SOCRadar®
Your Eyes Beyond

MID-YEAR CYBER SECURITY Review Report

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary

In the first half of 2024, the cyber threat landscape has been marked by escalating sophistication and frequency of attacks, presenting unprecedented challenges for cybersecurity professionals. SOCRadar's Extended Threat Intelligence (XTI) platform has been pivotal in empowering security operations centers (SOCs) with actionable, context-rich intelligence, transforming how threats are detected and mitigated.

The period witnessed a surge in ransomware attacks, with cybercriminals adopting more complex and stealthy tactics. These attacks have not spared any sector, targeting both small businesses and large corporations with equal ferocity. Notable incidents include the breaches at high-profile organizations, illustrating the relentless pursuit of cyber adversaries.

Integrated Attack Surface Management has become crucial in this hostile environment, providing enhanced visibility into vulnerabilities that could be exploited by attackers. Similarly, Brand Protection has shielded organizations from the growing threats emanating from the Dark Web, where stolen credentials and sensitive data are traded.

The role of Cyber Threat Intelligence has been paramount in this period, enabling SOC teams to anticipate and thwart potential attacks before they can cause significant damage. This proactive approach has been essential in maintaining the integrity and security of organizational networks.

Executive Summary

As we move forward, the reliance on artificial intelligence and machine learning in cybersecurity is set to increase. These technologies are proving indispensable in identifying and mitigating threats at speed and scale. The first half of 2024 has underscored the importance of a multi-faceted cybersecurity strategy that incorporates advanced threat intelligence, real-time monitoring, and rapid response capabilities.

Looking ahead, the cyber threat landscape shows no signs of abating. Ransomware will continue to be a dominant threat, with attackers constantly evolving their techniques. The Dark Web will remain a hotbed of illicit activities, necessitating continuous monitoring and vigilance. As organizations navigate these turbulent waters, the emphasis on robust, actionable threat intelligence will be more critical than ever.

In summary, the first half of 2024 has been a testament to the dynamic and challenging nature of cybersecurity. SOCRadar's XTI has been at the forefront, providing the tools and intelligence necessary to navigate these threats. As we anticipate the second half of the year, the commitment to enhancing cybersecurity measures and staying ahead of cyber adversaries remains unwavering.

Cybersecurity Predictions for 2024 Second Half

Surge in Ransomware Attacks:
Ransomware is expected to continue as a major threat, focusing on critical infrastructure and high-value targets. Attackers will likely use more sophisticated encryption methods and stealth tactics to evade detection and increase their impact.

AI-Driven Cyber Attacks:
The role of artificial intelligence and machine learning in cyber attacks will grow, leading to more effective and automated threats. This includes AI-enhanced phishing campaigns and advanced malware that can adapt to defenses in real-time.

Expansion of Cybercrime-as-a-Service (CaaS):
The underground market for cybercrime services will expand, providing advanced tools to a wider range of criminals. This will result in more frequent and varied attacks, enabling even less experienced attackers to carry out significant cyber operations.

Increase in Supply Chain Attacks:
Attackers will increasingly target supply chain vulnerabilities, focusing on third-party vendors to infiltrate larger networks. This strategy bypasses direct security measures and exploits weaker links in the supply chain, leading to widespread disruption.

Rise in Zero-Day Exploits:
The exploitation of zero-day vulnerabilities will become more common, with attackers taking advantage of unknown weaknesses before patches are available. This trend will cause significant disruptions and highlight the need for proactive vulnerability management.

Focus on Cloud Security:
As cloud adoption continues to rise, attacks on cloud infrastructure and services will become more complex. Organizations will need to implement specific security measures for the cloud, such as robust encryption and authentication protocols, to protect sensitive data and ensure compliance.

Enhanced Dark Web Activities: The Dark Web will remain a critical hub for illegal activities, including the sale of stolen data and hacking tools. Proactive monitoring and intelligence gathering on the Dark Web will be crucial for preempting threats.

Targeted Attacks on IoT Devices: The increase in Internet of Things (IoT) devices will create new vulnerabilities. Cybercriminals will exploit weaknesses in IoT devices to access broader networks, necessitating improved security measures for these devices.

SOCRADAR WITH NUMBERS

10.189 Users

300M+ IP Search

100B+ Port Search

1.644.567
Domains Discovered

- **1.459.036** IP Address
- **318.893** Web Sites
- **5.554.612** Ports
- **14.179** Login Pages
- **1.769** Rogue Mobile Apps
- **514.034** SSL Certificate

We Shared

824
Regional News

709
Threat Actors

5.764
Ransomware News

1M+ Contextualized Phishing Alarms

5.932.351 Generated Alarms	**64.488** Detected Credit Card
178.063 Detected Impersonating Accounts	**5.181.005** Discovered PII Exposures

4.349
Malware Analyzed

1.500
YARA and Sigma Rules

4.349
Unique IOC

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 ;

TOP DATA BREACHES IN THE FIRST HALF OF 2024

Snowflake Data Breach:
In January 2024, Snowflake experienced a significant data breach that exposed sensitive customer information. Attackers exploited a vulnerability to access and leak critical data, highlighting the ongoing risks even for highly secure cloud environments. You can visit our blog post for more information.

Mother of All Breaches (MOAB):
Also in January 2024, the "Mother of All Breaches" (MOAB) was reported, involving a massive data leak of 12 terabytes covering over 26 billion records from platforms such as LinkedIn, Twitter, and Dropbox. This breach underscored the severe implications of aggregated data breaches.

Bank of America Data Breach:
In February 2024, Bank of America revealed a data breach resulting from an attack on Infosys McCamish Systems. This breach exposed sensitive data such as names, social security numbers, and account details of 57,028 individuals, highlighting vulnerabilities within interconnected service ecosystems.

LoanDepot Ransomware Incident:
In January 2024, LoanDepot was hit by a ransomware attack that compromised the personal data of approximately 16.6 million customers, leading to significant service disruptions and underscoring the increasing threat posed by ransomware.

VARTA Data Breach:
On February 12, 2024, German battery manufacturer VARTA experienced a cyber attack that halted production across five plants. This breach affected IT systems and production equipment, showcasing the impact of cyber attacks on critical infrastructure.

Trello Data Breach:
In January 2024, a significant data breach at Trello affected over 15 million users. The breach, caused by a vulnerable API, exposed email addresses, names, and usernames, leading to the data being sold on hacking forums.

Planeta Data Breach:
In January 2024, Ukrainian hackers targeted the Russian Center for Space Hydrometeorology (Planeta), deleting 2 petabytes of critical data and affecting numerous state agencies, including the Ministry of Defense of the Russian Federation.

Tangerine Telecom Data Breach:
On February 18, 2024, Tangerine Telecom in Australia disclosed a breach where over 200,000 records were stolen. This breach was linked to compromised login credentials, potentially leading to phishing risks.

Cross Switch Data Breach:
In January 2024, Cross Switch, an online payment gateway management platform, faced a data breach compromising the personal data of 3.6 million users, including names, usernames, phone numbers, and banking details.

Spoutible Data Breach:
In January 2024, Spoutible, a social media platform, experienced a breach impacting 207,000 records. An API exploit exposed email addresses and bcrypt hashed passwords.

TOP CYBERSECURITY INCIDENTS IN THE FIRST HALF OF 2024

1.

Change Healthcare Ransomware Attack:

February 2024 saw Change Healthcare, a subsidiary of UnitedHealth, facing a significant ransomware attack. This attack disrupted healthcare payment processing across the U.S., costing over $872 million, with the ALPHV/BlackCat group responsible.

2.

Twitter Data Breach:

In January 2024, a massive data breach at Twitter exposed the personal information of 235 million users, raising serious privacy and security concerns.

3.

MGM Resorts Cyber Attack:

In February 2024, MGM Resorts suffered a cyber attack that led to the theft of personal data of 142 million guests, causing significant disruptions to their operations.

4.

Cencora Healthcare Data Breach:

In April 2024, Cencora faced a significant data breach that exposed sensitive patient information, affecting millions of records and underscoring the need for robust cybersecurity in healthcare.

5.

UK Ministry of Defence Payroll Hack:

In May 2024, the payroll system of the UK Ministry of Defence was hacked, exposing the personal data of nearly 270,000 current and former staff. The attack, attributed to Chinese hackers, raised significant national security concerns.

6.

French State DDoS Attack:

March 2024 experienced a coordinated DDoS attack on multiple French government services by Anonymous Sudan, disrupting over 300 web domains and 177,000 IP addresses, causing extensive service interruptions.

7.

NHS Scotland Ransomware Attack:

In March 2024, NHS Dumfries and Galloway in Scotland was targeted by the Inc Ransomware Group, which released sensitive patient and staff data on the dark web, significantly affecting public health services.

8.

El Salvador's Chivo Wallet Hack:

In April 2024, hackers targeted El Salvador's national cryptocurrency wallet, Chivo, exposing 144 GB of sensitive information and publicly releasing the source code, compromising personal data of millions of Salvadorians.

TOP VULNERABILITIES IN THE FIRST HALF OF 2024

In the first six months of 2024, a series of critical vulnerabilities were identified, posing significant risks to various platforms and technologies. These vulnerabilities underscore the need for timely patching and robust security measures to protect against potential exploits.

CVE-2024-3094
(XZ Utils SSH Backdoor Vulnerability):
A severe vulnerability in XZ Utils allowed attackers to establish an SSH backdoor in widely used Linux distributions. This issue highlighted the increasing threat to Linux-based systems, especially those used in server environments.

CVE-2024-21762
(FortiOS SSL VPN Vulnerability):
This critical out-of-bounds write vulnerability in FortiOS SSL VPN could lead to Remote Code Execution (RCE). The proof-of-concept (PoC) exploit was shared on a hacker forum, significantly increasing the risk of exploitation. This vulnerability emphasizes the necessity for immediate patching to safeguard network appliances.

CVE-2024-21626
(runc Container Escape Vulnerability):
This vulnerability in the runc container runtime enabled attackers to escape from a container and execute arbitrary code on the host system. It emphasized the security challenges associated with containerized environments and the necessity for stringent security practices in DevOps.

CVE-2024-27198
(TeamCity CI/CD Tool Vulnerability):
A critical flaw in the TeamCity continuous integration and deployment tool permitted unauthorized access to developer systems. Exploiting this vulnerability could allow attackers to inject malicious code into software development pipelines, posing a significant risk to software integrity.

CVE-2024-23897

(Jenkins CLI Command Processing Vulnerability):

A critical vulnerability in the Jenkins automation server's command line interface (CLI) allowed remote attackers to execute arbitrary commands on the server. Given the widespread use of Jenkins in software development workflows, this flaw presented a substantial risk to many organizations.

CVE-2024-49583

(Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability):

A critical buffer overflow vulnerability in Citrix's remote access products allowed attackers to execute arbitrary code. The increase in attacks exploiting this vulnerability highlighted the urgent need for securing remote access solutions.

CVE-2024-33006

(SAP NetWeaver File Upload Vulnerability):

This critical file upload vulnerability in SAP NetWeaver allowed unauthenticated attackers to upload malicious files to the server, potentially compromising the entire system. This flaw highlighted the need for robust security measures in enterprise software.

CVE-2024-3095

(Ivanti Connect Secure and Policy Secure Vulnerabilities):

Critical vulnerabilities in Ivanti's secure access solutions enabled attackers to bypass authentication and gain unauthorized access to sensitive systems. The extensive deployment of these solutions in enterprise environments made these vulnerabilities particularly concerning.

CVE-2024-29822 to CVE-2024-29827

(Ivanti Endpoint Manager SQL Injection Vulnerabilities):

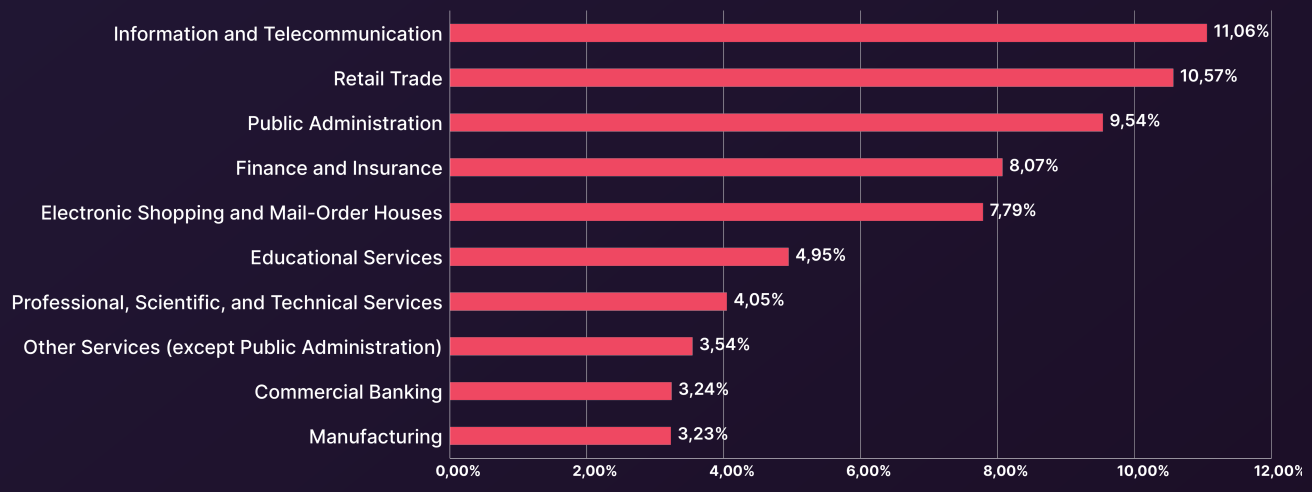
Multiple SQL injection vulnerabilities in Ivanti Endpoint Manager (EPM) could allow unauthenticated attackers to execute arbitrary code. These critical flaws underscored the importance of securing network management tools.

DARK WEB STATISTICS IN THE FIRST HALF OF 2024

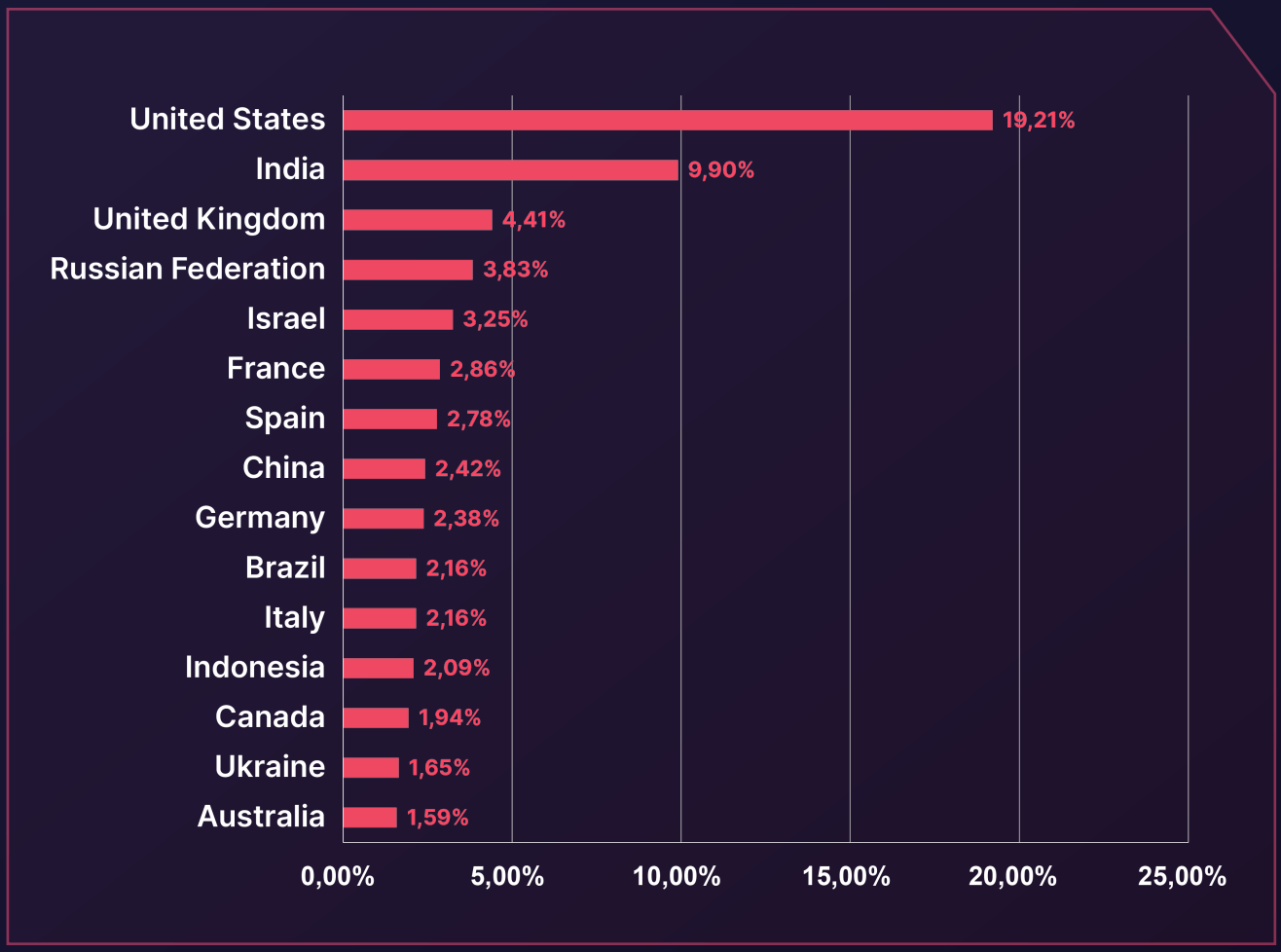
This section provides insights into the data gathered by SOCRadar during the first two quarters of 2024. This data was collected through the SOCRadar XTI Platform, which utilizes Machine Learning, Artificial Intelligence, and expert analysts to monitor threat actor activities across various sources, 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 6,419, with a daily average of 35.6 posts.

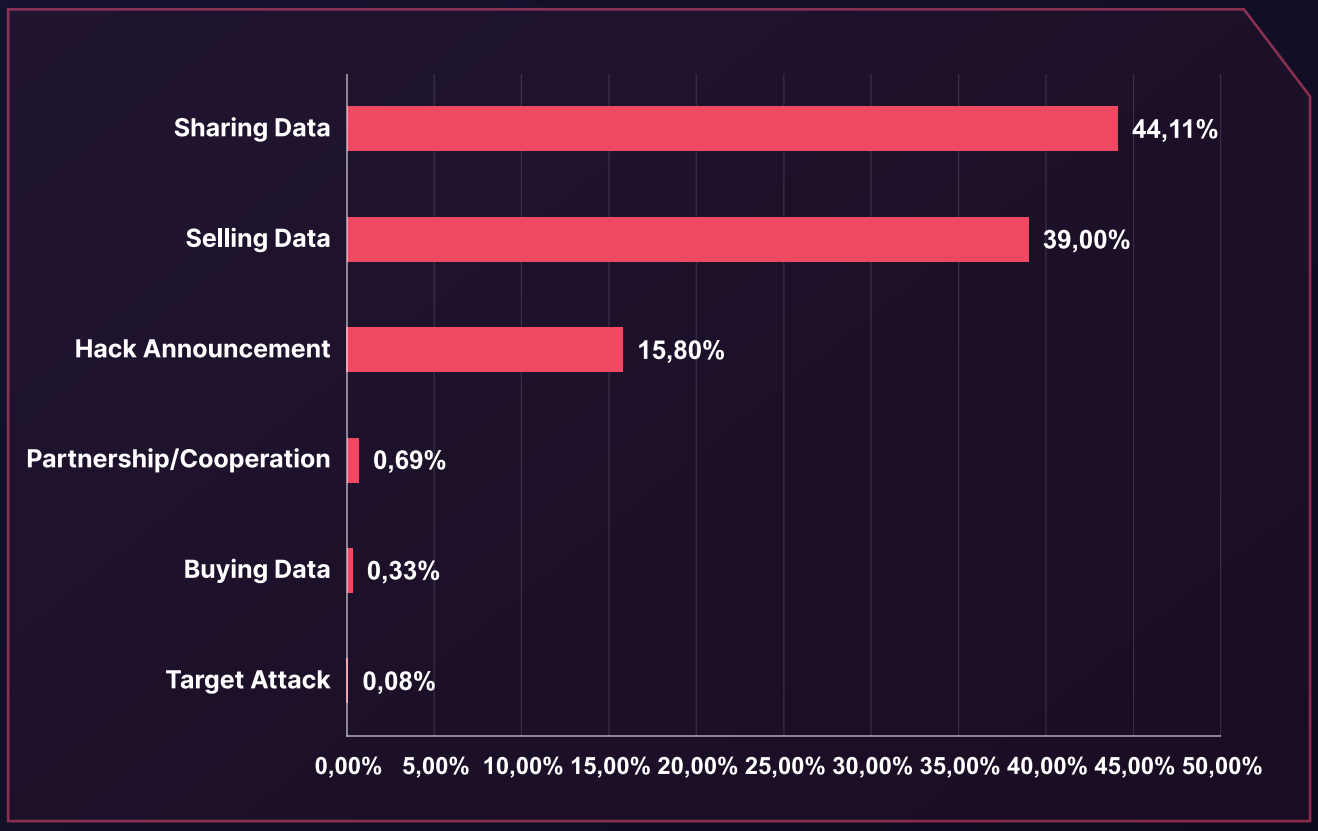
Dark Web Posts Industry Mention Analysis



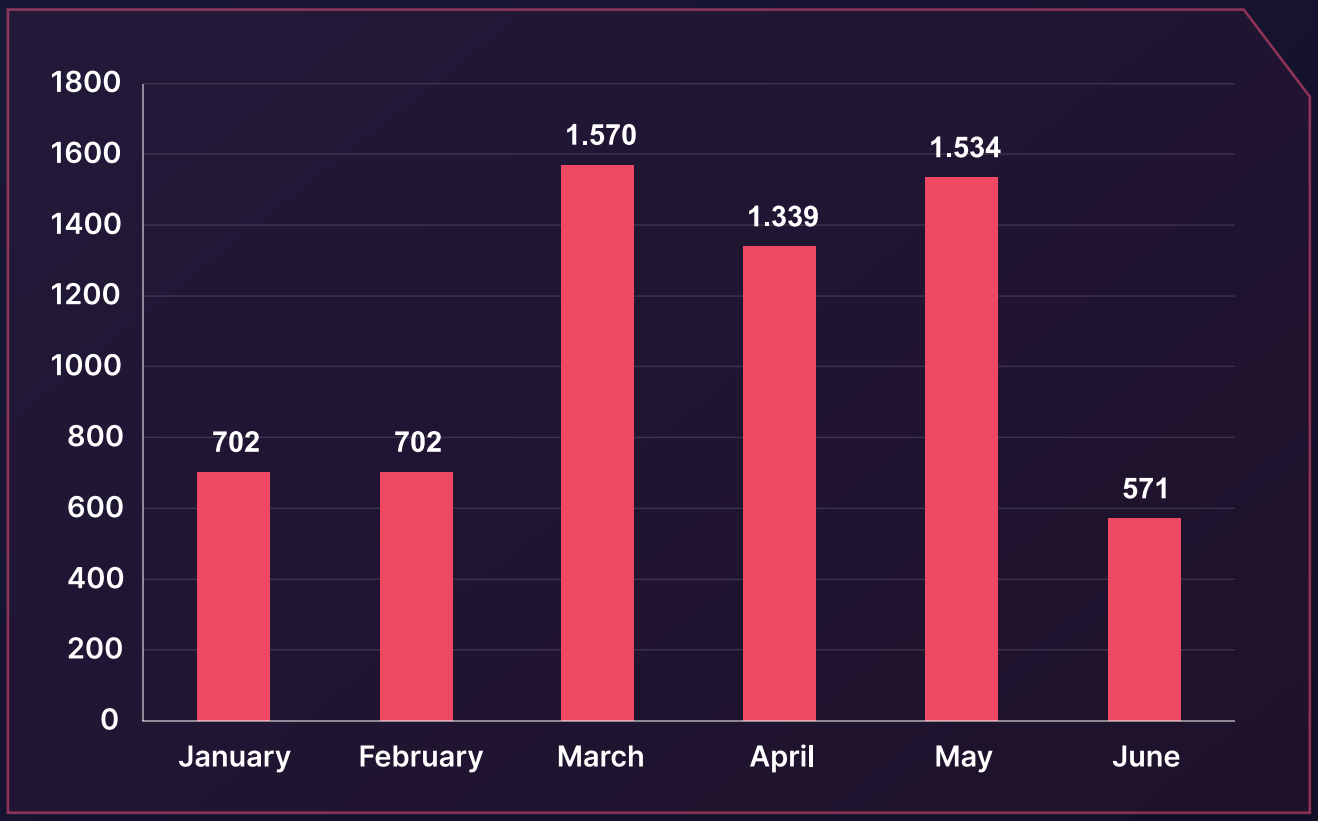
Dark Web Threats - Distribution by Target Country



Dark Web Post Subjects Analysis



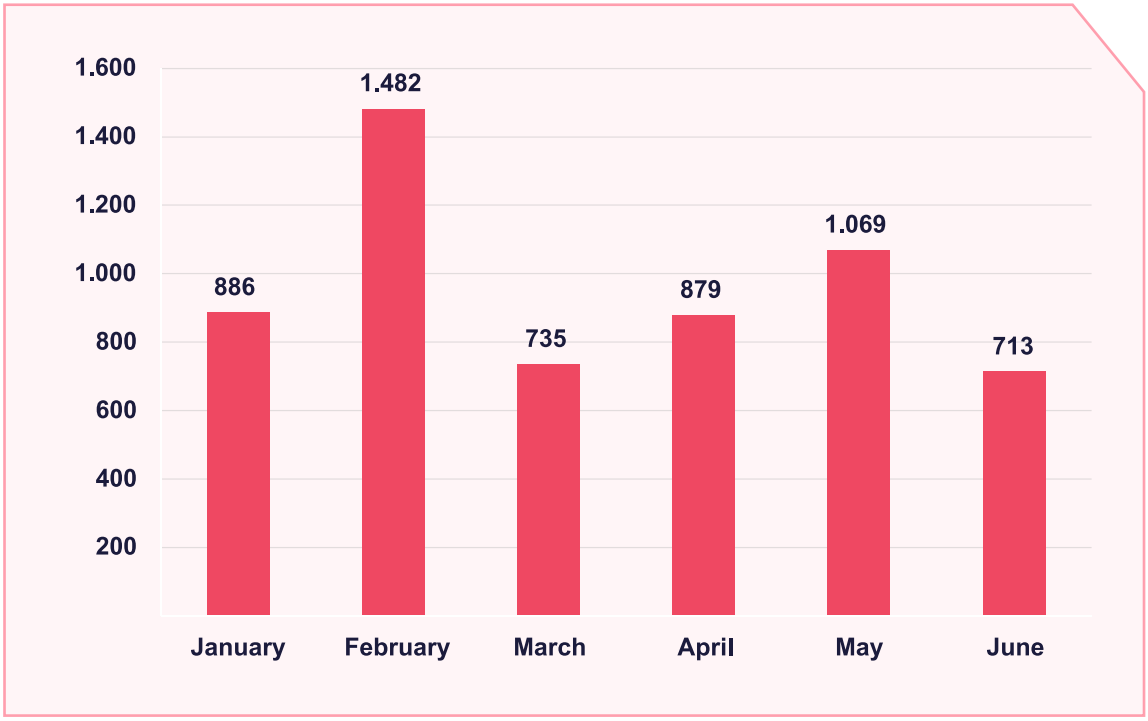
Monthly Dark Web Threat Trends



RANSOMWARE STATISTICS IN THE FIRST HALF OF 2024

The data is sourced from a comprehensive analysis conducted by SOCRadar analysts during the first half of 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 5,764 posts related to ransomware attacks, equating to an average of 960 posts per month or 32 posts per day.

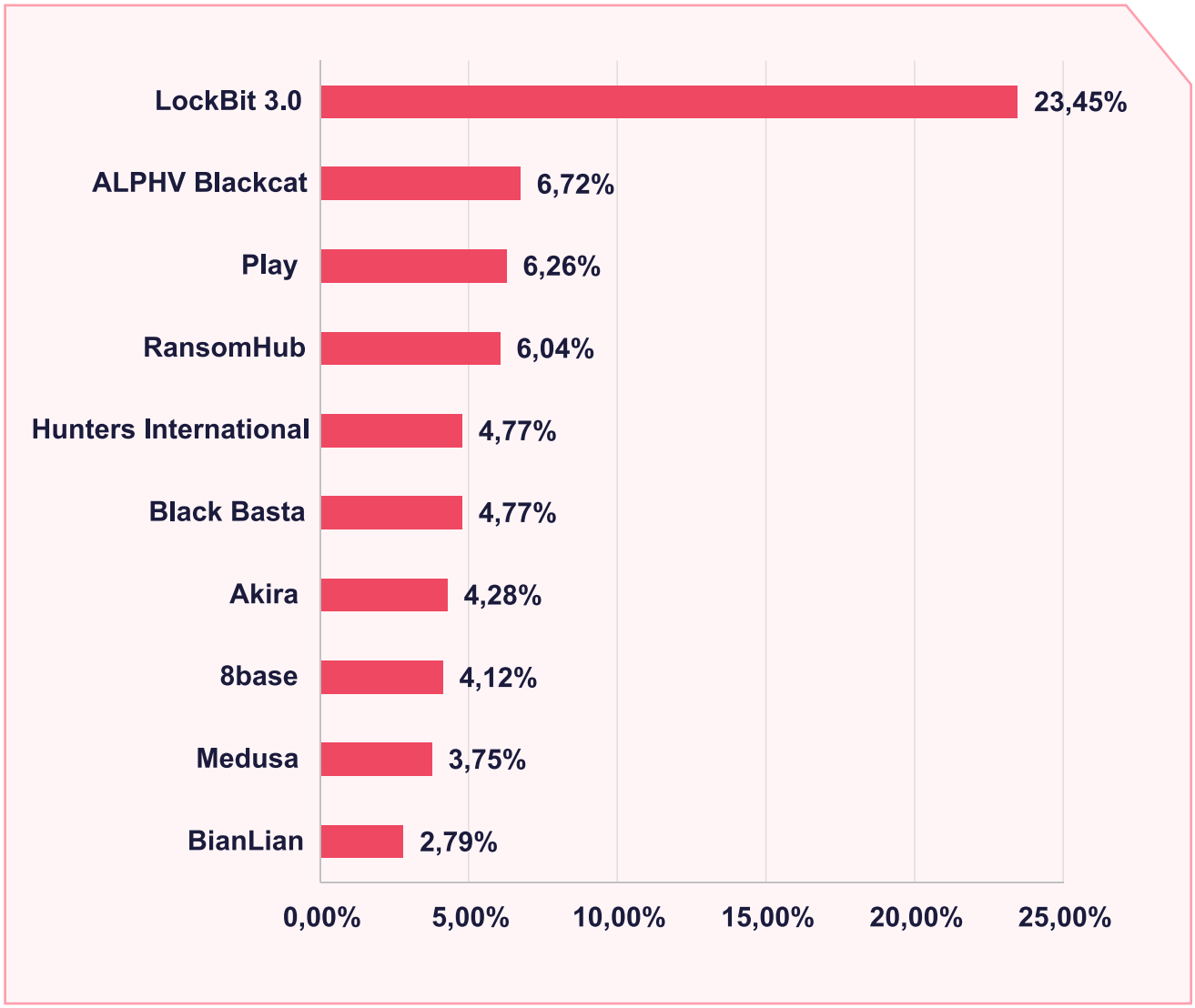
Monthly Analysis of Ransomware Activity



Monthly distribution of ransomware-related posts published on the SOCRadar Platform throughout the first half of 2024.

> The graph above shows a notable fluctuation in activity, with a distinct peak in February.

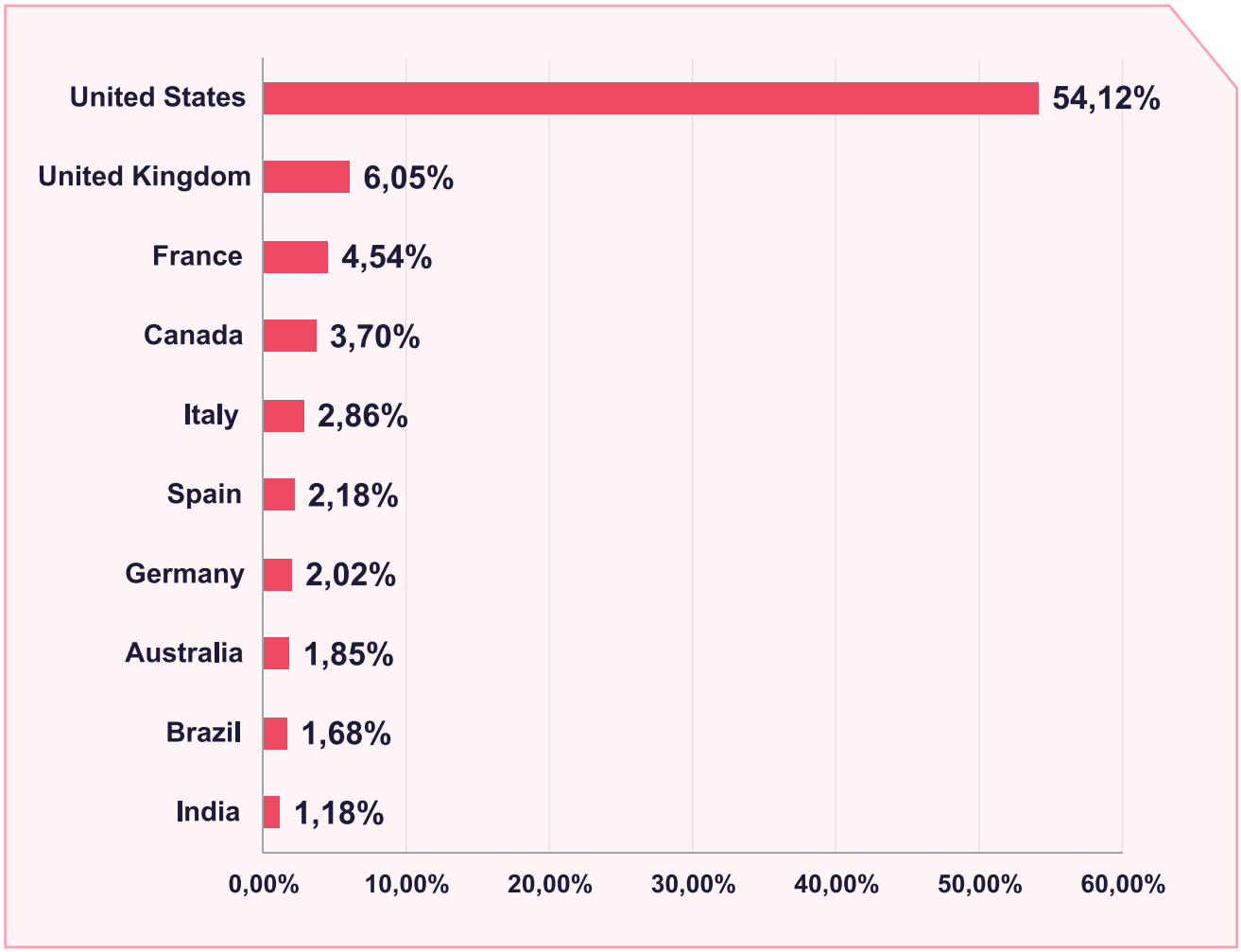
Ransomware Group Activity Analysis



An overview of the activities of the Top 10 ransomware groups as recorded on the SOCRadars Platform, highlighting contributions from 127 different groups.

> LockBit 3.0 leads with 23.45% of the posts, followed by ALPHV Blackcat and Play groups. The graph visually represents the proportion of posts related to each group, offering a clear perspective on the dominance and prevalence of these cyber threat entities in the digital landscape.

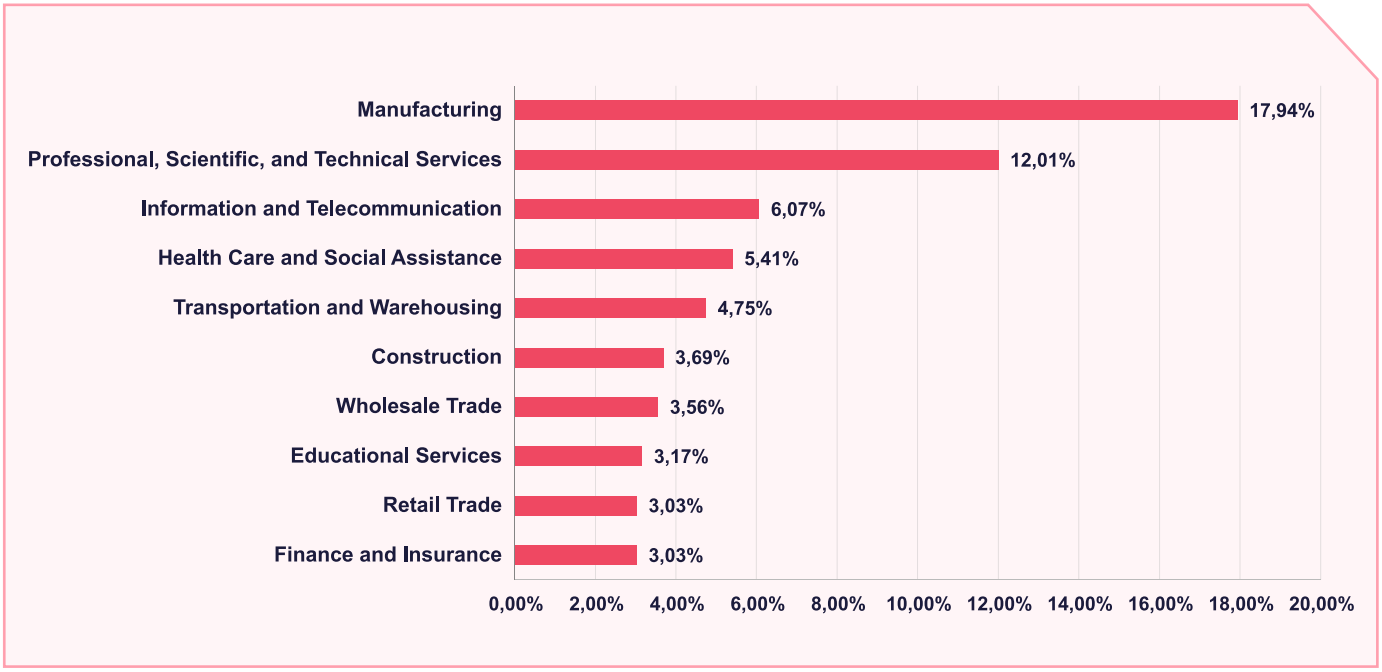
Geographical Analysis of Ransomware Attacks



Distribution of ransomware-related posts about organizations across the top 10 countries, as mentioned on the SOCRadars Platform.

This table showcases the distribution of ransomware-related posts about organizations across the top 10 countries, as mentioned on the SOCRadars Platform. The United States leads significantly with 54.12% of the mentions, followed by the United Kingdom and France. This data reflects the geographic focus of ransomware threats and the countries where organizations are most frequently discussed in the context of these cyber risks.

Ransomware Attacks - Distribution by Industries



Top 10 industries targeted in ransomware-related posts on the SOCRadars Platform.

> This graph presents the top 10 industries targeted in ransomware-related posts on the SOCRadars Platform. The manufacturing industry leads the chart, accounting for 17.94% of the posts, followed by sectors like Professional, Scientific, and Technical Services, and Information and Telecommunication.

MOST DANGEROUS THREAT ACTORS IN 2024 FIRST HALF

Hunters International

Country of Origin: Unkno

Hunters Internation
following the disrup
Hive ransomware gr
enforcement in Q3
Showing substantial
similarities, it ap
a successor or of
Hive.

Medusa Ransomware

known

RaaS group
June 2021 and
any variants.
primarily
American and
nizations.

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.

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

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

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

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

Country of Origin: Russia

Black Basta is a ransomware group that has been active since April 2022 and they employ a double-extortion attack technique. The group was also observed to be linked to the FIN7(Carbanak).

-Ransomware Group-

Motivation: Financial Gain

Target Countries: North America and Europe

Target Sectors: Manufacturing, Construction, Professional Services, Finance, Healthcare

Attack Type: Valid Credentials, RaaS, Ransomware, Double-extortion

-TTPs-

Valid accounts: T1078

Phishing: Spear-phishing attachment: T1566.001

Exfiltration over C2 channel: T1041

Country of Origin: Unknown

8Base is a ransomware group active since April 2022, targeting small and medium-sized businesses (SMBs) across various sectors, including business services, finance, manufacturing, and IT.

-Ransomware Group-

Motivation: Financial Gain

Target Countries: United States, Brazil, UK, Australia, Germany, Canada, Spain, Italy, Belgium

Target Sectors: Professional Services, Manufacturing, Construction, Finance, Healthcare, Transportation

Attack Type: RaaS, Ransomware, Double Extortion

-TTPs-

Phishing: Spearphishing Attachment: T1566.001

OS Credential Dumping: T1003

Exfiltration Over C2 Channel: T1041

-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

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Canada, India, Australia, Europe
Target Sectors:	Financial Institutions, Law, Government, Professional Services, Manufacturing, Media & Entertainment, Education
Attack Type:	Spearphishing, Data Exfiltration, Ransomware, Double-extortion

-TTPs-

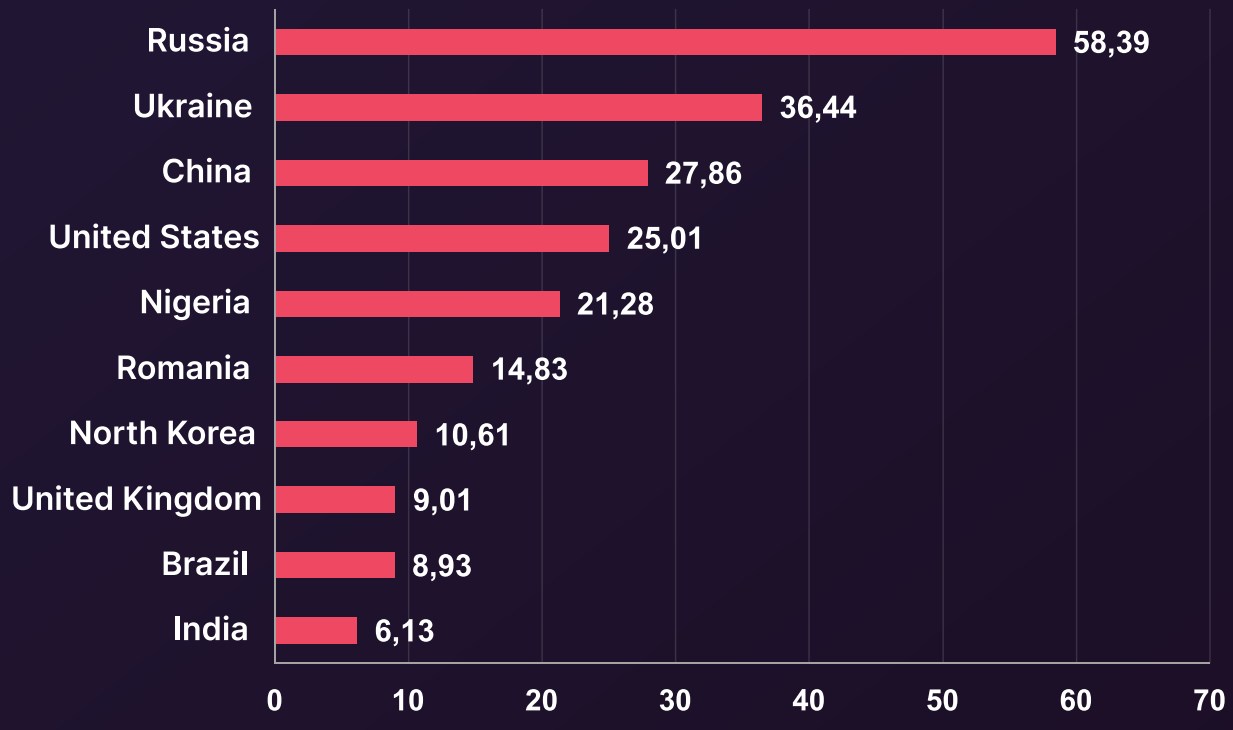
Remote Desktop Protocol:	T1021.001
Data Encrypted for Impact:	T1486
Exfiltration to Cloud Storage:	T1586.002

2024 GLOBAL CYBERCRIME INDEX RANKINGS

Cyber attacks originate from some of the world's most powerful nations, not just targeting them. Data breaches and denial of service attacks are frequently launched from these countries.

Recent research (2024) by Oxford University has resulted in the development of a Cybercrime Index, which utilizes the World Cybercrime Index (WCI) score. This index, represented in the graph below, reflects the threat levels based on expert analysis from cybercrime specialists.

Global Cybercrime Index Ranking by WCI Scores



(The WCI score quantifies the threat level according to research by cybercrime experts.)

> Although it is challenging to draw direct correlations from these figures, the data reveals that Russia stands out as the foremost cybersecurity threat.

Lessons Learned: Key Insights and Strategic Recommendations

Upon examining the cybersecurity threats facing organizations globally in the first half of 2024, several critical lessons and recommendations have emerged. These insights, enhanced by SOCRadar's capabilities, provide a strategic roadmap to bolster cyber resilience and safeguard operational integrity. Here are the key takeaways from our analysis:

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:

As DDoS attacks become more complex and voluminous, organizations must prioritize implementing robust DDoS mitigation strategies. This involves deploying advanced DDoS protection technologies that can 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.

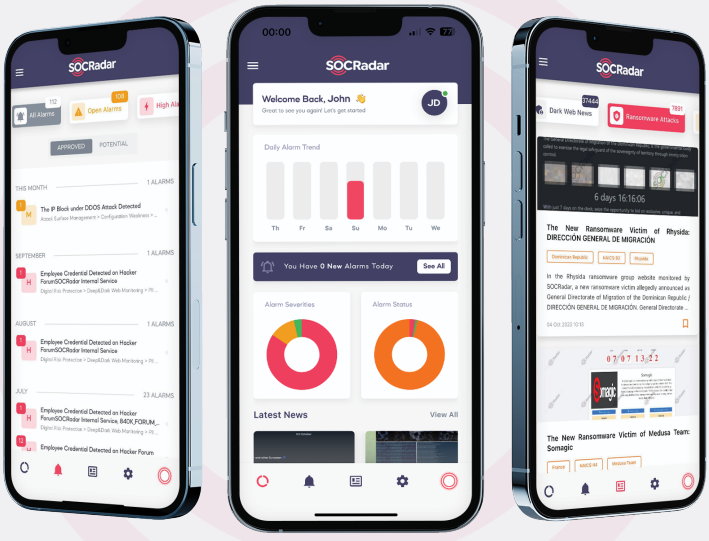
GET ACCESS FOR FREE

MEET THE NEW MOBILE APP

Access threat intelligence, act on-the-go, and be instantly notified of new threats.View alerts, breaking Dark Web news, and new ransomware attacks

Download on the App Store

GET IT ON Google Play



Gartner Peer Insights™ 4.8/5

SOCRadar®
Your Eyes Beyond

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

Call
+1 (571) 249-4598

Email
info@socradar.io

socradar.io

Virtual Addresses

London, UK
167 City Road Old Street, London EC1V 1AW

Dubai, UAE
8W building 5th Floor, DAFZA, Dubai

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

Bangalore, India
The Estate, 8th Floor Dickenson Road 560042 Bangalore Karnataka