End of The Year
2025 Report

SOCRadar®
Your Eyes Beyond

socradar.io

Executive Summary

2025 revealed a troubling evolution in how cybercriminals operate. Credential theft became industrialized and became the primary gateway for more damaging attacks.

What Changed This Year

- 388 million stolen credentials across just the top ten platforms is a huge number and it represents a fundamental shift in threat actors' strategy. Cybercriminals are no longer breaking down doors; they're stealing keys at scale. Facebook alone saw 93 million credentials compromised, while gaming platforms like Roblox became a goldmine for attackers.
- The dark web has become an efficient marketplace. Nearly 60% of activity now centers on selling access and data, while sharing dropped to 33%. What's particularly concerning is that Public Administration led all sectors in dark web discussions at 13%, suggesting government entities are being actively targeted and traded.

The Geographic Divide

- We're seeing two distinct threat landscapes emerge. Developing nations like India, Brazil, and Indonesia are drowning in credential theft. This is likely due to rapid digital adoption without corresponding security awareness. Meanwhile, ransomware groups are laser-focused on wealthy English-speaking countries. The US absorbed 41% of all ransomware attacks, with the UK taking another 18%.

What This Means

- The connection between these trends is what should concern us most. Those millions of stolen credentials are enabling account takeovers as well as providing initial access for ransomware operations. Attackers are using cheap, stolen credentials to breach high-value targets.
- The fragmentation among ransomware groups suggests a mature, competitive criminal ecosystem rather than dominance by any single threat actor which makes it harder to track all the possible threats targeting your industry or country.
- Organizations can no longer treat credential compromise as a password reset issue. Every stolen credential is a potential backdoor into your network, and the attackers know how to monetize that access.

Top Takeaways

Dark Web Threat Landscape:

Public Administration and technology sectors face the highest dark web exposure, with stolen data and database compromises representing nearly two-thirds of all threats.

The US dominates dark web discussions at 20%, while selling activities (59%) far exceed other threat categories, indicating a mature commercial cybercrime marketplace.

Ransomware Threats:

The ransomware threat distribution is highly concentrated, with the United States and the United Kingdom accounting for nearly 60 percent of all cases. The remaining countries show a steep drop-off, indicating limited activity or lower visibility outside a small set of highly digitalized markets.

Phishing Threats:

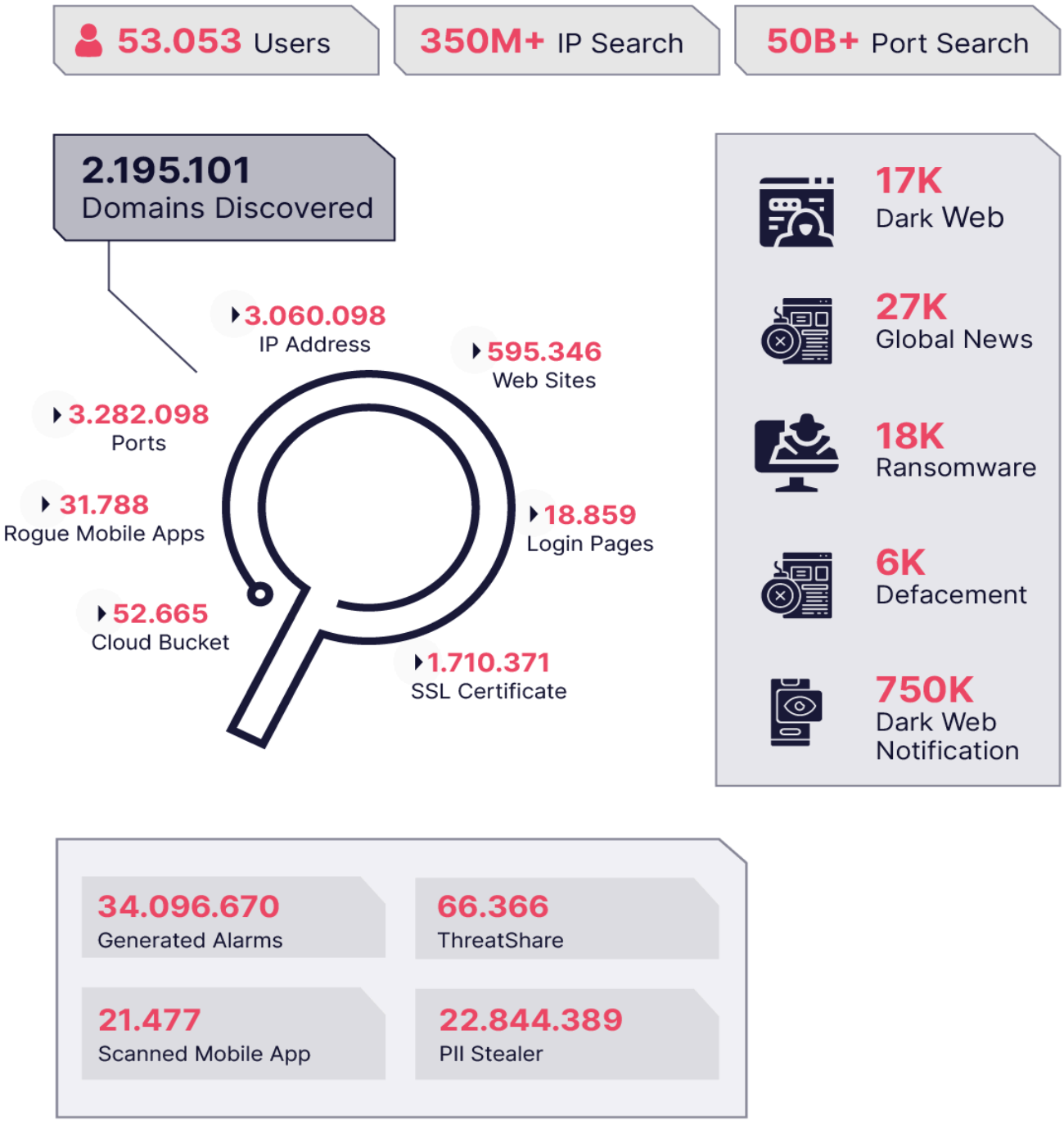
Over 72% of phishing sites now use HTTPS encryption, effectively weaponizing the traditional "look for the padlock" security advice that users have been taught.

Financial services and cryptocurrency platforms collectively represent over 31% of phishing targets, reflecting direct monetary motivations behind these campaigns.

Stealer Logs:
Stealer log data shows a clear concentration around globally used consumer platforms and large user populations. High-volume domains such as Facebook, Google, Instagram, and major gaming services dominate the exposed credentials.

When we look at the infections, we see that they are most prevalent in countries with large and active internet user bases, led by India, Brazil, and Southeast Asia. This indicates widespread, non-targeted stealer distribution with a focus on services that provide broad account access and downstream monetization opportunities.

SOCRadar with Numbers

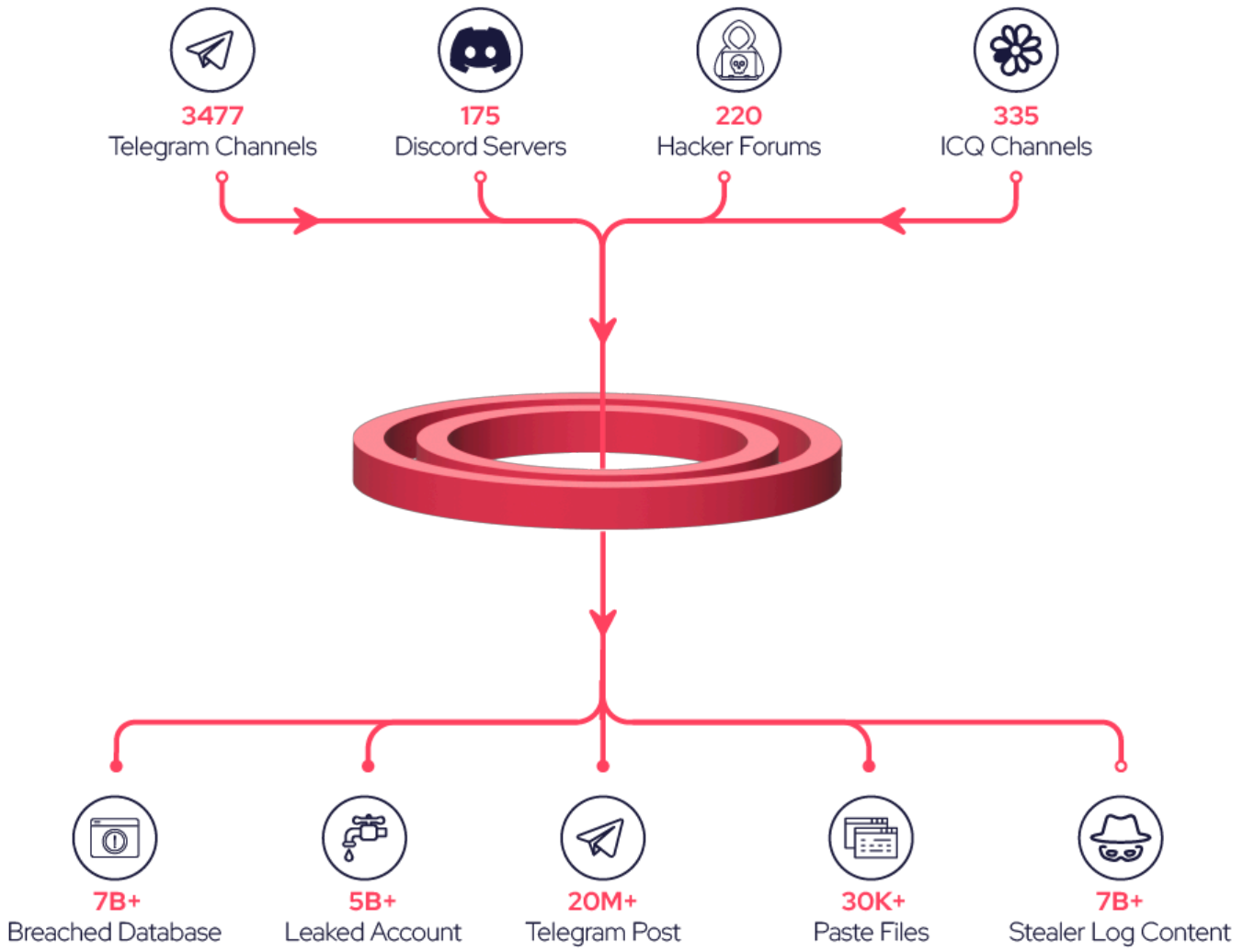


Dark Web with Numbers

See behind the shadows:

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

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



Top Data Breaches of 2025

SK Telecom SIM authentication data breach

SK Telecom, South Korea's largest mobile carrier, confirmed a major cyber attack that exposed sensitive USIM card data belonging to its entire customer base (reportedly over 23 million users). Detected on April 19, the breach raised widespread concerns over SIM swapping, a tactic where threat actors use stolen SIM data to hijack phone numbers and intercept communications.

Yale New Haven Health data breach

Yale New Haven Health, Connecticut's largest healthcare system, confirmed a data breach affecting more than 5.5 million individuals following a cyber attack in March 2025. The attackers gained access to personally identifiable information (PII) and healthcare-related data from patients across the provider's network.

Oracle Confirmed Legacy Server Breach

Oracle privately confirmed to customers that threat actors breached a legacy environment, known as Oracle Cloud Classic, exfiltrating old client credentials including usernames, hashed passwords, and email addresses. The breach reportedly began in January 2025 using a 2020 Java exploit to deploy malware and access Oracle Identity Manager data. The breach was detected in late February.

Royal Mail Group Breach Leaked 144GB of Internal Data

In March 2025, a hacker known as GHNA leaked 144GB of data allegedly stolen from Royal Mail Group, including internal communications, delivery route data, customer PII, and marketing lists. The leak featured Zoom recordings and backend files, much of it linked to Spectos, a third-party analytics vendor. Royal Mail acknowledged the incident was under investigation with Spectos.

Hertz Corporation Data Breach

Hertz Corporation has disclosed a data breach affecting customers of its Hertz, Thrifty, and Dollar brands after attackers exploited zero-day vulnerabilities in the Cleo integration platform during incidents in October and December 2024. The company confirmed the breach on February 10, 2025, stating that exposed data may include names, contact details, dates of birth, credit card and driver's license information, workers' compensation records, and in some cases Social Security or passport numbers.

Allianz Life Data Breach

On July 16, 2025, Allianz Life disclosed a data breach stemming from a supply chain compromise involving its cloud-based Customer Relationship Management (CRM) system. Threat actors employed social engineering to impersonate IT helpdesk staff, persuading Allianz employees to grant access to the Salesforce Data Loader tool. This utility allowed bulk extraction of sensitive records from the platform, which Allianz uses to manage customer, financial professional, and employee information.

Marks & Spencer ransomware

Marks & Spencer confirmed that its April 17, 2025, network breach originated from a sophisticated impersonation attack against a third-party service provider. Threat actors posed as a legitimate associate to convince help desk staff to reset an employee's password, granting them access to M&S systems. The attack, involving IT outsourcing partner Tata Consultancy Services, has been attributed to actors linked to the Scattered Spider group, who deployed the DragonForce ransomware.

Salesforce Data Breach

In mid-2025, a series of coordinated intrusions targeted the Salesforce environments of multiple high-profile companies across diverse sectors, including Technology, Retail, Luxury Fashion, Aviation, and Insurance. In one high-profile ransom message, the threat actors claimed the campaign had compromised data from 91 organizations worldwide. Victims included Adidas, Cartier, Google, Louis Vuitton, Dior, Chanel, Tiffany & Co., Qantas Airways, Air France–KLM, Allianz Life, Cisco, Pandora, and others. The campaign, attributed to a financially motivated group tracked by Google as UNC6040 and often linked to the ShinyHunters name, relied entirely on social engineering rather than exploiting any flaw in Salesforce's infrastructure.

Coinbase Breach Tied to Insider Abuse at TaskUs India Office

Coinbase disclosed in a May 2025 SEC filing that a customer data breach may cost up to $400 million, with new reporting linking part of the incident to insider activity at outsourcing partner TaskUs. According to multiple former TaskUs employees, the breach traces back to January 2025, when an India-based support agent in Indore was caught photographing customer data from her workstation using a personal phone. The employee, along with an alleged accomplice, reportedly leaked Coinbase customer data in exchange for bribes.

Samsung Data Leak

A major data leak has exposed about 270,000 customer support records linked to Samsung Germany after a threat actor exploited long-compromised credentials belonging to a third-party vendor. The attacker, identified as "GHNA," used login details stolen in 2021 through the Racoon infostealer from an employee at Spectos GmbH, a service quality provider for Samsung, which were never rotated. This allowed access to Samsung systems in 2025 and led to the public release of the data, which includes customer names, email addresses, physical addresses, order and tracking information, and customer support communications.

Top 10 Cybersecurity Incidents of 2025

Cloudflare Blocks Record 7.3 Tbps DDoS Attack on Hosting Provider

Cloudflare said it automatically mitigated the largest distributed denial-of-service attack ever recorded, blocking traffic that peaked at 7.3 terabits per second. The attack, detected in mid-May 2025, targeted an unnamed hosting provider and delivered 37.4 terabytes of data in just 45 seconds. Cloudflare said the incident highlights a growing trend of large-scale DDoS attacks aimed at hosting providers and core internet infrastructure, which remain attractive targets due to their central role in online services.

Jaguar Land Rover (JLR)

The automaker Jaguar Land Rover (JLR), owned by India's Tata Motors, confirmed that it was forced to shut down its IT systems after detecting a serious incident that has "severely disrupted" its retail and production operations. JLR stressed there was no evidence that customer data had been compromised but admitted the disruption was significant in a statement. The breach comes amid a surge of sophisticated attacks targeting major UK brands.

CodeRED's Emergency Alert System Targeted by the INC Ransom Group

A cyber incident disrupted CodeRED, an emergency alert system used by local governments to send time-sensitive notifications for severe weather, evacuations, missing persons, and other critical events. The outage was reportedly caused by a ransomware attack claimed by the INC Ransom group, which published screenshots that appear to show stolen customer data, including email addresses and clear-text passwords. In response, Crisis24 shut down the platform's legacy environment and rebuilt CodeRED within a new, isolated infrastructure to contain the incident and restore services.

First Reported AI-orchestrated Cyber Espionage Campaign

In mid-September 2025, Anthropic detected a cyber espionage operation and assessed with high confidence that it was conducted by a Chinese state-sponsored group designated GTG-1002. The investigation identified a well-funded and professionally coordinated campaign, targeting about 30 organizations, with several confirmed compromises. The operation showed deep and sustained use of AI across the full attack lifecycle, including reconnaissance, vulnerability discovery, exploitation, lateral movement, credential harvesting, data analysis, and data exfiltration. It was assessed that AI systems executed roughly 80 to 90 percent of tactical actions without direct human input, operating at task execution rates that exceed human capability.

Cl0p's Oracle EBS Zero-Day Campaign

The Cl0p ransomware group has returned to the spotlight with a new wave of attacks that target Oracle EBS (E-Business Suite) zero-day vulnerabilities. The threat group has a long history of abusing high impact flaws in major enterprise and file transfer systems. Cl0p is running a large extortion campaign that abuses Oracle E-Business Suite zero-day flaws. The group uses these vulnerabilities to access systems, steal files, and push victims into ransom talks. So far, they have listed a wide range of global companies and published many stolen datasets through torrent and magnet links.

Massive npm Supply Chain Attack Exposes Millions to Crypto-Stealing Malware

Researchers issued a warning about a major npm supply chain attack that has disrupted the JavaScript ecosystem. Attackers compromised widely used packages such as chalk, debug, and ansi-styles, injecting malware designed to hijack cryptocurrency transactions.

React2Shell: Critical RCE in React and Next.js Explained

A Remote Code Execution (RCE) vulnerability, widely referred to as React2Shell, has been identified in the React Server Components (RSC) ecosystem used by React 19 and frameworks such as Next.js. The issue involves critical flaws now tracked as CVE-2025-55182 and CVE-2025-66478.

Upbit Cryptocurrency Heist

A cyberattack on South Korea's largest cryptocurrency exchange, Upbit, was allegedly carried out by North Korea's state-backed Lazarus hacking group, according to South Korean officials. About $30 million in cryptocurrency was stolen after attackers reportedly impersonated Upbit administrators and transferred the funds to external wallets. Authorities said the tactics and laundering methods match previous Lazarus operations, including a 2019 Upbit theft of about $40 million, and noted that some stolen funds have already been traced and efforts are underway to freeze them.

BRICKSTORM Malware Campaign

BRICKSTORM is a sophisticated backdoor targeting VMware vSphere and Windows environments and has been observed mainly in the government services, facilities, and information technology sectors. CISA said the malware enables stealthy persistence and secure command and control, with capabilities that support initial access, continued presence, and lateral movement.

Attackers Exploit 'ToolShell' Vulnerabilities in On-Premises SharePoint Servers

Microsoft warned in late July 2025 that attackers were actively exploiting vulnerabilities in on-premises SharePoint servers in campaigns affecting sectors such as government and healthcare. The attacks targeted internet-facing deployments and chained two flaws, CVE-2025-53770 and CVE-2025-53771, rated critical and high severity. The combined exploitation technique was labeled as ToolShell.

Most Exploited Vulnerabilities of 2025

In 2025, several vulnerabilities have been notably exploited, posing significant risks to organizations and systems. Here are some of the most exploited vulnerabilities identified this year, along with their CVSS scores:

CVE-2025-53770
CVSS Score: **9.8**

Details: Deserialization of untrusted data in on-premises Microsoft SharePoint Server allows an unauthorized attacker to execute code over a network.

CVE-2025-55182
CVSS Score: **10**

Details: A pre-authentication remote code execution vulnerability exists in React Server Components versions 19.0.0, 19.1.0, 19.1.1, and 19.2.0 including the following packages: react-server-dom-parcel, react-server-dom-turbopack, and react-server-dom-webpack. The vulnerable code unsafely deserializes payloads from HTTP requests to Server Function endpoints.

CVE-2025-64446
CVSS Score: **9.8**

Details: A relative path traversal vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.1, FortiWeb 7.6.0 through 7.6.4, FortiWeb 7.4.0 through 7.4.9, FortiWeb 7.2.0 through 7.2.11, FortiWeb 7.0.0 through 7.0.11 may allow an attacker to execute administrative commands on the system via crafted HTTP or HTTPS requests.

CVE-2025-49844
CVSS Score: **9.9**

Details: Redis 8.2.1 and below allow an authenticated user to use a specially crafted Lua script to manipulate the garbage collector, trigger a use-after-free and potentially lead to remote code execution. The problem exists in all versions of Redis with Lua scripting. This issue is fixed in version 8.2.2.

CVE-2025-32433
CVSS Score: **10**

Details: Erlang/OTP is a set of libraries for the Erlang programming language. Prior to versions OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20, a SSH server may allow an attacker to perform unauthenticated remote code execution (RCE). By exploiting a flaw in SSH protocol message handling, a malicious actor could gain unauthorized access to affected systems and execute arbitrary commands without valid credentials.

CVE-2025-24893
CVSS Score: **9.8**

Details: XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any guest can perform arbitrary remote code execution through a request to `SolrSearch`. This impacts the confidentiality, integrity and availability of the whole XWiki installation.

CVE-2025-1974
CVSS Score: **9.8**

Details: A security issue was discovered in Kubernetes where under certain conditions, an unauthenticated attacker with access to the pod network can achieve arbitrary code execution in the context of the ingress-nginx controller. This can lead to disclosure of Secrets accessible to the controller.

CVE-2025-25257
CVSS Score: **9.8**

Details: An improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability [CWE-89] in Fortinet FortiWeb version 7.6.0 through 7.6.3, 7.4.0 through 7.4.7, 7.2.0 through 7.2.10 and below 7.0.10 allows an unauthenticated attacker to execute unauthorized SQL code or commands via crafted HTTP or HTTPs requests.

CVE-2025-59287
CVSS Score: **9.8**

Details: Deserialization of untrusted data in Windows Server Update Service allows an unauthorized attacker to execute code over a network.

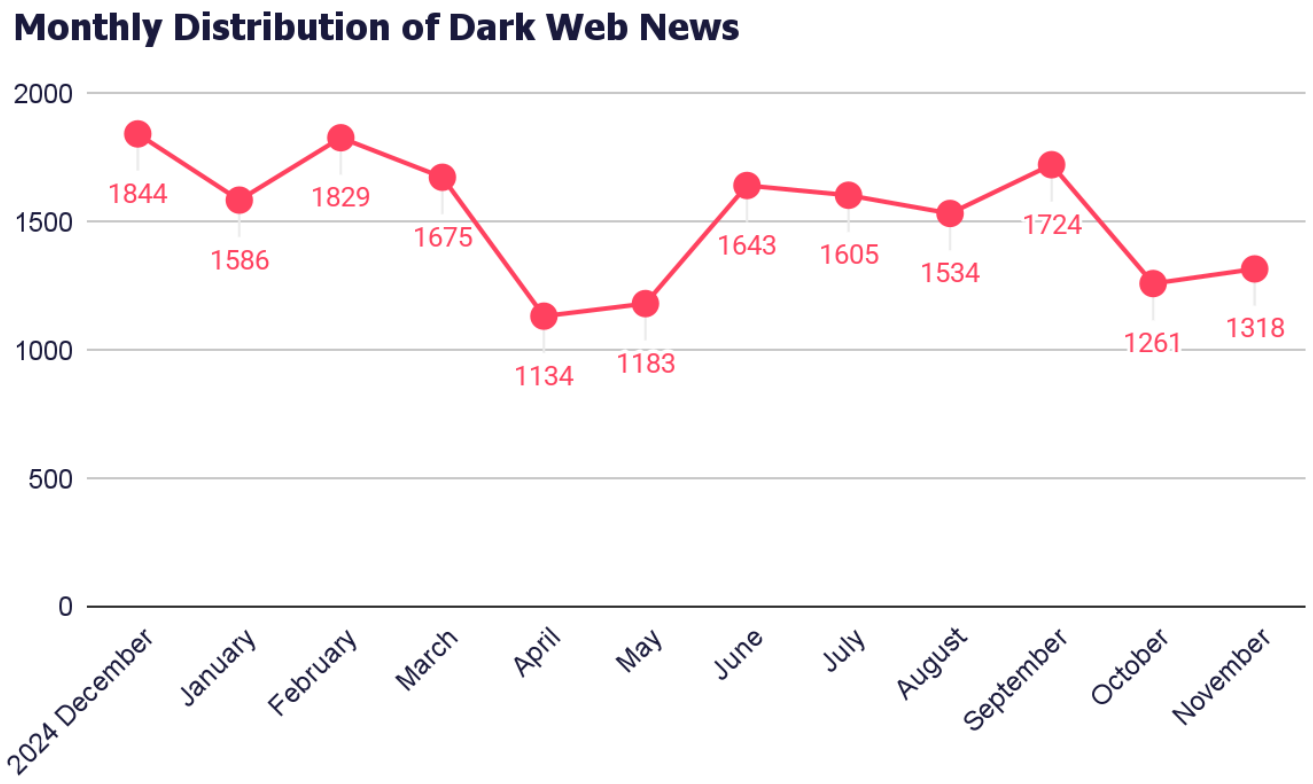
CVE-2025-3248
CVSS Score: **9.8**

Details: Langflow versions prior to 1.3.0 are susceptible to code injection in the /api/v1/validate/code endpoint. A remote and unauthenticated attacker can send crafted HTTP requests to execute arbitrary code.

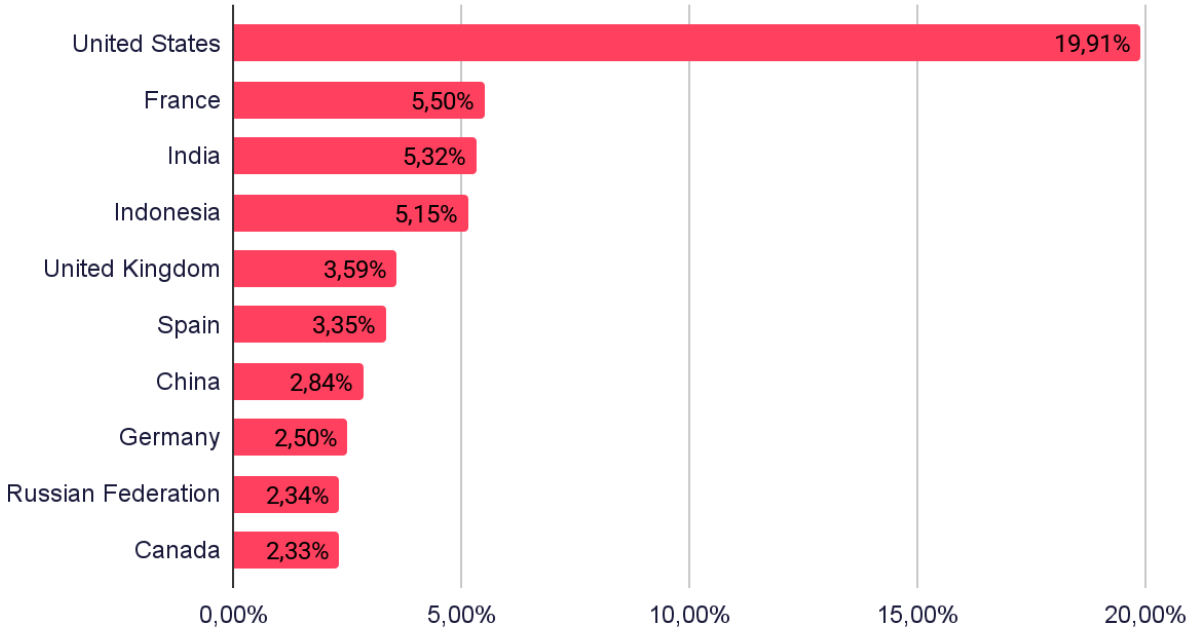
Dark Web Statistics of 2025

This section provides insights into the data gathered by SOCRadar in 2025. 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.

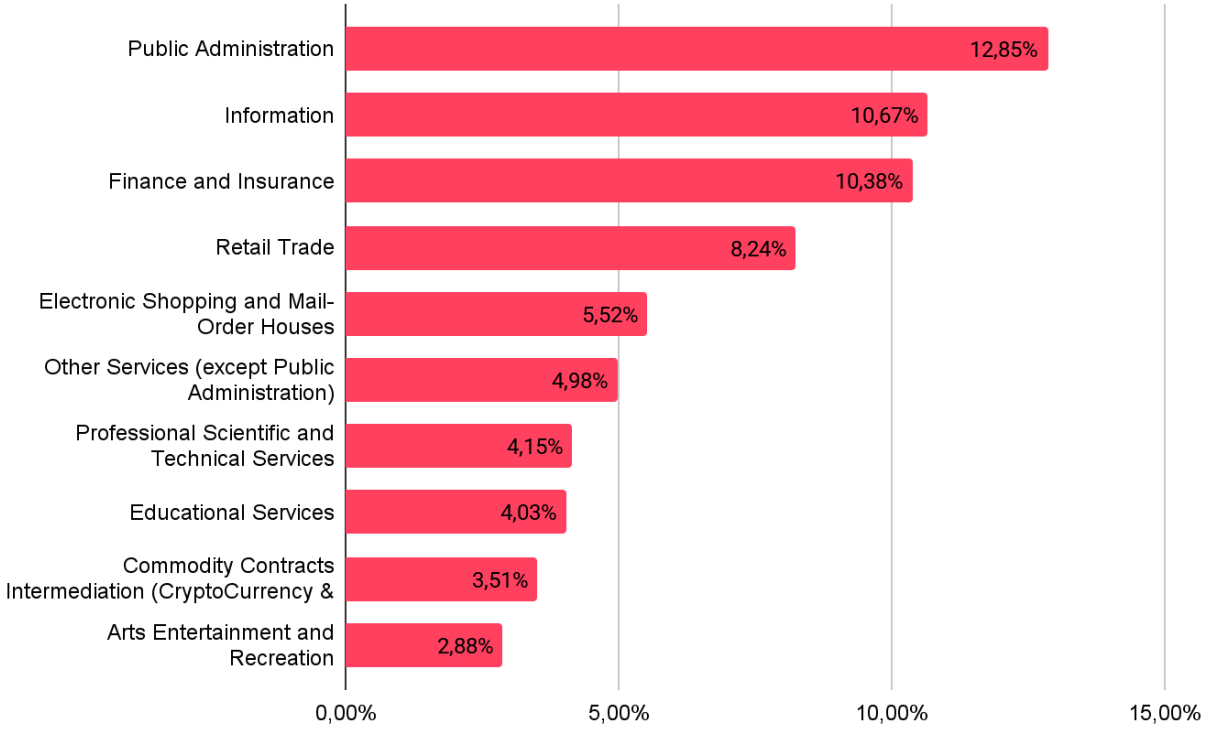
The total number of posts published on the platform's Dark Web News channel during this period was 18,336.

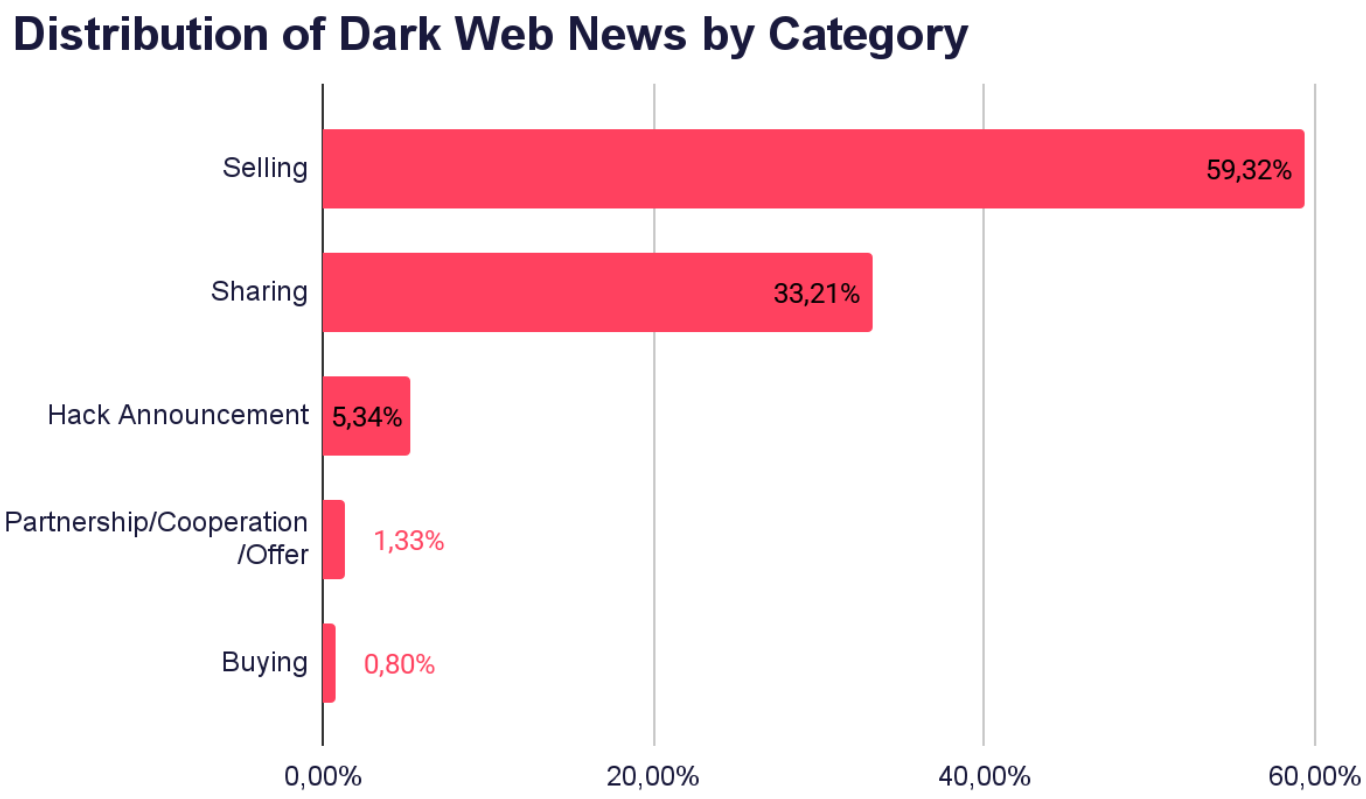


Distribution of Dark Web News by Country



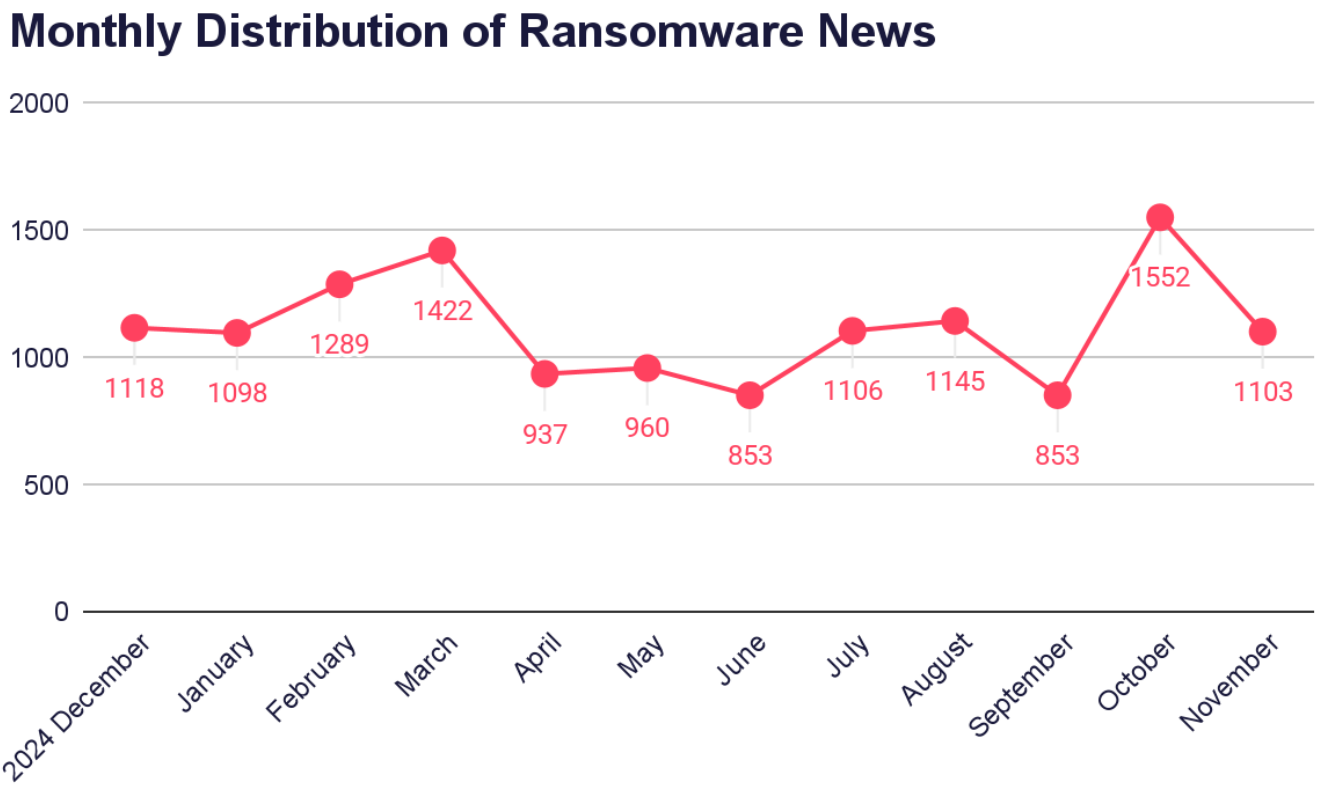
Distribution of Dark Web News by Industry



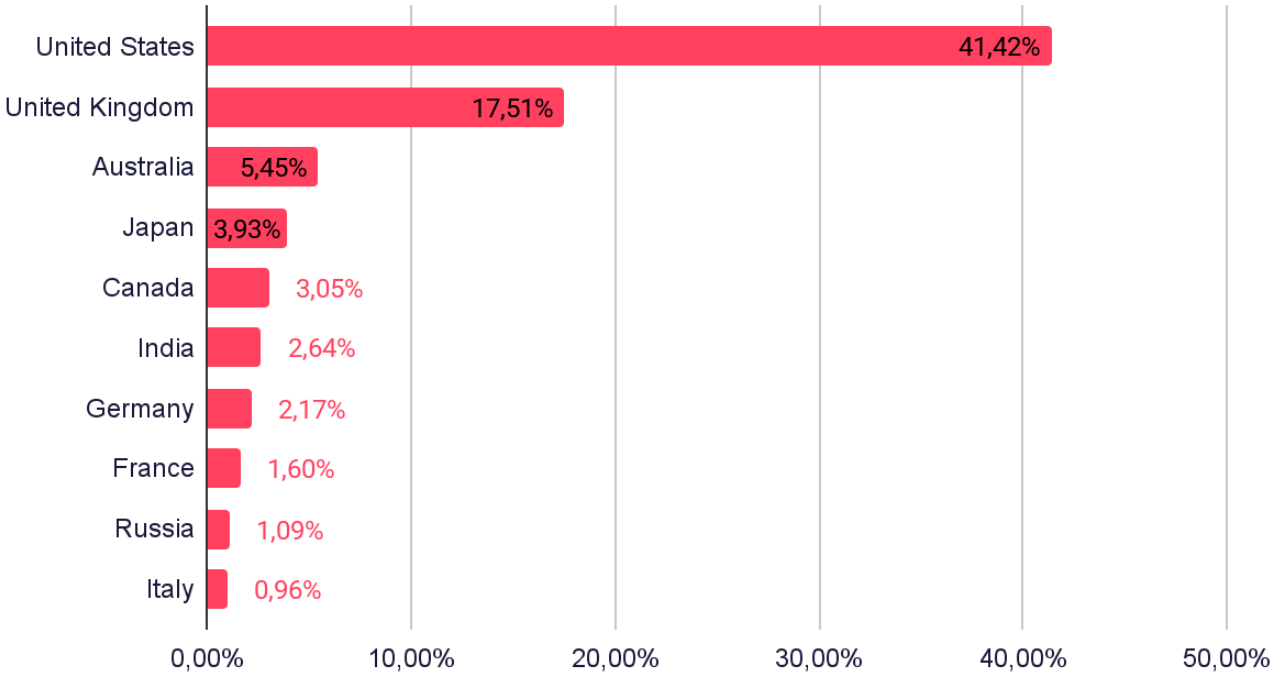

Distribution of Dark Web News by Category
Selling
59,32%
Sharing
33,21%
Hack Announcement
5,34%
Partnership/Cooperation /Offer
1,33%
Buying
0,80%
0,00%
20,00%
40,00%
60,00%

Ransomware Statistics of 2025

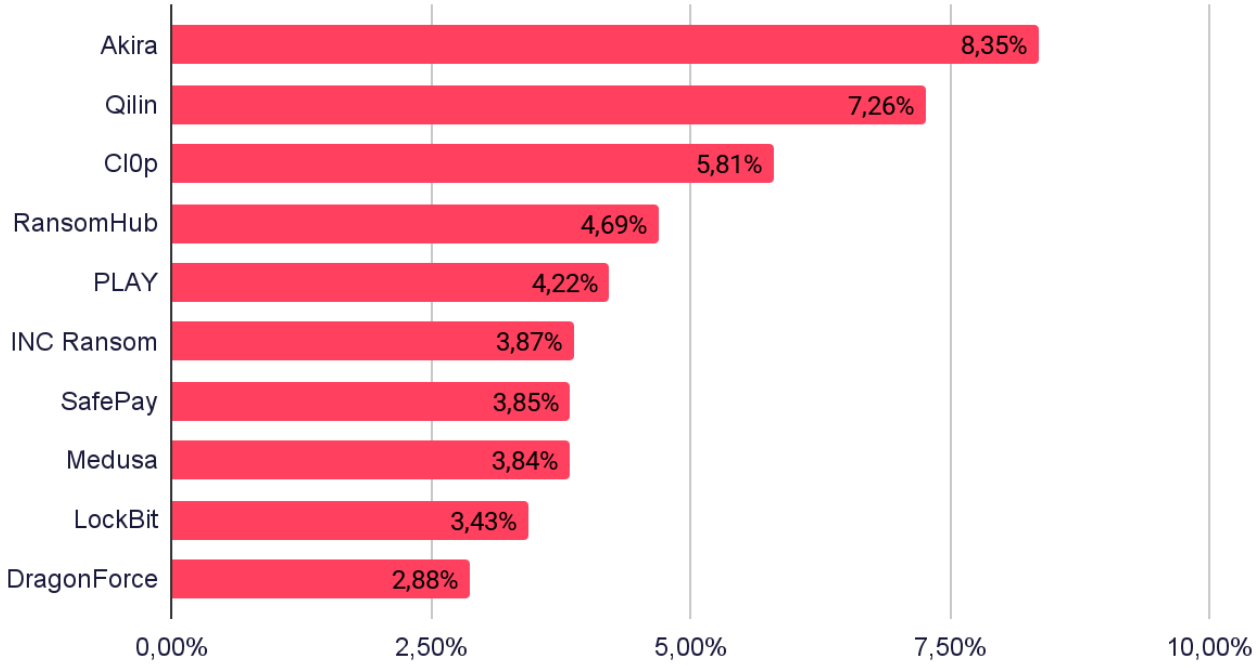
The data is sourced from a comprehensive analysis conducted by SOCRadar analysts during 2025. We've scoured ransomware groups' blog sites, leak sites, and Telegram channels to compile a trove of valuable information. Over this period, we've gathered a staggering total of 13,436posts related to ransomware attacks.



Distribution of Ransomware Attacks by Target Country



Top 10 Most Active Ransomware Groups



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

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

Cl0p

Country of Origin: Russia

A Ransomware group that has been active since 2019 and currently brings up its name by exploiting zero-day vulnerabilities that existed in GoAnyWhere MFT and MOVEit MFT software.

-Ransomware Group-

Motivation: Financial Gain

Target Countries: The US, Canada, The UK, Australia, Colombia, Sweden, Germany, India, Mexico, Turkey

Target Sectors: IT, Healthcare, Finance, Professional Services, Retail, Media, Telecommunication

Attack Type: Spearphishing, Zero-Day Exploitation, Compromised RDP, Ransomware, Data exfiltration, Double-extortion

-TTPs-

Exploit Public-Facing Application: T1190

Exploitation for Privilege Escalation: T1068

Exfiltration Over C2 Channel: T1041

-Ransomware-

Motivation: Financial Gain

Target Countries: United States, United Kingdom, Brazil, Indonesia, Vietnam, Canada

Target Sectors: Healthcare, Manufacturing, Business Services

Attack Type: Ransomware, Data Leakage, Extortion

-TTPs-

Exploit Public-Facing Application: T1190

Data Encrypted for Impact: T1486

Remote Services: Remote Desktop Protocol: T1021.001

-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

-Ransomware Group-

Motivation: Financial

Target Countries: US, UK, Australia

Target Sectors: Professional Services, Manufacturing, Construction

Attack Type: Phishing, Extortion, Ransomware

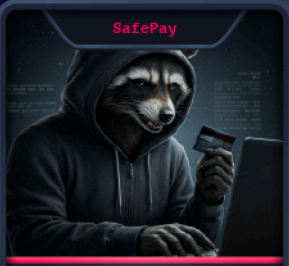
-TTPs-

Spear-Phishing: T1566

Valid Accounts: T1078

Data Destruction: T1485

SafePay



Country of Origin: Russia(?)

SafePay is a rapidly emerging ransomware group that rose from obscurity in early 2025 to become one of the most active and dangerous threats on the global cyber landscape. In just a few months, it has launched attacks against over 200 victims worldwide.

-Ransomware-

Motivation: Financial Gain

Target Countries: US, Germany, UK, Canada, Australia, Singapore

Target Sectors: Manufacturing, Business Services, Technology, Education

Attack Type: Double-Extortion, Ransomware, Data Leak

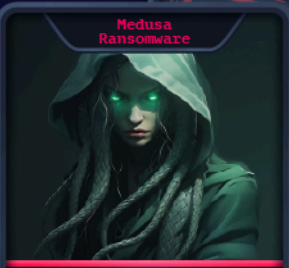
-TTPs-

System Binary Proxy Execution: T1218

Valid Accounts: T1078

Data Encrypted for Impact: T1486

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

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

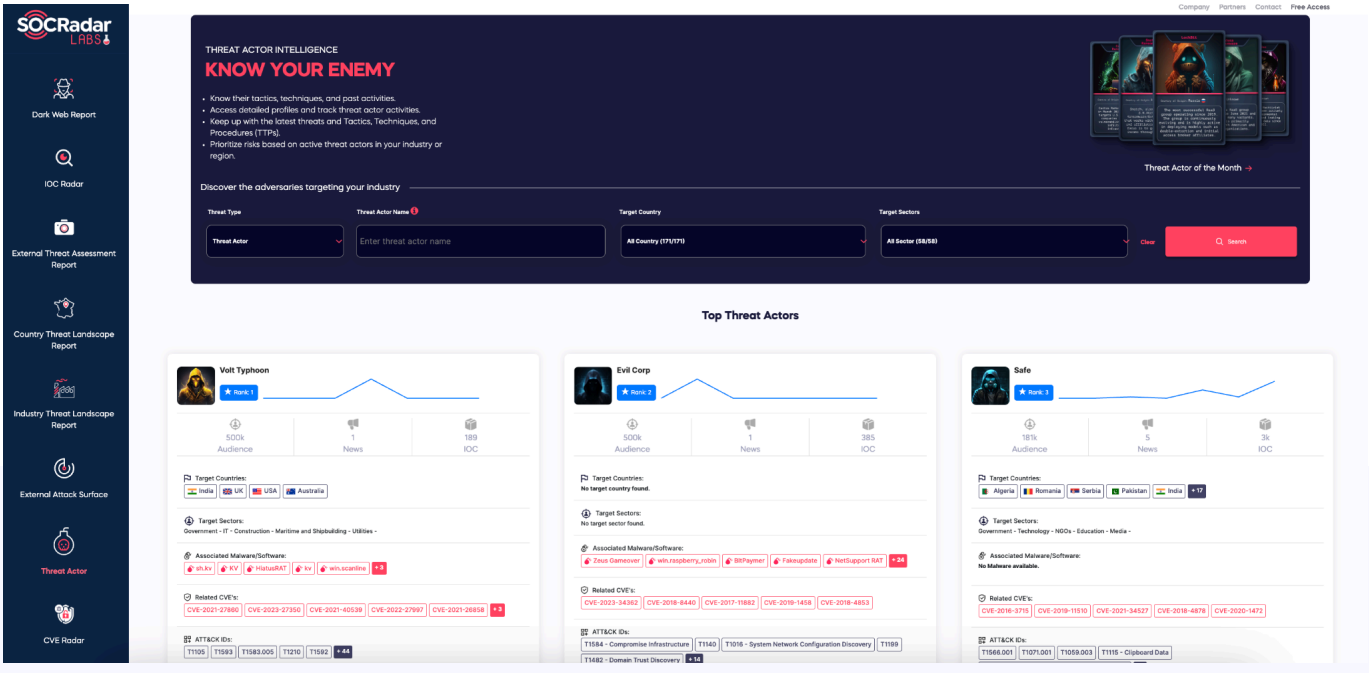
Attack Type: Phishing, RDP and VPN access Exploitation, Ransomware, Data Exfiltration, Double-extortion

-TTPs-

Exploit Public-Facing Application: T1190

Remote Desktop Protocol: T1021.001

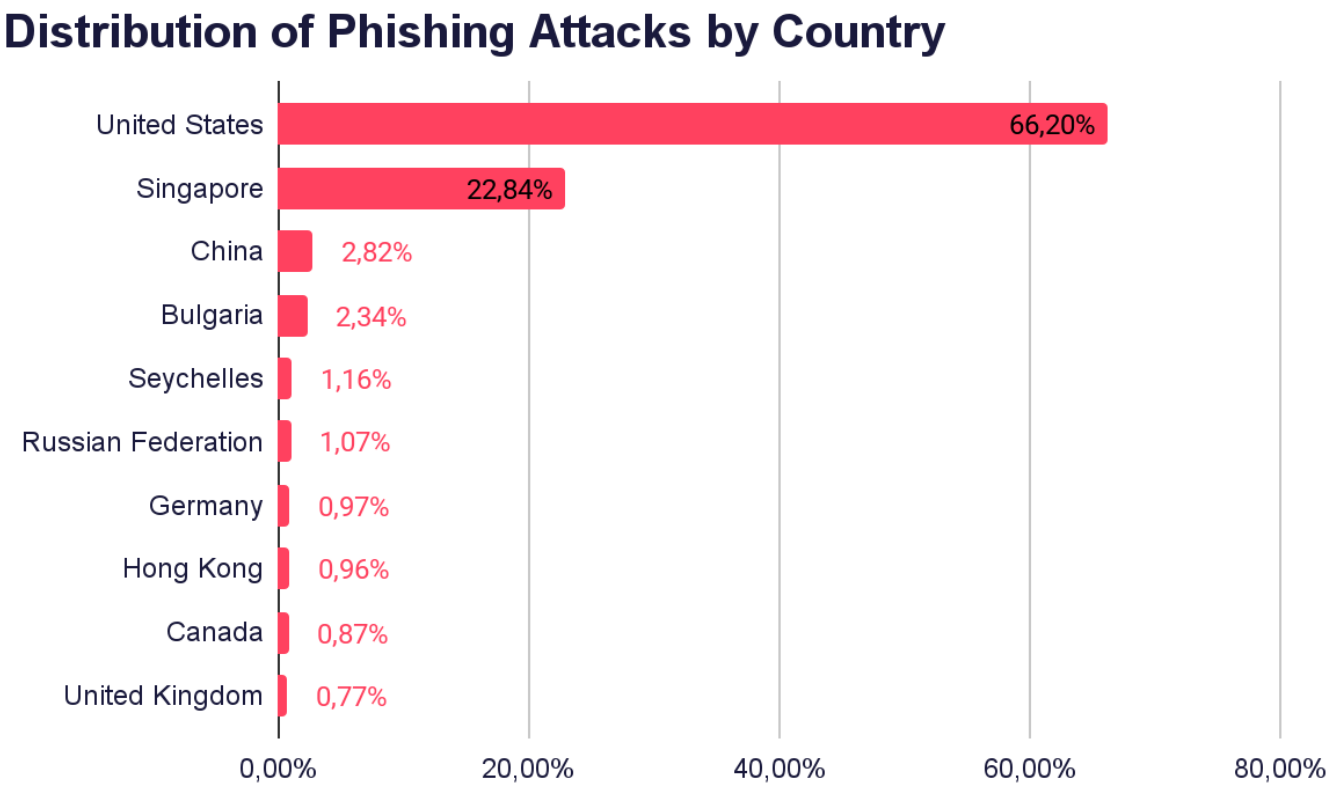
Data Encrypted for Impact: T1486



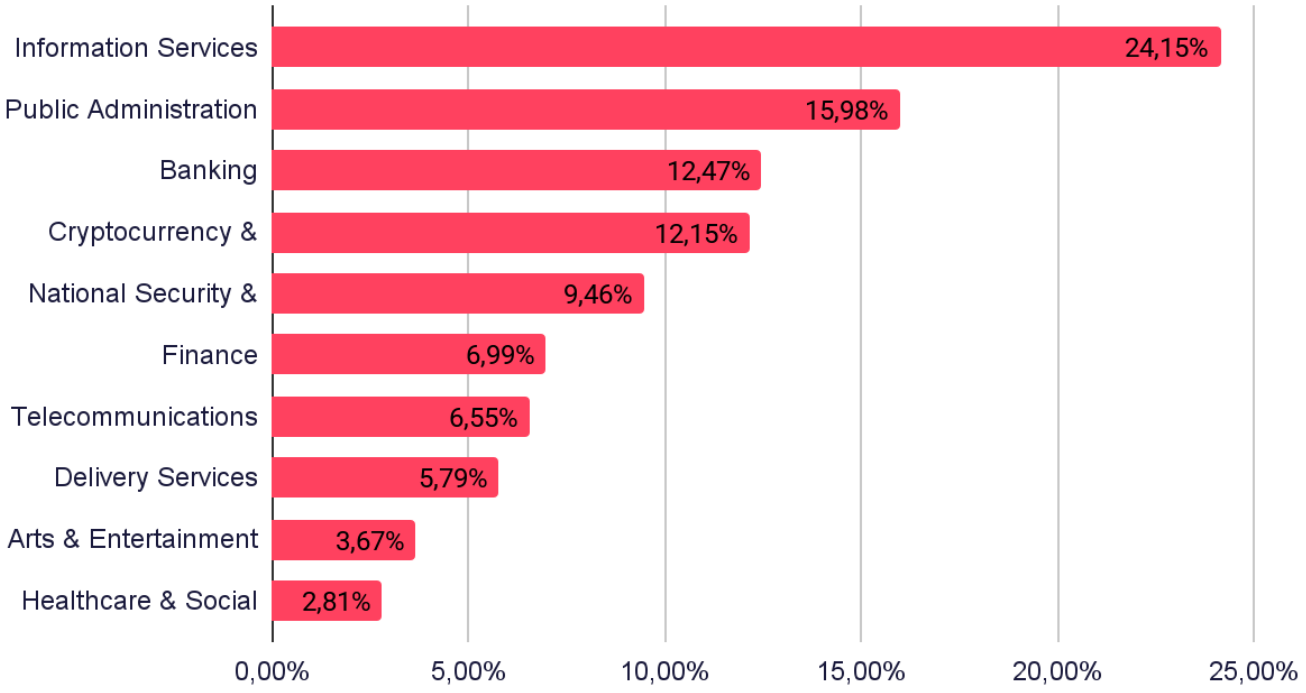
SOCRadar enhances cybersecurity measures with its [Threat Actor Intelligence Module](), which features advanced Threat Actor Tracking capabilities for organizations that want to stay ahead of cyber threats in real time.

Global Phishing Trends

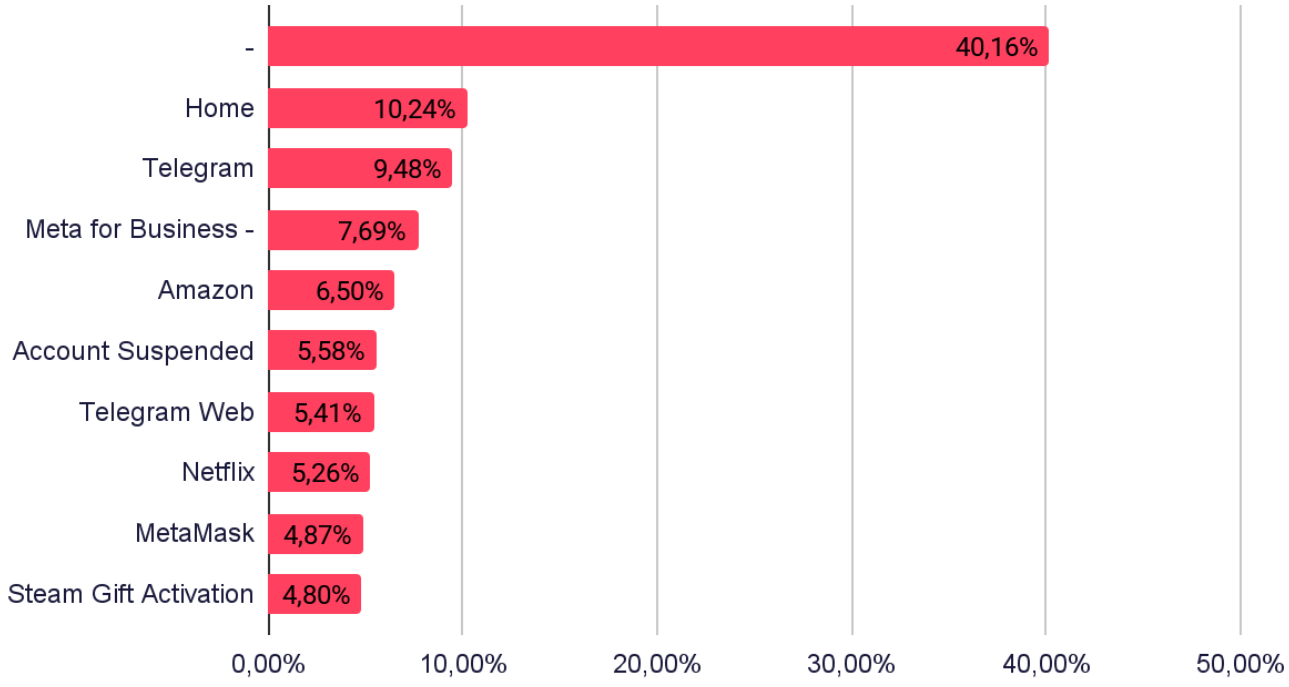
Phishing remains a highly effective tactic for breaching an organization's infrastructure. It often involves tricking individuals into providing sensitive credentials on fake websites.



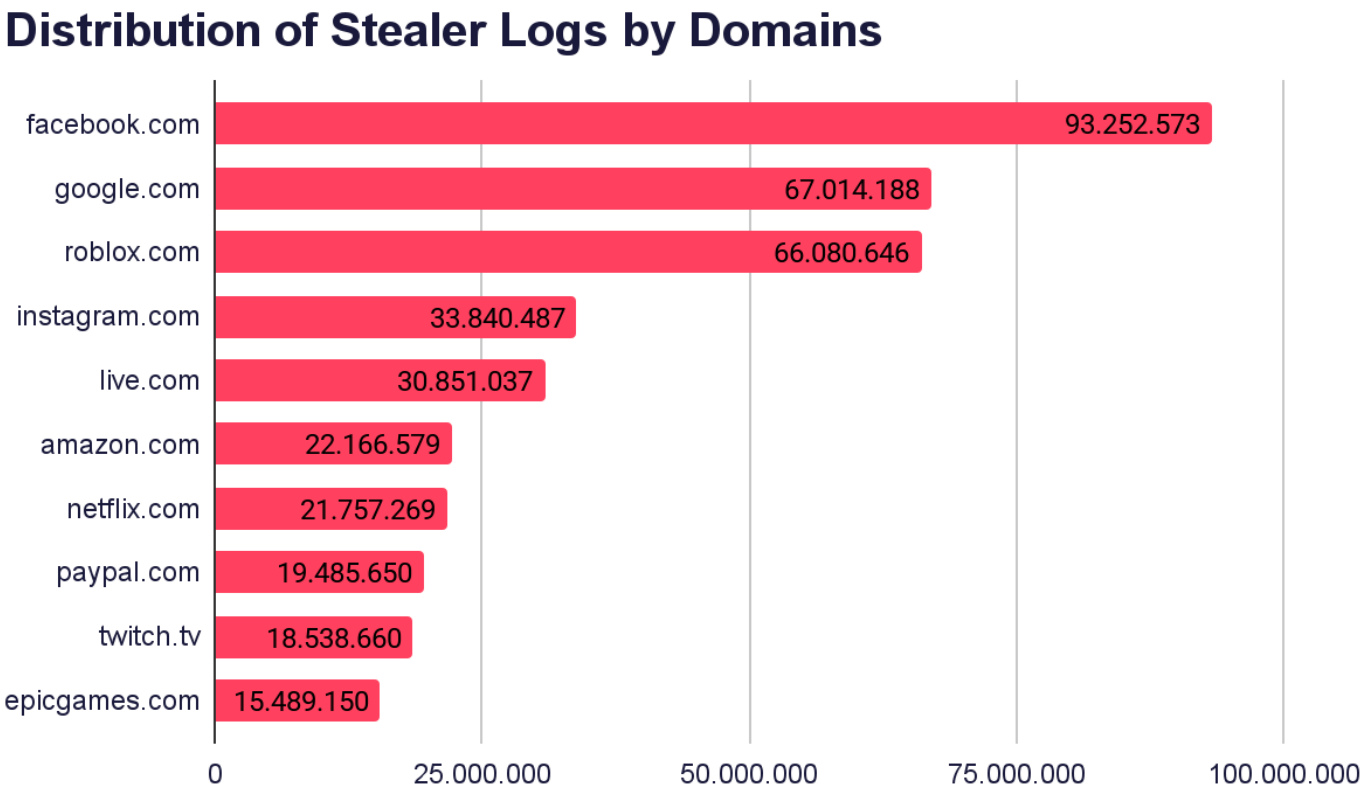
Distribution of Phishing Attacks by Industry



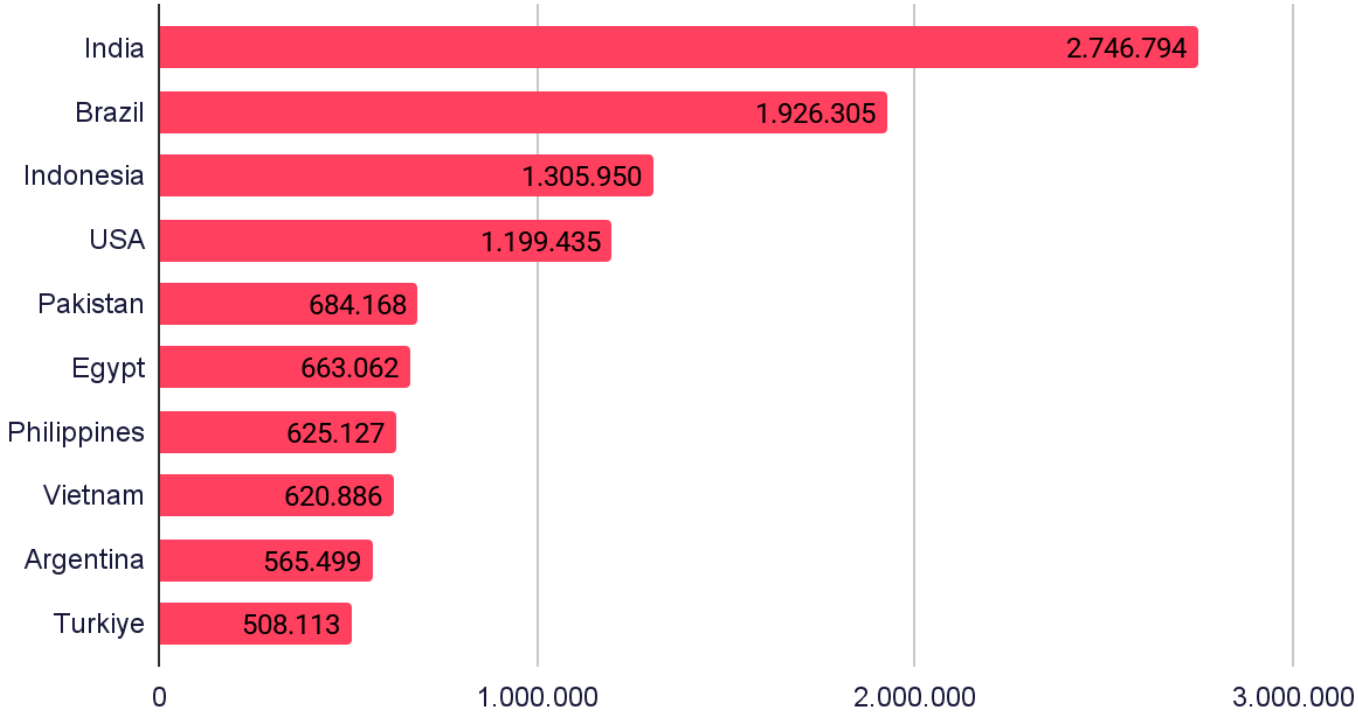
Distribution of Phishing Attacks by Page Title



Stealer Log Statistics



Distribution of Stealer Logs by Country



Lessons Learned: Key Insights and Strategic Recommendations

An analysis of the global cybersecurity threats in 2025 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?

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.