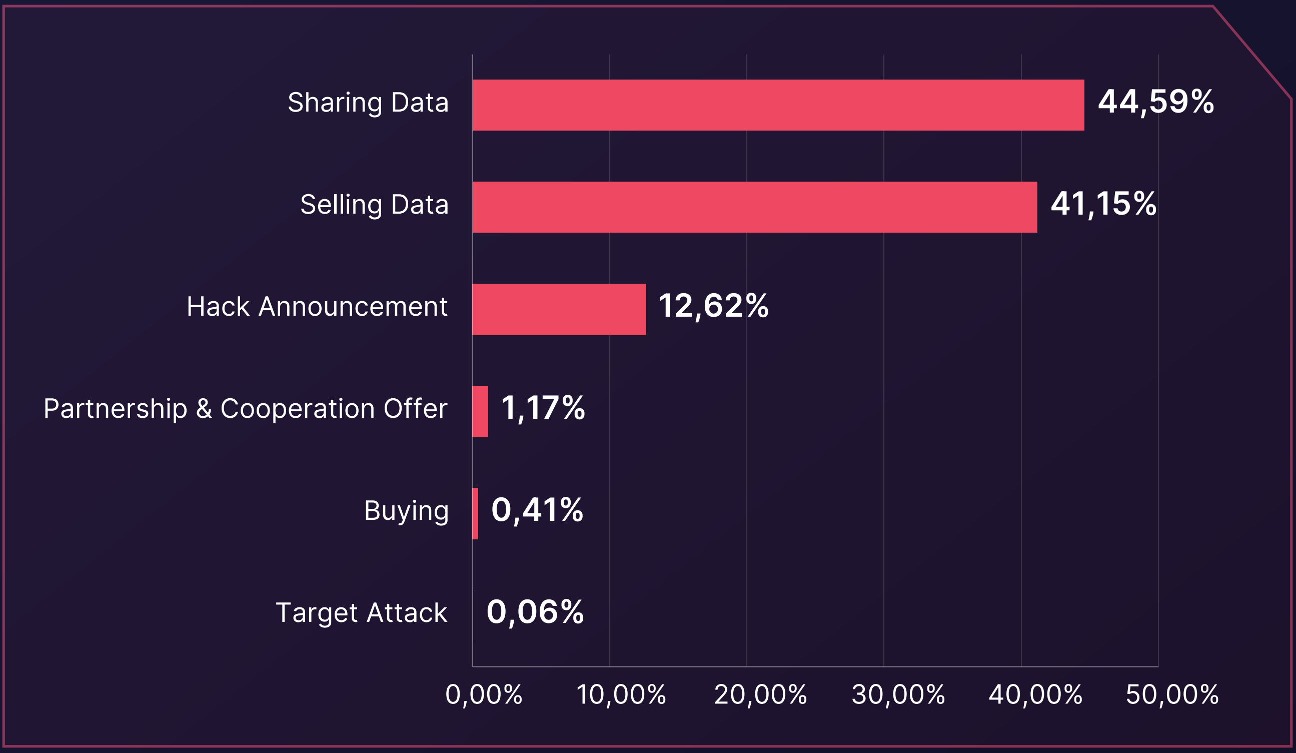
Dark Web Threats - Distribution by Target Country

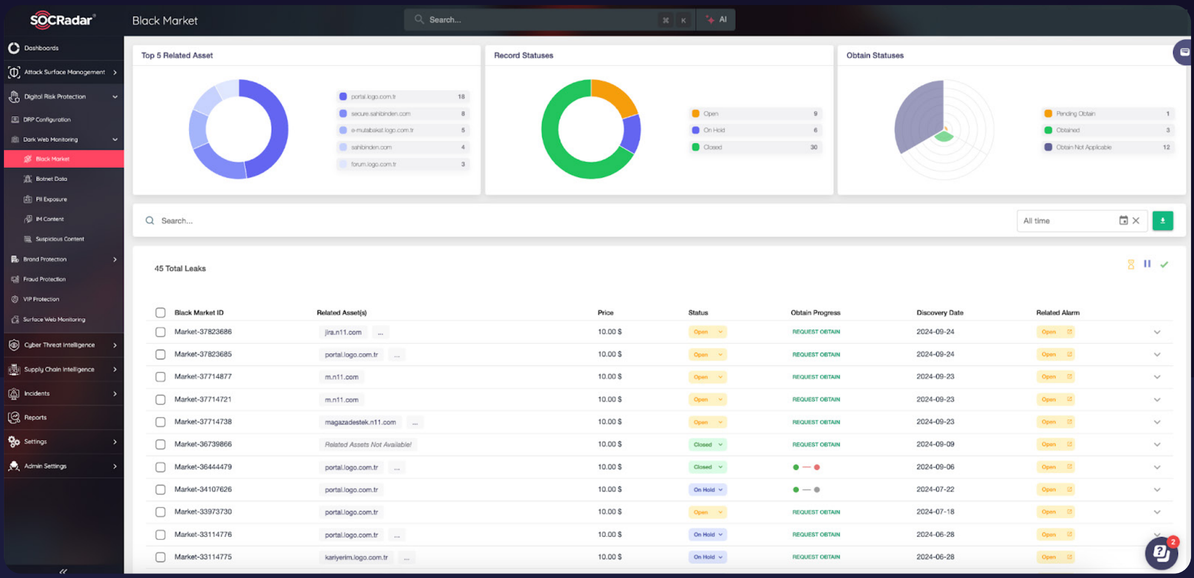


Dark Web Threats - Distribution by Industry



Dark Web Threats - Distribution by Threat Category





45 Total Leaks

Black Market ID	Related Asset(s)	Price	Status	Obtain Progress	Discovery Date	Related Alarm
Market-37823686	jira.n11.com ...	10.00 $	Open	REQUEST OBTAIN	2024-09-24	Open
Market-37823685	portal.logo.com.tr ...	10.00 $	Open	REQUEST OBTAIN	2024-09-24	Open
Market-37714877	m.n11.com	10.00 $	Open	REQUEST OBTAIN	2024-09-23	Open
Market-37714721	m.n11.com	10.00 $	Open	REQUEST OBTAIN	2024-09-23	Open
Market-37714738	magazadestek.n11.com ...	10.00 $	Open	REQUEST OBTAIN	2024-09-23	Open
Market-36739866	*Related Assets Not Available!*	10.00 $	Closed	REQUEST OBTAIN	2024-09-09	Open
Market-36444479	portal.logo.com.tr ...	10.00 $	Closed	● — ●	2024-09-06	Open
Market-34107626	portal.logo.com.tr	10.00 $	On Hold	● — ●	2024-07-22	Open
Market-33973730	portal.logo.com.tr	10.00 $	Open	REQUEST OBTAIN	2024-07-18	Open
Market-33114776	portal.logo.com.tr ...	10.00 $	On Hold	REQUEST OBTAIN	2024-06-28	Open
Market-33114775	kariyerim.logo.com.tr ...	10.00 $	On Hold	REQUEST OBTAIN	2024-06-28	Open

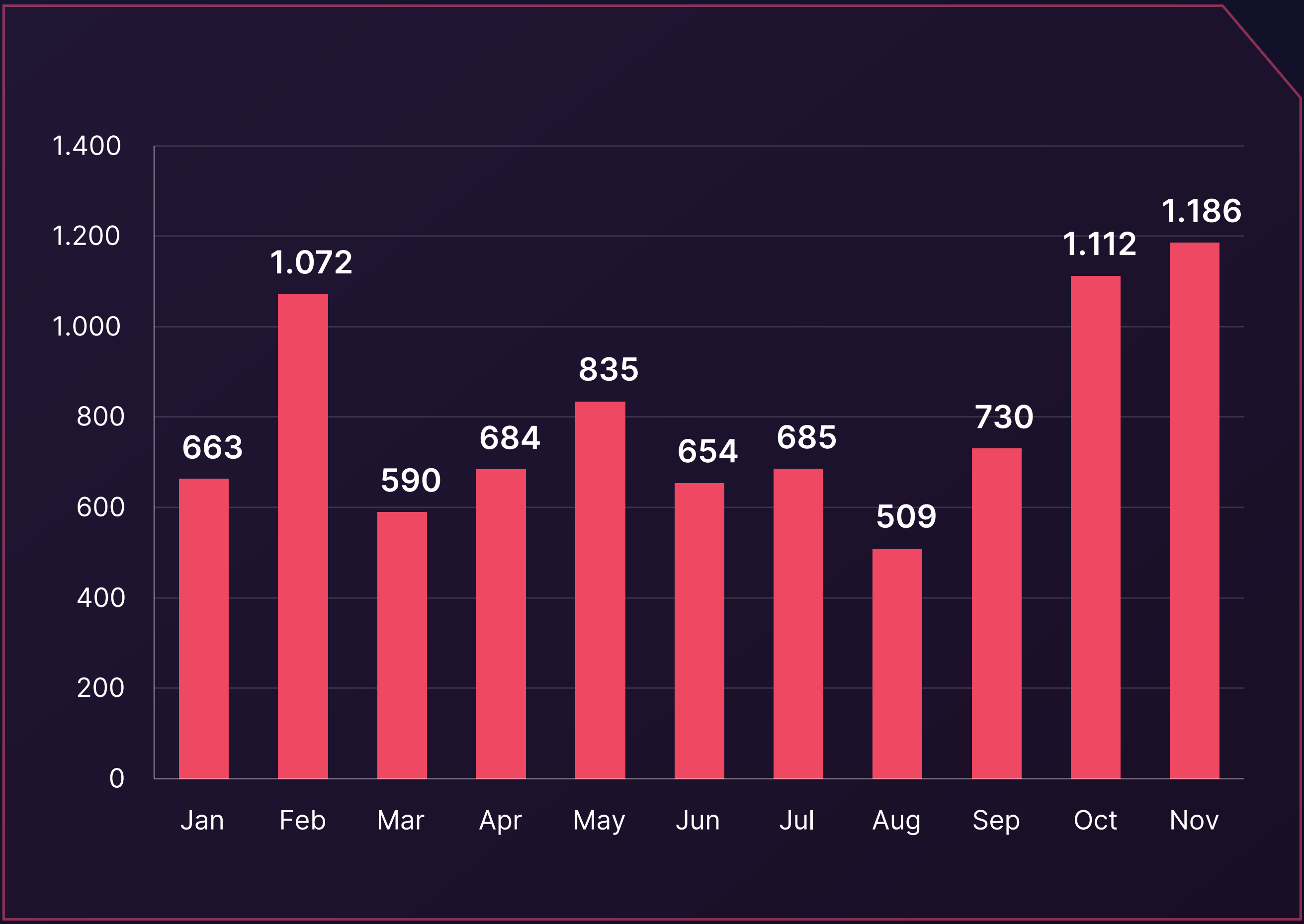
SOCRadar's Advanced Dark Web Monitoring equips organizations in Nordic countries with vital insights into hidden threats targeting key industries such as finance, insurance, and information technology, which have faced significant risks over the past year. By providing real-time monitoring of underground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

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

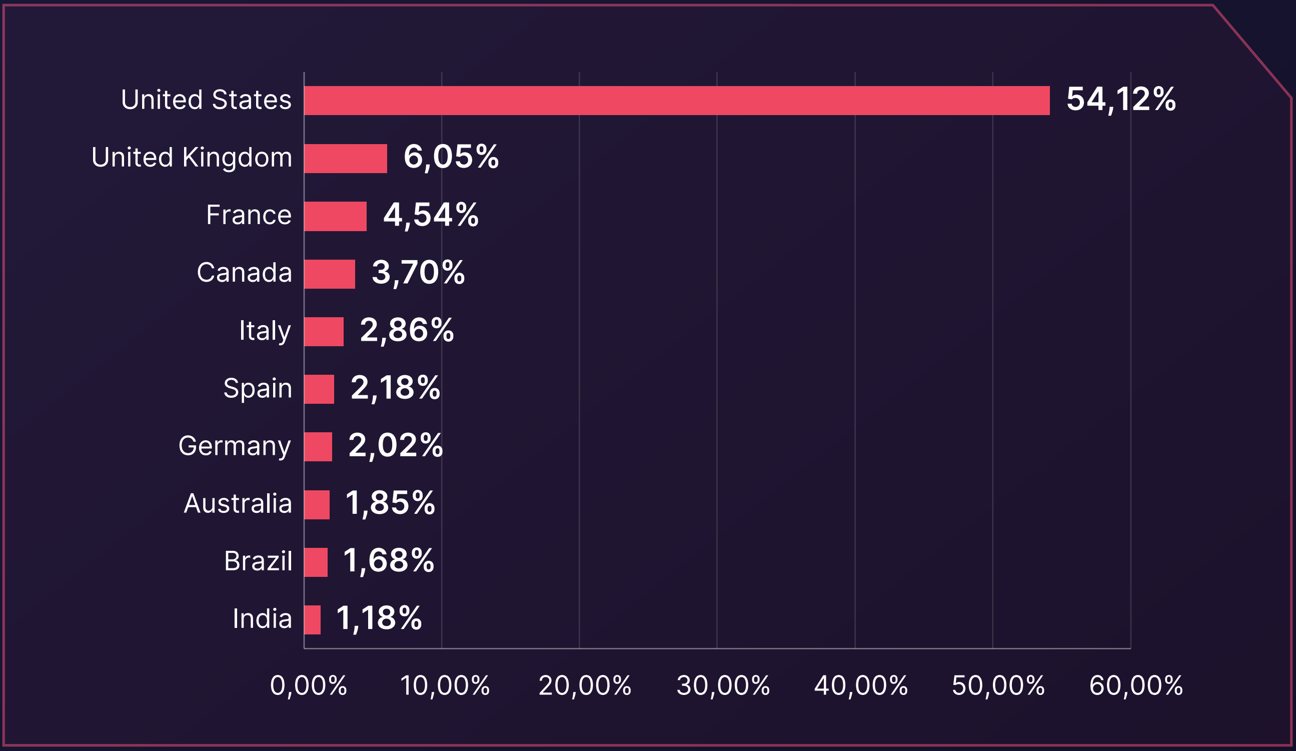
Ransomware Statistics of 2024

The data is sourced from a comprehensive analysis conducted by SOCRadar analysts during 2024. We've scoured ransomware groups' blog sites, leak sites, and Telegram channels to compile a trove of valuable information. Over this period, we've gathered a staggering total of 9,678 posts related to ransomware attacks, equating to an average of 806 posts per month or 27 posts per day.

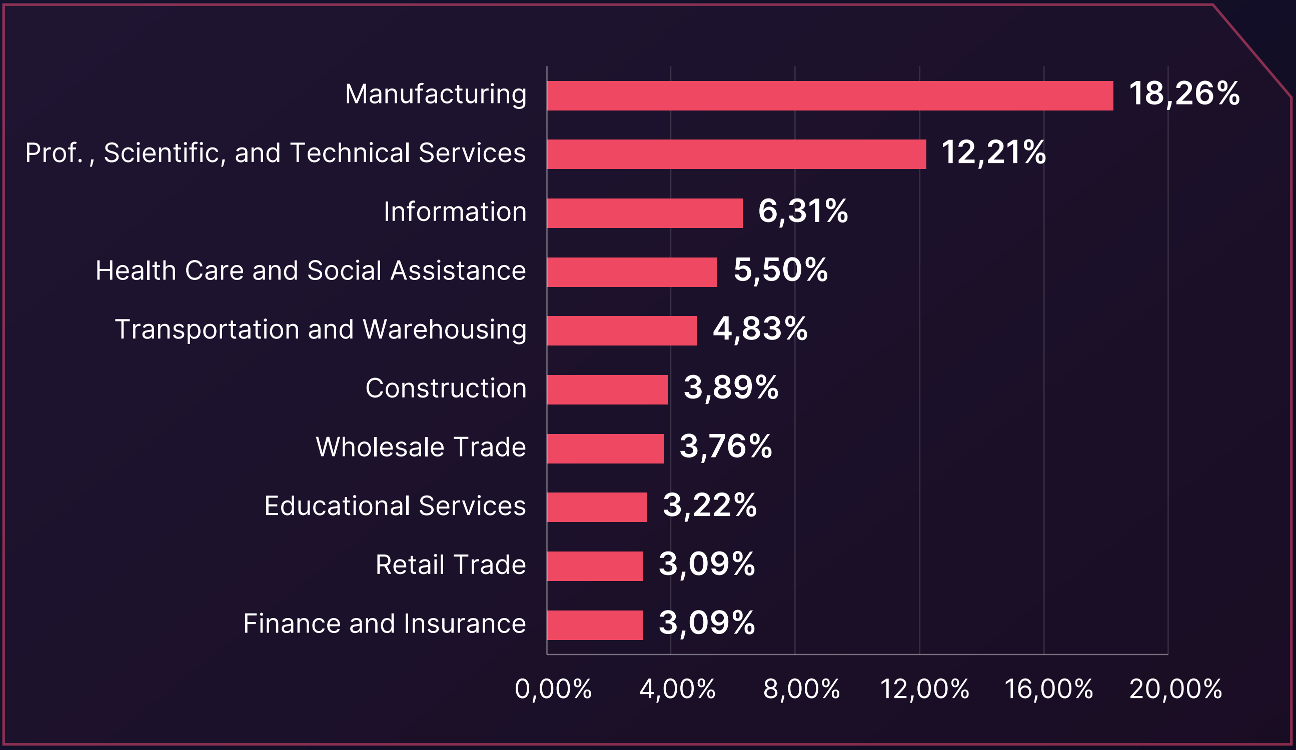
Ransomware Attacks - Monthly Distribution



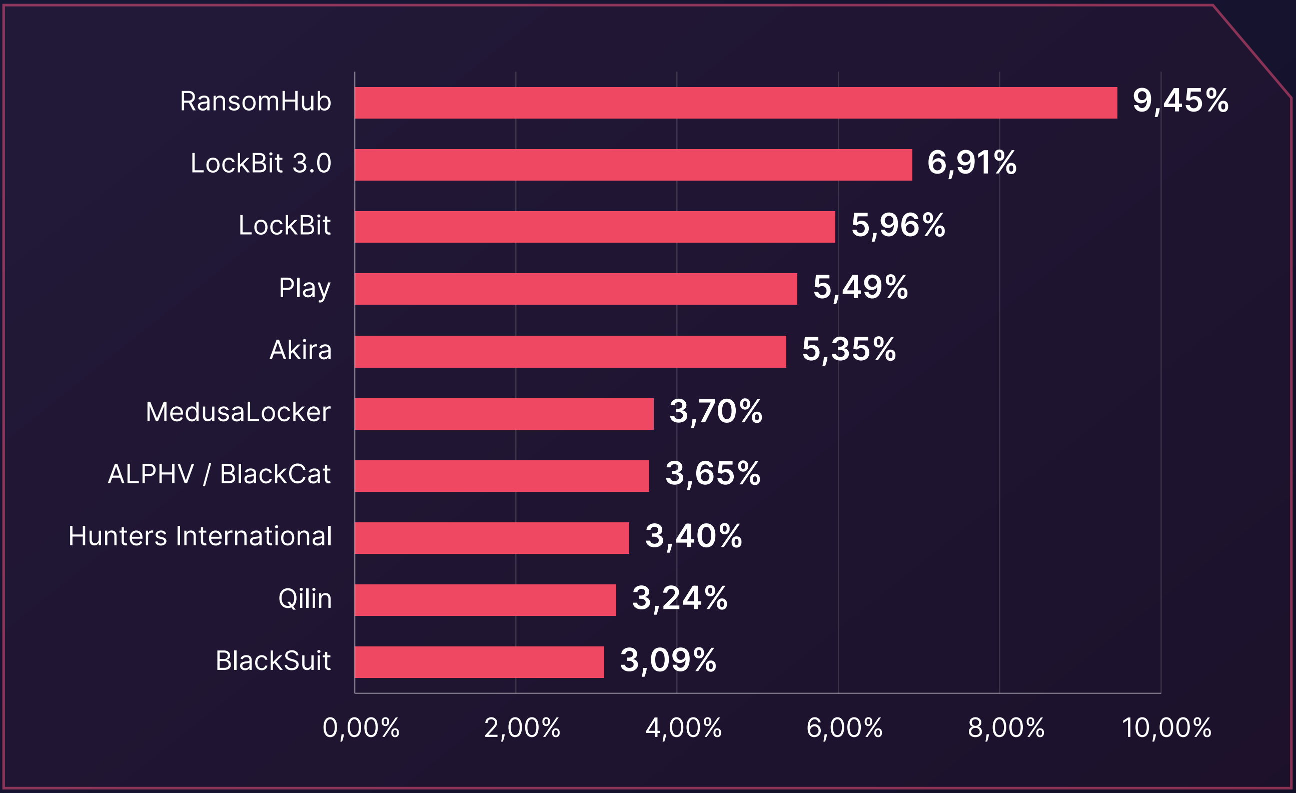
Ransomware Attacks - Distribution by Target Country

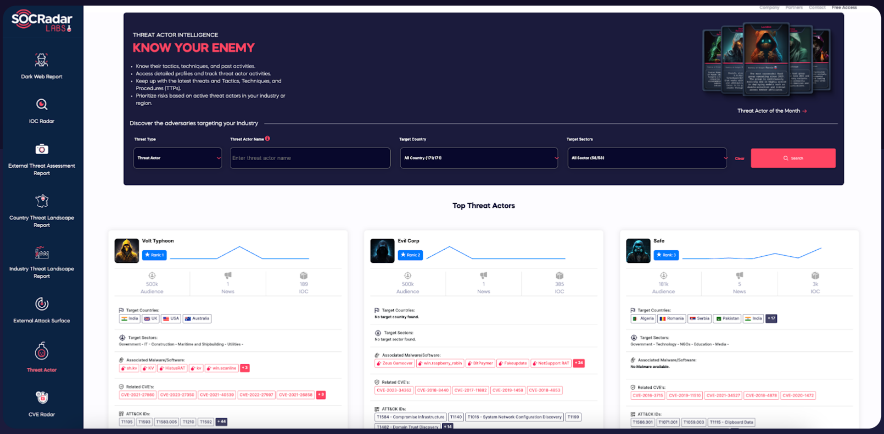


Ransomware Attacks - Distribution by Industries



Ransomware Group Activity Analysis





THREAT ACTOR INTELLIGENCE

KNOW YOUR ENEMY

- Know their tactics, techniques, and past activities.
- Access detailed profiles and track threat actor activities.
- Keep up with the latest threats and Tactics, Techniques, and Procedures (TTPs).
- Prioritize risks based on active threat actors in your industry or region.

Discover the adversaries targeting your industry

Threat Type: Threat Actor
Threat Actor Name: Enter threat actor name
Target Country: All Country (171/171)
Target Sectors: All Sector (58/58)

Top Threat Actors

Volt Typhoon
★ Rank: 1
500k Audience | 1 News | 189 IOC
Target Countries: India, UK, USA, Australia
Target Sectors: Government - IT - Construction - Maritime and Shipbuilding - Utilities -
Associated Malware/Software: sh.kv, KV, HiatusRAT, kv, win.scanline, +3
Related CVE's: CVE-2021-27860, CVE-2023-27350, CVE-2021-40539, CVE-2022-27997, CVE-2021-26858, +3
ATT&CK IDs: T1105, T1593, T1583.005, T1210, T1592, +44

Evil Corp
★ Rank: 2
500k Audience | 1 News | 385 IOC
Target Countries: No target country found.
Target Sectors: No target sector found.
Associated Malware/Software: Zeus Gameover, win.raspberry_robin, BitPaymer, Fakeupdate, NetSupport RAT, +24
Related CVE's: CVE-2023-34362, CVE-2018-8440, CVE-2017-11882, CVE-2019-1458, CVE-2018-4853
ATT&CK IDs: T1584 - Compromise Infrastructure, T1140, T1016 - System Network Configuration Discovery, T1199, T1482 - Domain Trust Discovery, +14

Safe
★ Rank: 3
181k Audience | 5 News | 3k IOC
Target Countries: Algeria, Romania, Serbia, Pakistan, India, +17
Target Sectors: Government - Technology - NGOs - Education - Media -
Associated Malware/Software: No Malware available.
Related CVE's: CVE-2016-3715, CVE-2019-11510, CVE-2021-34527, CVE-2018-4878, CVE-2020-1472
ATT&CK IDs: T1566.001, T1071.001, T1059.003, T1115 - Clipboard Data

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

SOCRadar®
Your Eyes Beyond

MOST DANGEROUS THREAT ACTORS IN 2024

Qilin Ransomware

Country of Origin: Russ

Qilin, also known a
ransomware, represents
threat in cybercrime.
known RaaS groups, is c
adaptability in mind, a
customize attacks ba
victims' specific env
Originating from a so
background, Qilin lever
tactics to extort org

Akira Ransomware

nknown

, active since
nown for its
rategy and
a leak site,
ted over 250
and amassed
42 million in
proceeds.

LockBit

Country of Origin: Russia

The most successful RaaS group operating since 2019. The group is continuously evolving and is highly active in deploying models such as double-extortion and initial access broker affiliates.

RansomHub

Country of Origin: Unknown

RansomHub, discovered in early 2024, emerged as a major ransomware threat, leveraging RaaS to exploit vulnerabilities and share ransoms with affiliates.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	US, UK, France, Brazil, Indonesia, Vietnam, Canada
Target Sectors:	Healthcare, Manufacturing, Business Services
Attack Type:	Ransomware, Data Leakage, Extortion

-TTPs-

Exploit Public-Facing Application:	T1190
Remote Services: Remote Desktop Protocol:	T1486
Data Encrypted for Impact:	T1133

LockBit

Country of Origin: Russia

The most successful RaaS group operating since 2019. The group is continuously evolving and is highly active in deploying models such as double-extortion and initial access broker affiliates.

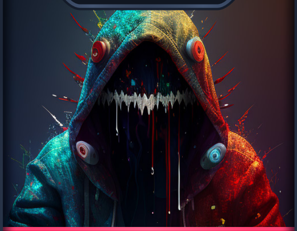
-Ransomware Group-

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

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

Akira Ransomware

Country of Origin: Unknown

Akira Ransomware, active since early 2023, known for its extortion strategy and distinctive data leak site, Akira has affected over 250 organizations and amassed approximately $42 million in ransomware proceeds.

-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

Medusa Ransomware

Country of Origin: Unknown

Medusa is a RaaS group operating since June 2021 and known for its many variants. The group is primarily targeting North American and European organizations.

-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

BlackCat Ransomware

Country of Origin: Russia 🇷🇺

BlackCat, or ALPHV, is a ransomware group known for being the pioneer to use Rust and the group first announced its RaaS affiliate program in a Dark Web forum in December 2021.

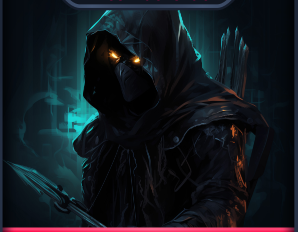
-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Canada, Germany, Australia, France, Italy, Spain
Target Sectors:	Professional Services, Manufacturing, Healthcare, Finance, Information Technology
Attack Type:	Spearphishing, Stolen Credentials, RaaS, Ransomware, Triple-Extortion

-TTPs-

User Execution: Malicious File:	T1204.002
Defacement:	T1491
Data Encrypted for Impact:	T1486

Hunters International



Country of Origin: Unknown

Hunters International surfaced following the disruption of the Hive ransomware group by law enforcement in Q3 of 2023. Showing substantial technical similarities, it appears to be a successor or offshoot of Hive.

-Ransomware Group-

Motivation:	Financial
Target Countries:	US, Europe, Canada, Brazil, New Zealand, Japan
Target Sectors:	Healthcare, Manufacturing, Automative, Logistics, Education
Attack Type:	Extortion, Encryption

-TTPs-

Boot or Logon Autostart Execution:	T1547.001
Obfuscated Files or Information:	T1027
Data Encrypted for Impact:	T1486

Qilin Ransomware

Country of Origin: Russia

Qilin, also known as Agenda ransomware, represents a formidable threat in cybercrime. One of the known RaaS groups, is designed with adaptability in mind, allowing it to customize attacks based on its victims' specific environments. Originating from a sophisticated background, Qilin leverages advanced tactics to extort organizations.

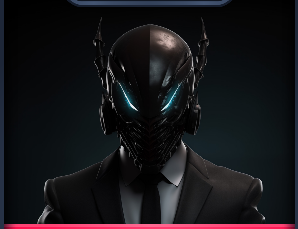
-Ransomware Group-

Motivation:	Financial
Target Countries:	US, UK, Brazil,Argentina
Target Sectors:	Public Administration, Healthcare, Education
Attack Type:	Encryption, Data Theft, Double Extortion

-TTPs-

Phishing:	T1566
System Services: Service Execution:	T1569.002
Data Encrypted for Impact:	T1486

BlackSuit Ransomware



Country of Origin: Russia

BlackSuit first emerged in May 2023 and appears to be closely linked to the Royal ransomware gang, which itself originated from the remnants of the infamous Conti group. BlackSuit has gained notoriety for carrying out major attacks targeting organizations in critical sectors such as healthcare and education, among others.

-Ransomware-

Motivation:	Financial
Target Countries:	US, Canada, Brazil,Italy
Target Sectors:	Public Administration, Healthcare, Education
Attack Type:	Encryption, Data Theft, Exfiltration

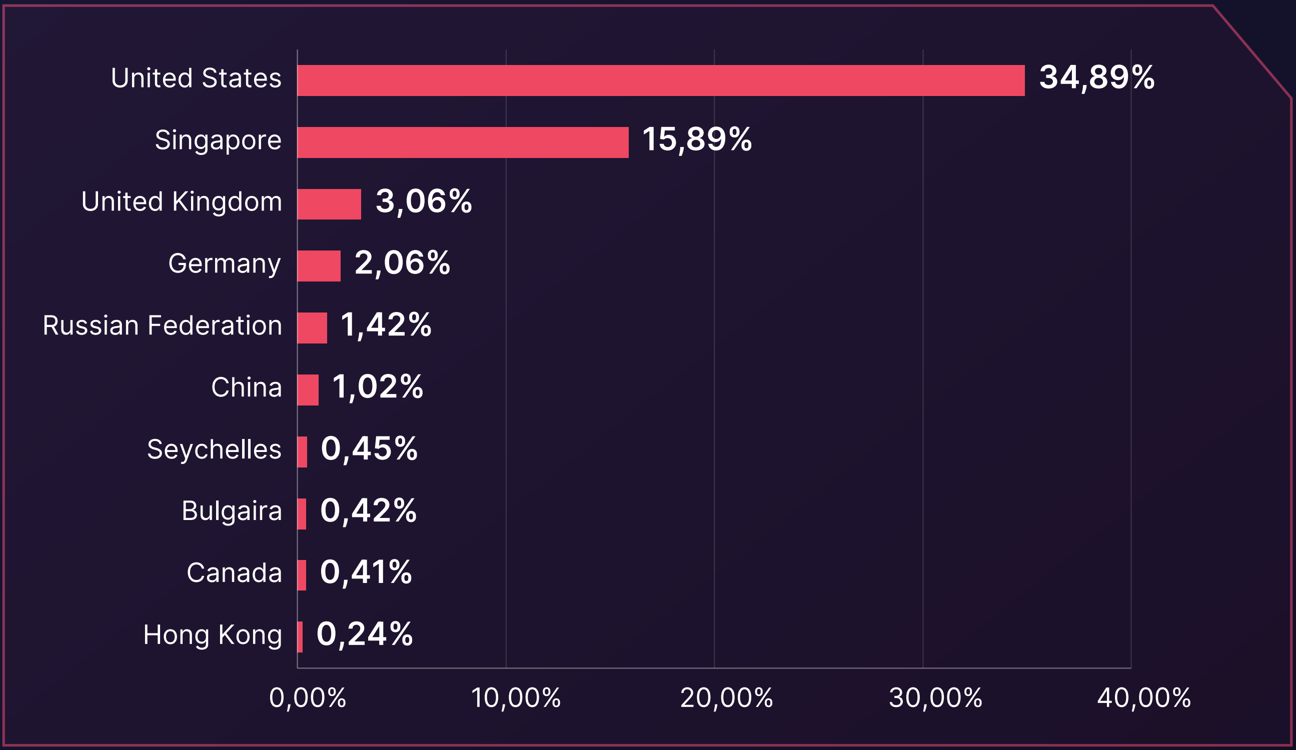
-TTPs-

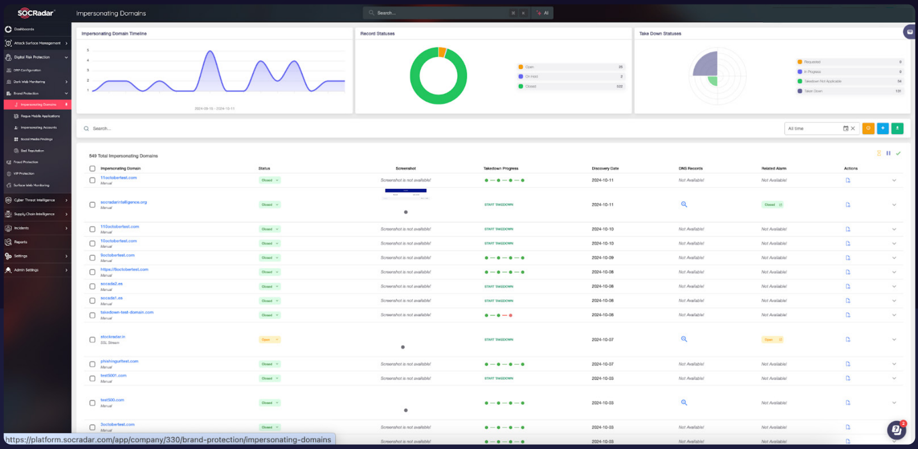
User Execution:	T1204
File and Directory Discovery:	T1083
Data Encrypted for Impact:	T1486

Global Phishing Trends

Phishing remains a highly effective tactic for breaching an organization's infrastructure. It often involves tricking individuals into providing sensitive credentials on fake websites.

Phishing Attacks - Distribution by Target Country





Record Statuses

Open	25
On Hold	2
Closed	522

Take Down Statuses

Requested	0
In Progress	0
Takedown Not Applicable	54
Taken Down	131

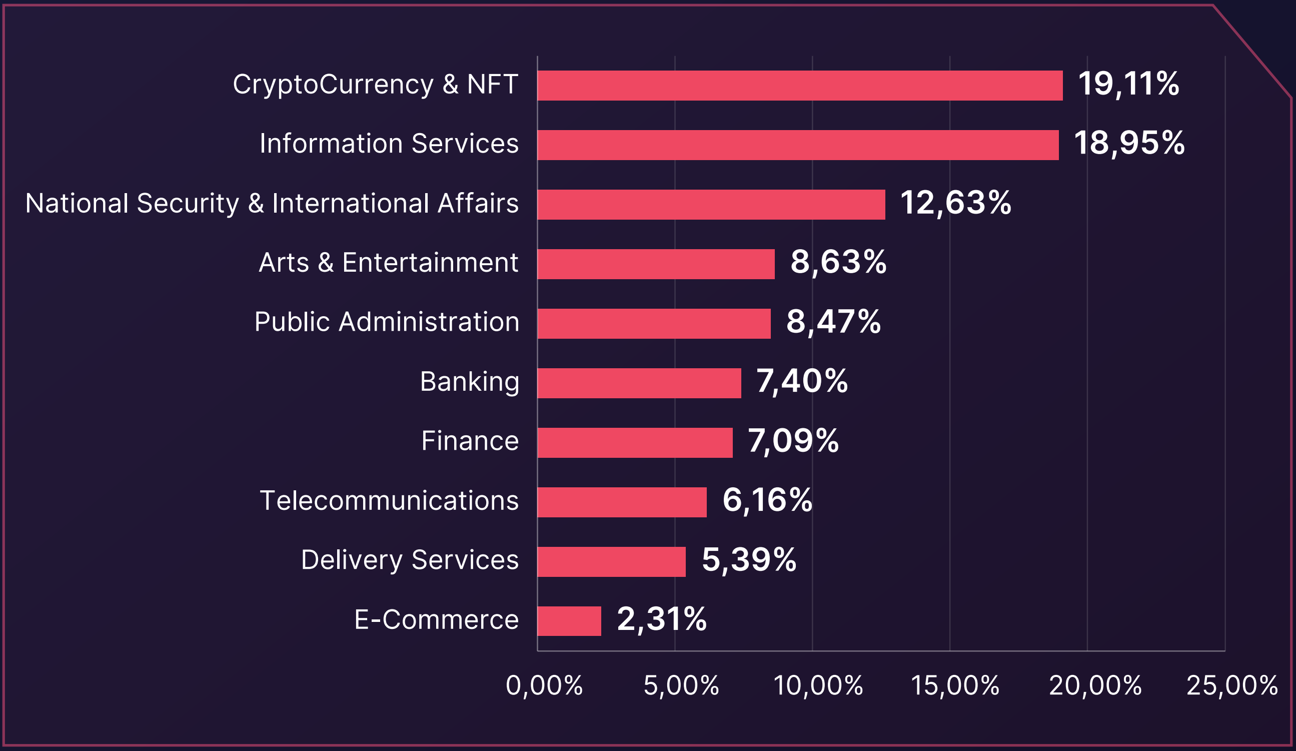
549 Total Impersonating Domains

□	Impersonating Domain	Status	Screenshot	Takedown Progress	Discovery Date	DNS Records	Related Alarm	Actions
□	11octobertest.com Manual	Closed	Screenshot is not available!	●—●—●—●	2024-10-11	Not Available!	Not Available!	
□	socradarintelligence.org Manual	Closed		START TAKEDOWN	2024-10-11		Closed	
□	110octobertest.com Manual	Closed	Screenshot is not available!	START TAKEDOWN	2024-10-10	Not Available!	Not Available!	
□	10octobertest.com Manual	Closed	Screenshot is not available!	START TAKEDOWN	2024-10-10	Not Available!	Not Available!	
□	9octobertest.com Manual	Closed	Screenshot is not available!	●—●—●—●	2024-10-09	Not Available!	Not Available!	
□	https://8octobertest.com Manual	Closed	Screenshot is not available!	●—●—●—●	2024-10-08	Not Available!	Not Available!	
□	socada2.es Manual	Closed	Screenshot is not available!	START TAKEDOWN	2024-10-08	Not Available!	Not Available!	
□	socada1.es Manual	Closed	Screenshot is not available!	START TAKEDOWN	2024-10-08	Not Available!	Not Available!	
□	takedown-test-domain.com Manual	Closed	Screenshot is not available!	●—●—●	2024-10-08	Not Available!	Not Available!	
□	stockradar.in SSL Stream	Open		START TAKEDOWN	2024-10-07		Open	
□	phishingurltest.com Manual	Closed	Screenshot is not available!	●—●—●—●	2024-10-07	Not Available!	Not Available!	
□	test5001.com Manual	Closed	Screenshot is not available!	START TAKEDOWN	2024-10-03	Not Available!	Not Available!	
□	test500.com Manual	Closed		●—●—●—●	2024-10-03		Not Available!	
□	3octobertest.com Manual	Closed	Screenshot is not available!	●—●—●—●	2024-10-03	Not Available!	Not Available!	
			Screenshot is not available!	●—●—●—●	2024-10-03	Not Available!	Not Available!	

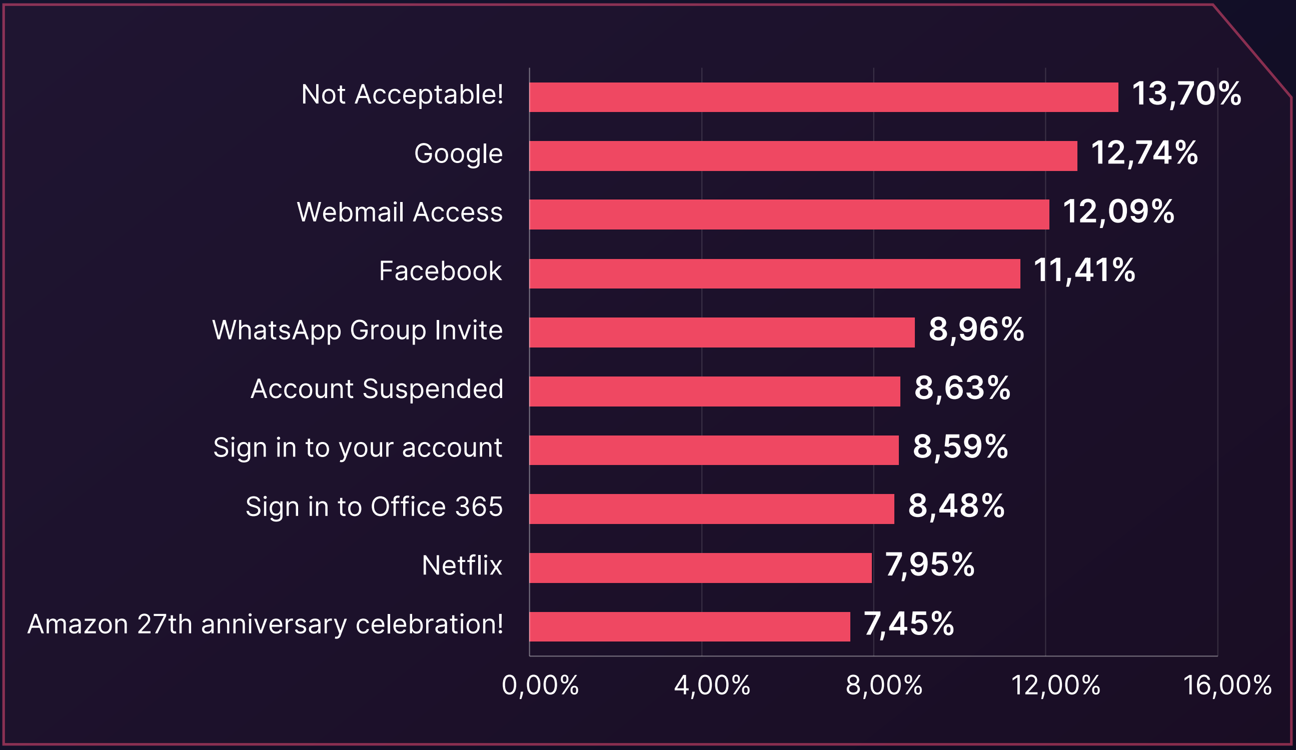
https://platform.socradar.com/app/company/330/brand-protection/impersonating-domains

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.**

Phishing Attacks - Distribution by Industry



Phishing Attacks - Distribution by Phishing Page Title



Stealer Log Statistics
Top Domains Worldwide

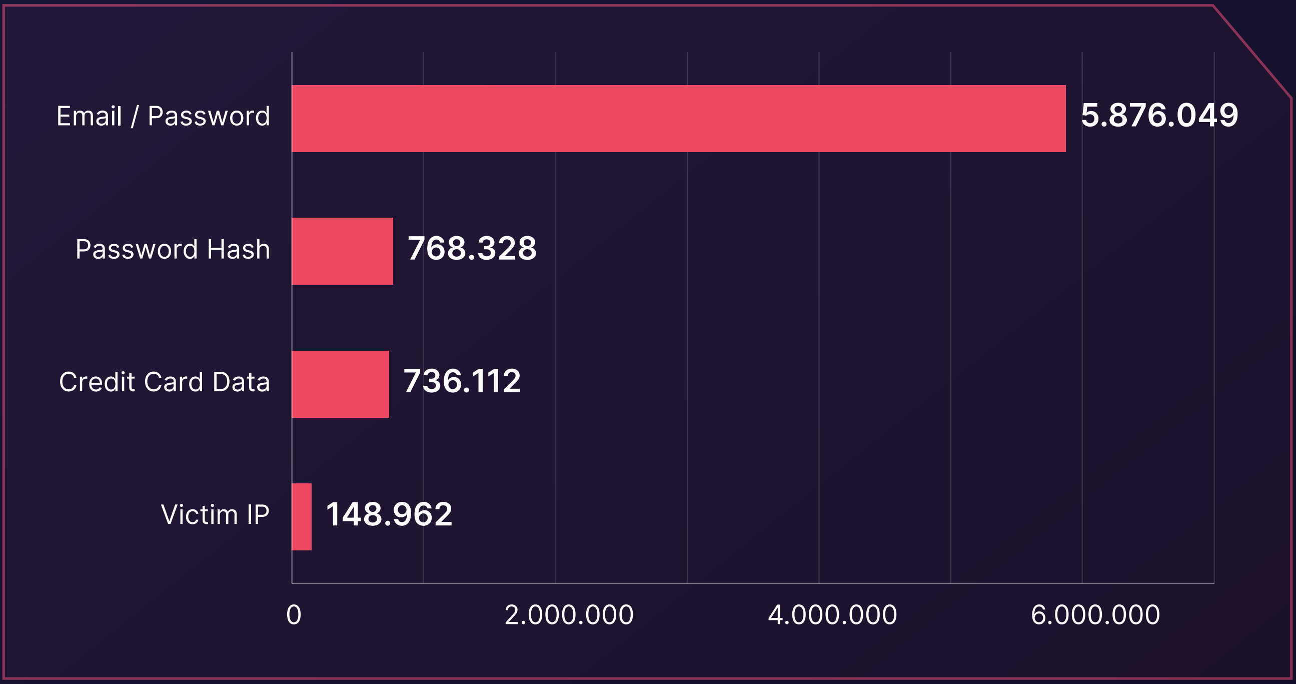
In 2024, Stealer Logs facilitated the compromise of thousands of user IDs, email addresses, passwords, credit card data, password hashes, and victim IPs, targeting accounts associated with some of the world's highest-traffic domains.

The table below lists the top 10 domains globally by traffic in 2024.

youtube.com
tiktok.com
instagram.com
facebook.com
amazon.com
x.com
reddit.com
canva.com
netflix.com
openai.com

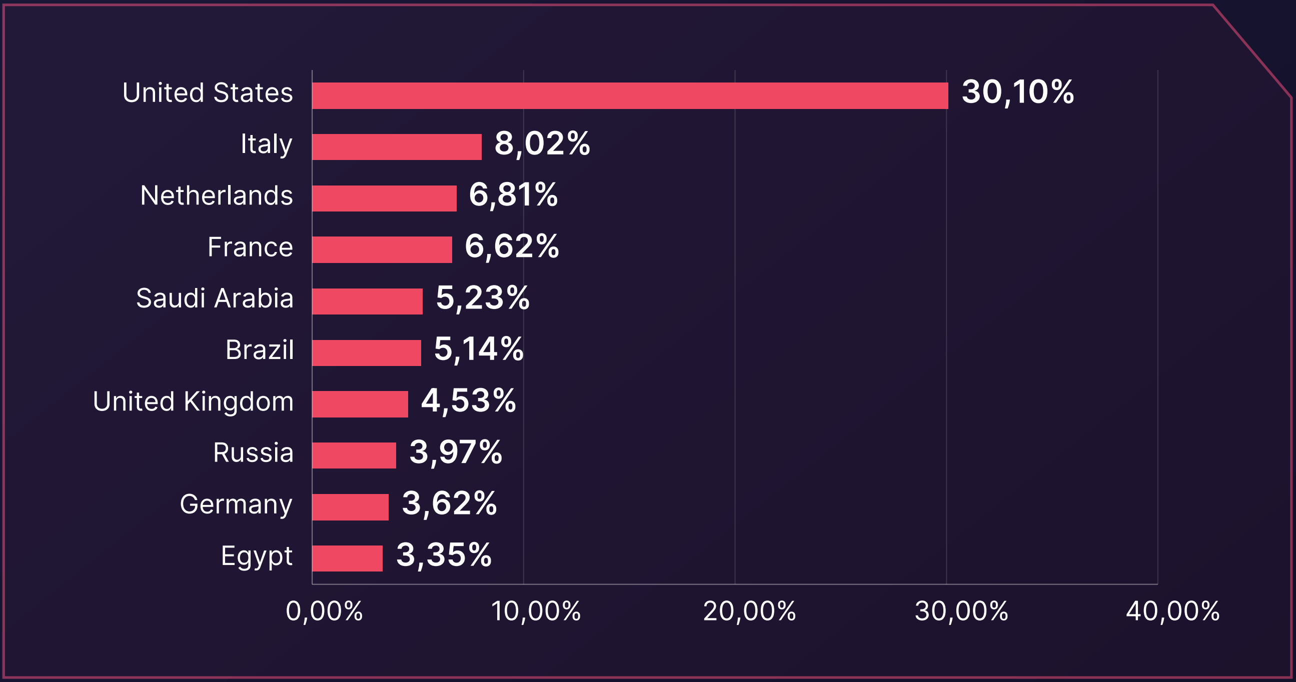
The graphs below display the distribution of compromised user data obtained through Stealer Logs across the domains with the highest traffic globally.

Stealer Logs - Compromised Data



> The data highlights an alarming volume of compromised information through Stealer Logs, including **5,876,049 email/password combinations, 768,328 password hashes, 736,112 credit card data entries, and 148,962 victim IPs**, showcasing the severity and scale of credential-based attacks in 2024.

Stealer Logs - Distribution by Country



Most stealer malware victims are from the United States, with 30.10% of the compromised credentials belonging to victims from this country. Italy ranks second, accounting for 8.02% of the exposed credentials, followed by the Netherlands at 6.81% and France at 6.62%.

These findings highlight the widespread impact of stealer logs globally and underscore the urgent need for enhanced cybersecurity measures to safeguard sensitive information effectively.

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.

Lessons Learned: Key Insights and Strategic Recommendations

An analysis of the global cybersecurity threats in 2024 reveals key lessons and actionable strategies to strengthen cyber resilience and protect operational integrity. Leveraging SOCRadar's advanced capabilities, these insights offer a comprehensive roadmap for organizations to proactively address emerging challenges and safeguard against evolving threats.

Vigilance in an Evolving Cyber Threat Landscape:

The dynamic nature of the cyber threat landscape, marked by an increase in dark web activities and ransomware incidents, demands constant vigilance. Organizations must keep pace with these changes by adapting their security strategies. By adopting a proactive approach like **SOCRadar's Extended Threat Intelligence** solution, organizations can gain real-time insights into emerging threats, positioning them to counteract cyber adversaries proactively.

Implementation of Multi-layered Security Measures:

Given the broad spectrum of industries targeted by cyber threats, it is essential to implement multi-layered security defenses. SOCRadar supports these efforts with its proactive **Threat Intelligence** and monitoring services, ensuring comprehensive protection.

Consistent Guard Against Ransomware:

The persistent ransomware threat underscores the need for strong defensive and responsive strategies. **SOCRadar's Attack Surface Management** capabilities are crucial for businesses to identify potential ransomware threats and to formulate effective countermeasures.

Continuous Employee Education and Training:

The ongoing risk of phishing attacks makes continuous employee education and training imperative. Enhancing their ability to recognize phishing tactics and detection methods is vital. SOCRadar's Digital Risk Protection suite provides comprehensive VIP Protection and Brand Protection services, effectively addressing the challenges posed by identity-based attacks.

Robust Defenses Against Stealer Malware:

Strengthening defenses against Stealer malware is crucial as it continues to be a significant threat. **SOCRadar's Identity & Access Intelligence** module is vital in detecting and mitigating data breach threats, enhancing an organization's security framework.

Strategies Against DDoS Attacks:

Organizations must prioritize implementing robust DDoS mitigation strategies as DDoS attacks become more complex and voluminous. This involves deploying advanced DDoS protection technologies that absorb high-volume traffic and effectively mitigate multi-vector attack strategies.

Enhance your DDoS defense with **SOCRadar's DoS Resilience module**, a sophisticated tool designed to assess and fortify your infrastructure's resilience to DoS attacks. Leveraging state-of-the-art AI and cloud technologies, this module provides a crucial layer of protection for global organizations.

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.

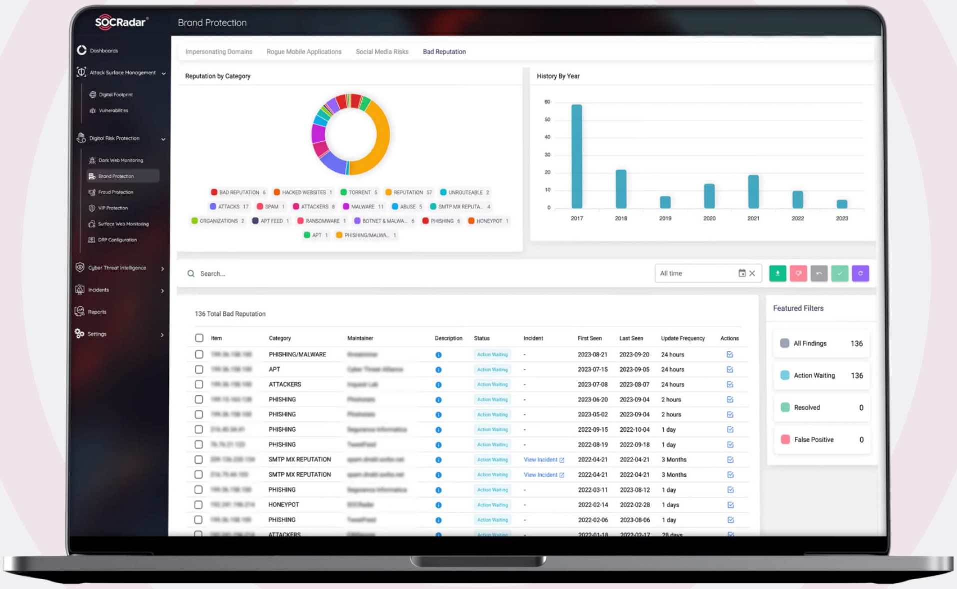
Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

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.



136 Total Bad Reputation

□	Item	Category	Maintainer	Description	Status	Incident	First Seen	Last Seen	Update Frequency	Actions
□	[illegible]	PHISHING/MALWARE	[illegible]	ℹ	Action Waiting	-	2023-08-21	2023-09-20	24 hours	☑
□	[illegible]	APT	[illegible]	ℹ	Action Waiting	-	2023-07-15	2023-09-05	24 hours	☑
□	[illegible]	ATTACKERS	[illegible]	ℹ	Action Waiting	-	2023-07-08	2023-08-07	24 hours	☑
□	[illegible]	PHISHING	[illegible]	ℹ	Action Waiting	-	2023-06-20	2023-09-04	2 hours	☑
□	[illegible]	PHISHING	[illegible]	ℹ	Action Waiting	-	2023-05-02	2023-09-04	2 hours	☑
□	[illegible]	PHISHING	[illegible]	ℹ	Action Waiting	-	2022-09-15	2022-10-04	1 day	☑
□	[illegible]	PHISHING	[illegible]	ℹ	Action Waiting	-	2022-08-19	2022-09-18	1 day	☑
□	[illegible]	SMTP MX REPUTATION	[illegible]	ℹ	Action Waiting	View Incident	2022-04-21	2022-04-21	3 Months	☑
□	[illegible]	SMTP MX REPUTATION	[illegible]	ℹ	Action Waiting	View Incident	2022-04-21	2022-04-21	3 Months	☑
□	[illegible]	PHISHING	[illegible]	ℹ	Action Waiting	-	2022-03-11	2023-08-12	1 day	☑
□	[illegible]	HONEYPOT	[illegible]	ℹ	Action Waiting	-	2022-02-14	2022-02-28	1 days	☑
□	[illegible]	PHISHING	[illegible]	ℹ	Action Waiting	-	2022-02-06	2023-08-06	1 day	☑
□	[illegible]	ATTACKERS	[illegible]	ℹ	Action Waiting	-	2022-01-18	2022-02-17	28 days	☑

Featured Filters	
All Findings	136
Action Waiting	136
Resolved	0
False Positive	0