



US

Threat Landscape Report



Table of Contents

Introduction	3
Notable Incidents	4
Recent Incidents	6
Dark Web Radar	10
The Ransomware Threat Landscape in the United States	18
Navigating the Cyber Threat Landscape Key Challenges for US Organizations	24
Looking Ahead: Cyber Threat Prospects for 2024	26
Conclusion	28

Introduction

In an era where digital transformation propels us forward, the cyber realm unfolds as a double-edged sword—empowering innovation and connectivity while simultaneously exposing us to the ever-evolving threats lurking within the cyber landscape.

This report delves into the intricacies of cybersecurity challenges and notable incidents that have shaped the security posture of the United States over recent years. It draws upon a comprehensive analysis of cyber incidents, from breaches impacting public sectors and educational institutions to sophisticated ransomware attacks that have put critical infrastructure at risk.

Through meticulous documentation and analysis, this report aims to shed light on the patterns, tactics, and profiles of adversaries that have dominated the cyber threat landscape. It serves as a testament to the persistent nature of cyber threats and underscores the imperative need for resilient cybersecurity measures, proactive defense strategies, and a collective commitment to safeguard our digital ecosystem against the multifaceted threats of today and tomorrow.

Notable Incidents

Plex Database Breach (August 2022)

Threat Actor: Unknown third party

Method: Database hack

Aftermath: Stolen emails, usernames, and encrypted passwords; system admins urged password reset.

Los Angeles Unified School District Ransomware Attack (September 2022)

Threat Actor: Vice Society

Method: Ransomware

Aftermath: 500GB of sensitive data leaked, including personal identifying information and student records.

PayPal Credential Stuffing Attack (December 2022)

Threat Actor: Unknown

Method: Credential stuffing

Aftermath: Breached 34,942 accounts, exposing sensitive info.

United States Marshals Service Ransomware Attack (February 2023)

Threat Actor: Unknown

Method: Ransomware

Aftermath: Compromised sensitive law enforcement data.

3CX Supply Chain Attack (March 2023)

Threat Actor: North Korean actors

Method: Supply chain attack, malicious code insertion

Aftermath: Global user impact, including in the US

Enzo Biochem Ransomware Attack (April 2023)

Threat Actor: Unknown

Method: Ransomware

Aftermath: Compromised test data and personal info of about 2.5 million individuals.

City of Oregon (Royal Ransomware) Attack (May 2023)

Threat Actor: Royal Ransomware

Method: Ransomware

Aftermath: Encrypted county data, significantly impacting government operations.

MOVEit Transfer and Cloud Vulnerability (June 2023)

Threat Actor: Cl0p, Russian-affiliated cyber gang

Method: Exploitation of a SQL injection vulnerability

Aftermath: Numerous organizations affected, including US government entities.

Real Estate Wealth Network Data Breach (December 2023)

Threat Actor: Unknown

Method: Unprotected database exposure

Aftermath: 1.5 billion records leaked, including sensitive real estate information.



HACKED

Recent Incidents

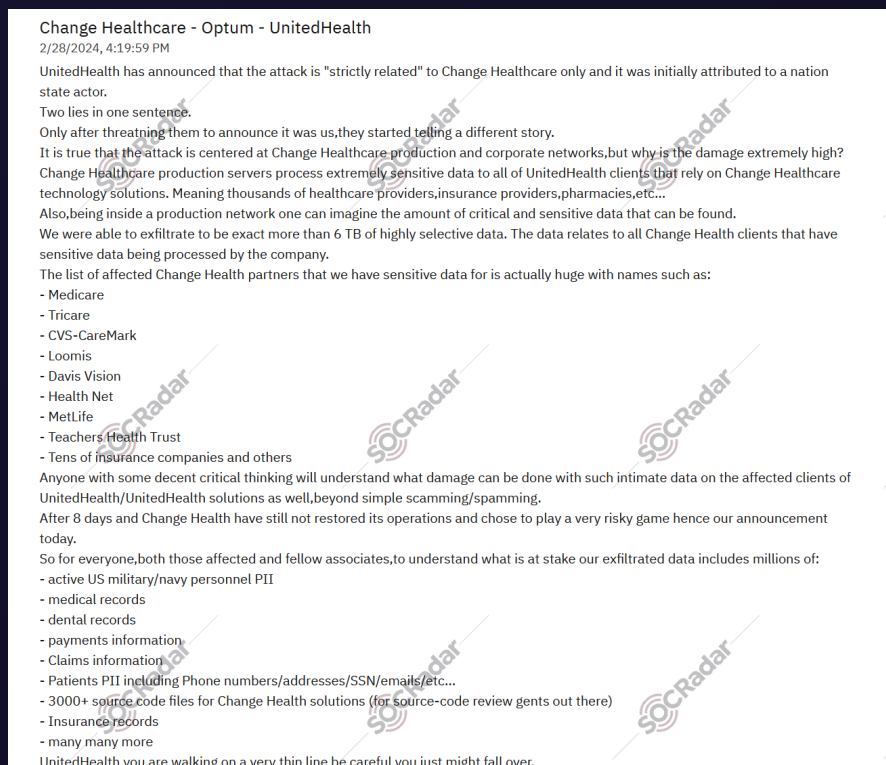
Phoenix Conducted DDoS Attack on Alaska Airlines



In the Phoenix's Telegram channel monitored by SOCRadar, the DDoS attack announcement was detected for Alaska Airlines.

Source: SOCRadar

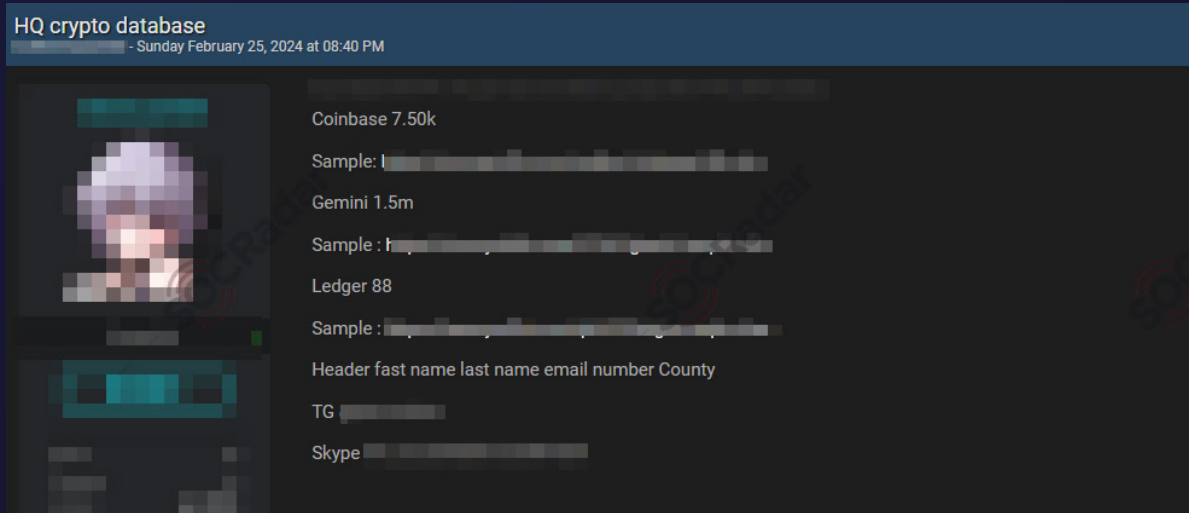
The New Ransomware Victim of AlpHV / BlackCat: Change Healthcare



In the AlpHV / BlackCat ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Change Healthcare.

Source: SOCRadar

Customer Databases of Coinbase, Gemini and Ledger are on Sale



Source: SOCRadar

In a hacker forum monitored by SOCRadar, a new alleged databases sale was detected for Coinbase, Gemini and Ledger.

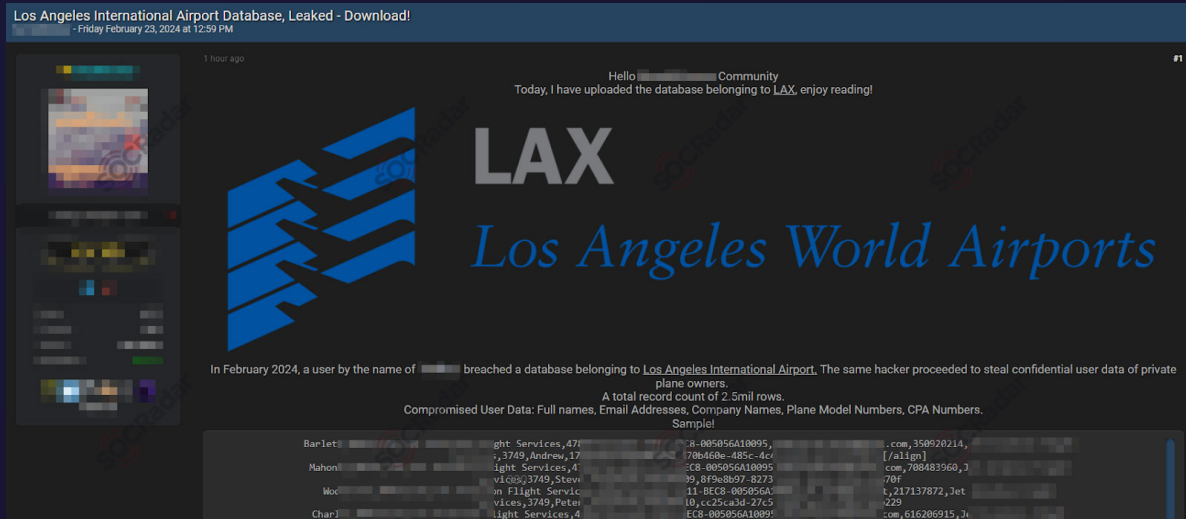
The New Ransomware Victim of LockBit 3.0: Eastern Shipbuilding Group



Source: SOCRadar

In the LockBit 3.0 ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Eastern Shipbuilding Group.

Database of Los Angeles International Airport was Leaked



Source: SOCRadar

In a hacker forum monitored by SOCRadar, a new alleged database leak was detected for Los Angeles International Airport.

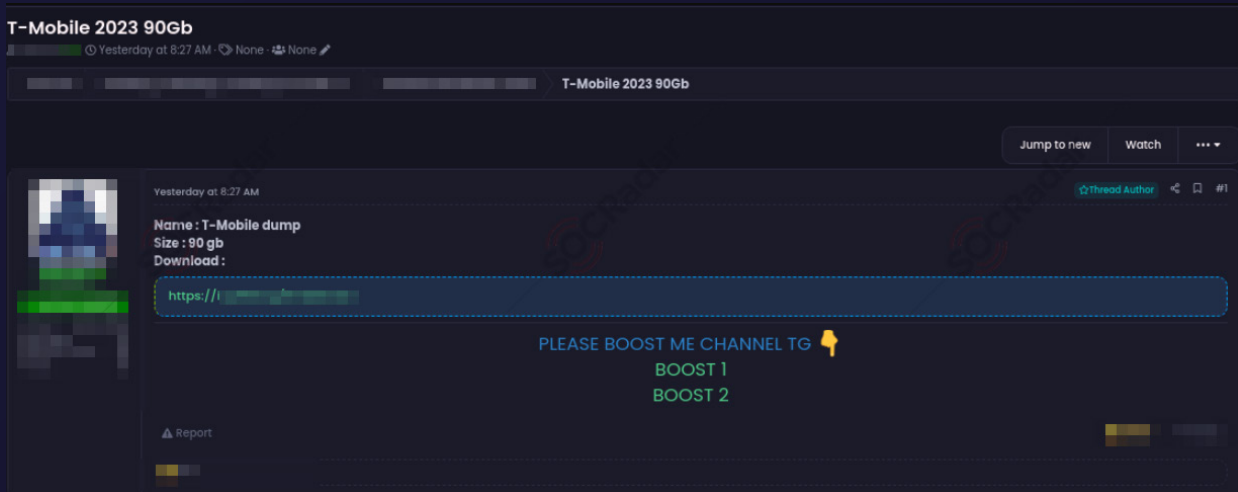
The New Ransomware Victim of Medusa Team: JS International



Source: SOCRadar

In the Medusa Team ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as JS International.

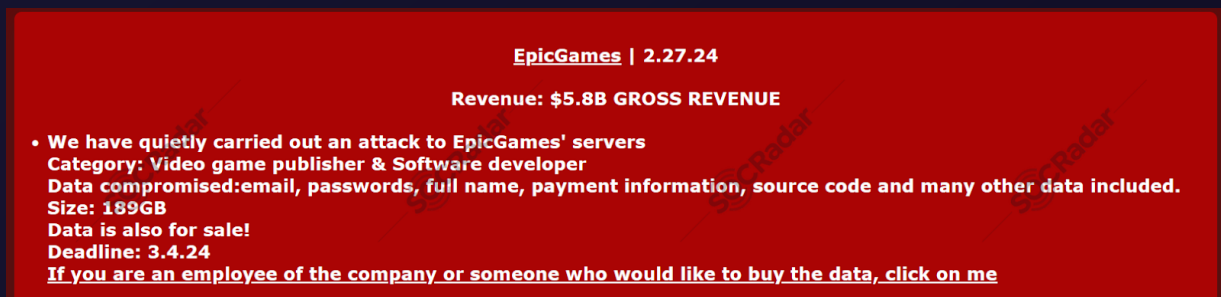
Alleged Database Leak of T-Mobile



Source: SOCRadar

In a hacker forum monitored by SOCRadar, a new alleged database leak was detected for T-Mobile.

The New Ransomware Victim of Mogilevich: Epic Games



Source: SOCRadar

In the Mogilevich ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Epic Games.

Dark Web Radar

In the rapidly evolving landscape of cybersecurity threats, one of the most insidious arenas for illegal activities is the dark web. SOCRadar, with its advanced Extended Threat Intelligence Platform, meticulously monitors this shadowy digital landscape. Our state-of-the-art tools actively crawl through dark web forums and Telegram channels, spaces frequently exploited by threat actors for communication, propaganda, and the dissemination of illicit information. Each significant incident related to cybersecurity threats is documented with meticulous care by our skilled analysts. This process is enhanced through extensive tagging, which includes the identification of the involved organization, the industry it belongs to, and its country of origin, as well as the entity that posted the information. This granular categorization allows us to provide a nuanced and valuable analysis of each incident. These findings are shared within our Dark Web News channel, an integral component of the SOCRadar platform, which serves as a vital resource for our clients.

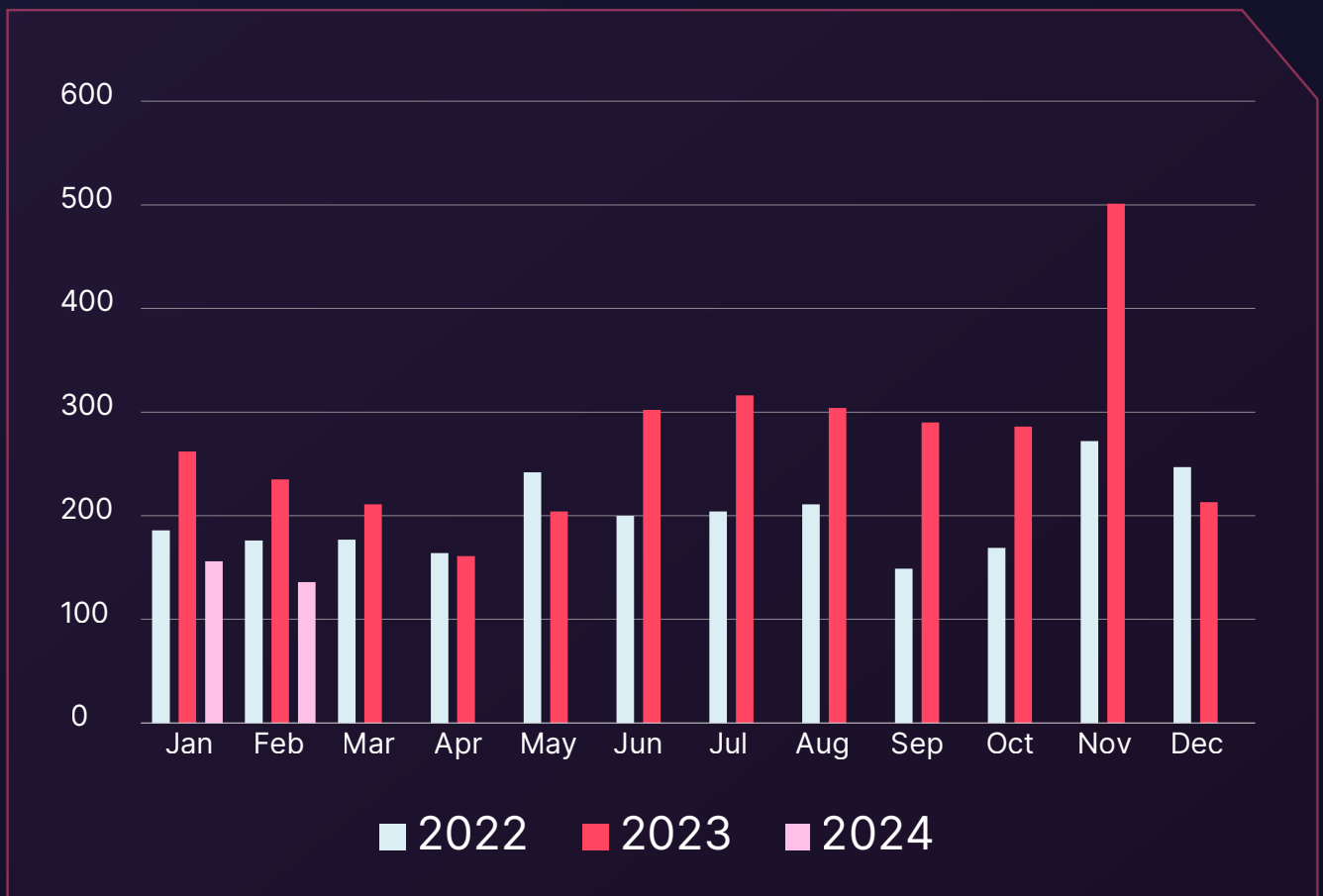
The forthcoming sections will delve into various aspects of the cyber threat landscape in the United States, with an emphasis on the period from January 2022 to February 2024. It's imperative to understand that the figures we discuss are not a direct correlation to the number of cyber attacks but rather the frequency of mentions in the dark web's clandestine channels. Hence, the data should be regarded as indicative of trends and not as absolute figures of cyber incidents.

We will explore the time distribution of these posts, identify the top industries targeted, categorize the nature of these mentions, and scrutinize the profiles of the post owners. Please note that the information presented here is more indicative than exact, providing insights into the trending discussions rather than direct correlations with the number of cyber attacks.

Dark Web Discussions Over Time

In this subsection, we analyze the distribution of dark web mentions related to cybersecurity incidents concerning the United States over the last two years. The data spans from January 2022 to February 2024 and reflects the frequency of such mentions captured by SOCRadar's extensive intelligence gathering.

▶ Monthly Distribution of Dark Web Mentions



This bar graph represents the monthly count of dark web mentions related to cybersecurity concerns in the United States from January 2022 to February 2024.

Analyzing the provided data, we observe a notable trend in the frequency of dark web mentions. The year 2023 shows a significant uptick in activity, particularly in the latter half, with November peaking at 501 mentions. This could indicate a surge in cyber threats or an increase in the sharing of intelligence within dark web circles during this period. The year 2024 begins with a downward trend, though data is only available for the first two months. It's important to consider external factors that may have influenced these discussions, such as geopolitical events like Israel - Hamas conflict or notable cybersecurity breaches. The consistency of the data throughout the years highlights the persistent and ever-present nature of cyber threats.

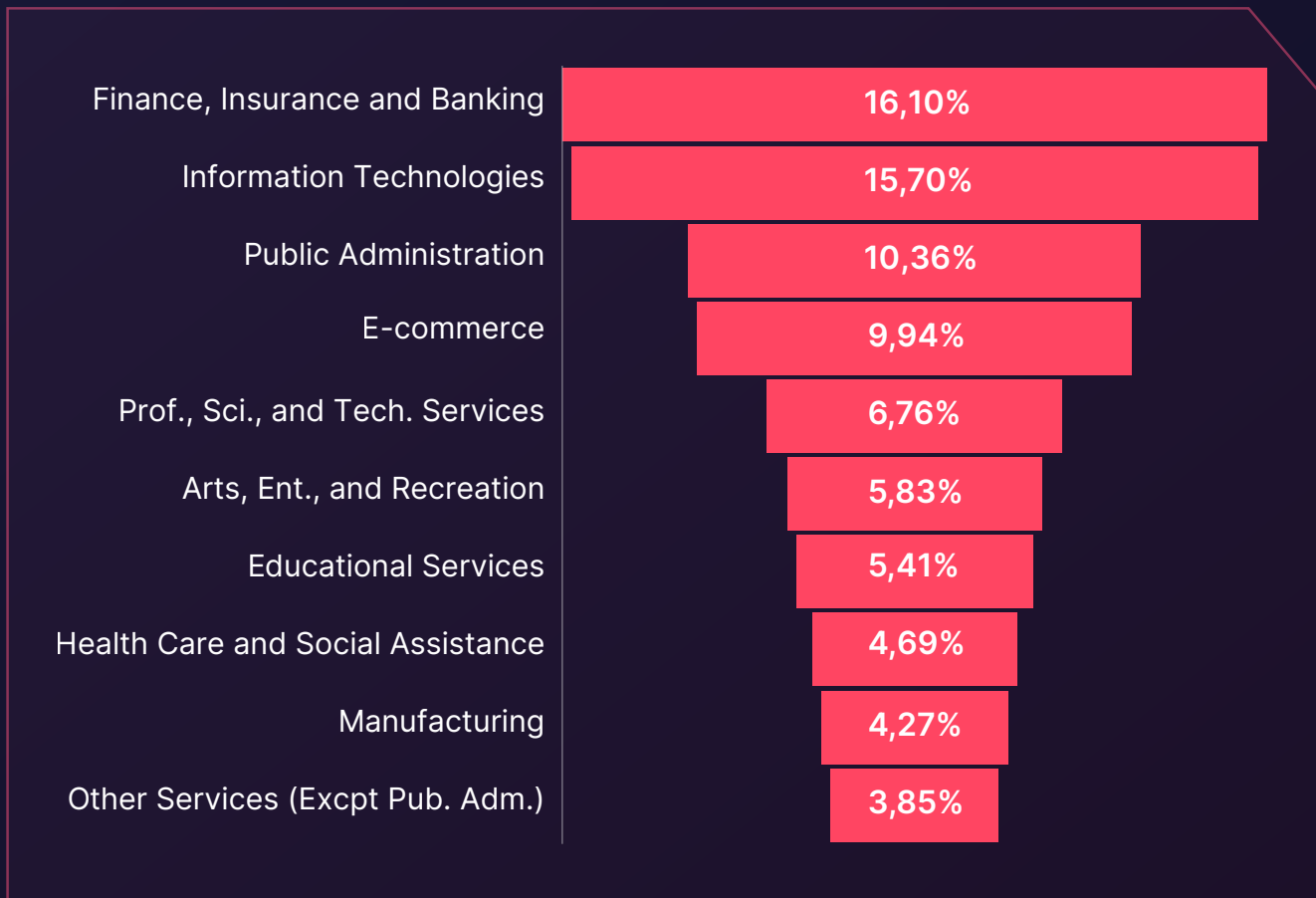
Upon closer inspection, the average monthly mentions exhibit a rising trajectory from an average of 199.75 in 2022 to 273.75 in 2023, reflecting a year-over-year increase in dark web chatter related to cybersecurity incidents. This escalation suggests an expanding concern or growing activity regarding cyber threats within the United States' context. However, it's important to recognize the abrupt decline in the first two months of 2024, with an average of 146 mentions, which could signify a potential shift in the cyber threat landscape or the efficacy of countermeasures impacting dark web discussions. The data's fluctuation could also be indicative of seasonal trends in cyber activities or the cyclic nature of how threat actors operate and communicate within the dark web arena.

This temporal analysis serves as a barometer for the dark web's interest and activity level concerning cybersecurity incidents in the United States, providing an essential perspective for threat anticipation and intelligence.



Industry Focus in Dark Web Conversations

► Proportional Focus on Industries in Dark Web Mentions



A representation of the top ten industries by proportion of mentions within dark web posts related to cybersecurity incidents in the United States from January 2022 to February 2024.

In analyzing the industries that dominate dark web discussions, we see that the Finance, Insurance, and Banking sector leads with 16.10% of all mentions. This is closely followed by Information Technologies at 15.70%, suggesting a high level of interest from threat actors in these sectors, likely due to their critical roles in the economy and the valuable data they hold.

Public Administration is the third most discussed industry with 10.36% of mentions, indicating its strategic importance and potential as a target for cyber threats. E-commerce follows with 9.94%, which may reflect its growing size and the corresponding increase in attack surfaces as more business is conducted online.

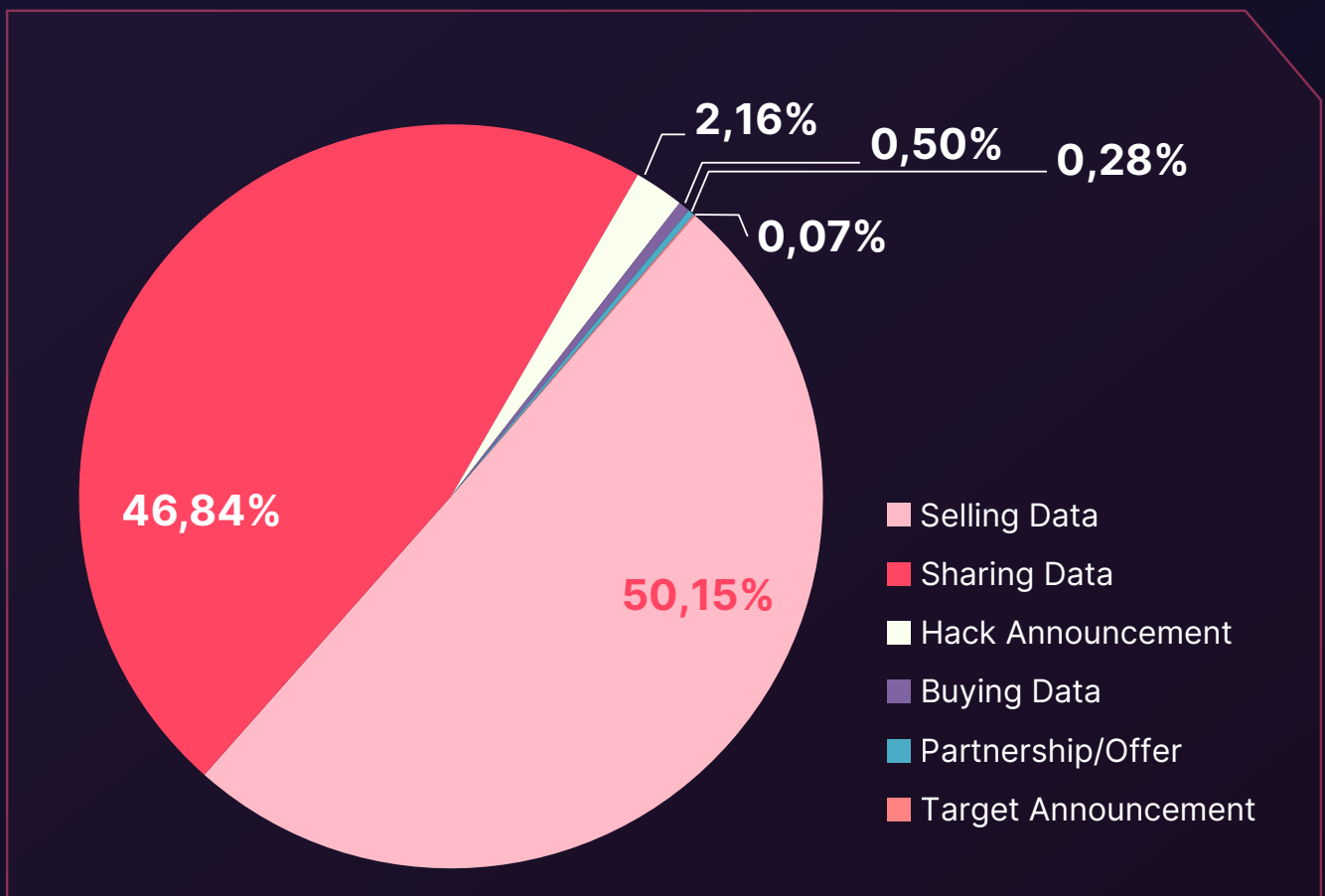
The Professional, Scientific, and Technical Services sector, Arts, Entertainment, and Recreation, as well as Educational Services, show moderate attention from the dark web, highlighting a diverse interest across various facets of the economy and society.

Health Care and Social Assistance, Manufacturing, and Other Services (except Public Administration) are less frequently mentioned but are still notable for their presence in these discussions. It's important to note that posts with multiple tags indicate a single post may reference more than one organization, which might skew individual industry percentages slightly when cross-sector incidents are reported.

This proportional analysis underscores the varying levels of interest and potential vulnerabilities across different sectors, signifying where threat actors may perceive opportunities or weaknesses. It serves as a vital signpost for industries to evaluate and bolster their cybersecurity defenses accordingly.

Dissecting the Intent and Content of Dark Web Exchanges

▶ Intentions Behind Dark Web Cybersecurity Posts



The pie chart depicts the breakdown of dark web post intentions related to cybersecurity threats involving the United States from January 2022 to February 2024.

The pie chart reveals that half of the dark web activities (50.15%) are related to selling data, indicating a significant market for illicitly obtained information. Close behind is the sharing of data, accounting for 46.84%, which suggests a strong community aspect among threat actors who are disseminating information perhaps as a means of collaboration or reputation building.

Notably, smaller proportions of posts are related to hack announcements (2.16%), indicating the communication of successful breaches, and buying data (0.50%), reflecting demand for specific data types or access. Partnerships or offers (0.28%) and target announcements (0.07%) represent a minor fraction, which could imply a more secretive process for these activities or that they occur through more private channels.

Dark Web Marketplace Commodities of the Cyber Underground

Leak Type	Sharing	Selling
Data	1,951	804
Sensitive Data	100	183
Customer Data	138	113
Employee Data	15	24
Credit Card	3	297
Access	23	568
RDP Access	1	228
Network Access	0	118
Admin Access	3	107
Shell Access	2	53
VPN Access	1	47

The table outlines the types of data and access credentials threat actors deemed valuable to sell or share on the dark web, highlighting the focus areas for these illicit transactions.

The table outlines the types of data and access being traded on the dark web, with a clear distinction between what is commonly shared and what is sold. The category with the most activity is generic "Data," which sees a substantial amount of sharing at 1,951 instances, pointing to a tendency among threat actors to exchange information without immediate financial gain. In contrast, this category also sees 804 instances of sales, suggesting that while the information is often shared, there's also a significant market for purchasing it. Sensitive data, which includes information that's either confidential or subject to regulatory protection, also shows notable activity. It's more often sold (183 instances) than shared (100 instances), highlighting its high value on the dark web.

The 'Credit Card' information shows a dominant selling trend with 297 instances, which suggests a significant market for financial exploitation. In contrast, only three instances are recorded under sharing, indicating such sensitive information is more commoditized than freely circulated. This trend totally reverses for what can be considered more actionable or directly profitable items like access credentials.

'RDP Access,' which allows remote control of another computer, has a marked commercial interest with 228 selling instances against a single instance of sharing. 'Network Access' and 'Admin Access' follow this pattern, with a clear preference for sales over sharing, showing figures of 118 and 107 for sales, respectively. These numbers underscore the premium placed on obtaining unauthorized access to systems, which can be leveraged for more complex cyber-attacks or espionage.

'VPN Access' also reflects a commercial inclination with 47 selling instances, again emphasizing the illicit market demand for secure and anonymous access points to networks.

Overall, the table illustrates a clear dichotomy: while general data is often shared, suggesting a focus on information spread and collaboration, access credentials are primarily sold, pointing to a dark web economy driven by the exploitation of such accesses for financial gain



Profiling Dark Web Post Owners

Activity Spectrum of Top Dark Web Post Owners

Post Owners	Total Post	Sharing	Selling
Hydra Market	193	100.00%	0.00%
Chucky	118	100.00%	0.00%
nixploiter	77	0.00%	100.00%
markitto35	66	98.48%	1.52%
IntelBroker	65	60.00%	40.00%
Osiris	61	100.00%	0.00%
FentanylTroia	53	100.00%	0.00%
kelvinsecurity	44	40.91%	59.09%
sandocan	38	0.00%	100.00%
Leakbase	29	96.55%	3.45%

This table presents the top ten dark web entities by the number of posts, highlighting their engagement in either sharing or selling information related to cybersecurity threats in the United States from January 2022 to February 2024.

The data presents an interesting spectrum of activities among the top post owners on the dark web. It challenges the general assumption that threat actors frequently share data to build trust before selling. Instead, we observe distinct operational profiles. For instance, 'Hydra Market' and 'Chucky' are entirely focused on sharing information, with zero instances of selling. This could indicate a strategy of fostering a community or gaining credibility within the dark web ecosystem.

Conversely, entities like 'nixploiter' and 'sandocan' have a 100% selling record with no posts logged under sharing. 'kelvinsecurity' also leans towards selling with a majority of 59.09%. This pattern suggests that certain entities may operate successfully within the black market without the need to establish trust through sharing, possibly utilizing mechanisms like escrow services to facilitate transactions.

Intermediate figures, such as 'IntelBroker', who has 60% sharing and 40% selling, depict a more balanced approach, combining community engagement with commercial activities.

'Leakbase' also shows a blended model but with a stronger inclination towards sharing (96.55%). The presence of entities like 'markitto35' with a high sharing percentage (98.48%) and a minimal selling record (1.52%) further underlines the diversity in operational tactics among post owners on the dark web.

This diverse operational behavior among the entities underscores the complexity of the dark web's black market. It indicates the existence of varied strategies and mechanisms that enable successful trade, challenging the simplistic view of trust-building through data sharing.

The Ransomware Threat Landscape in the United States

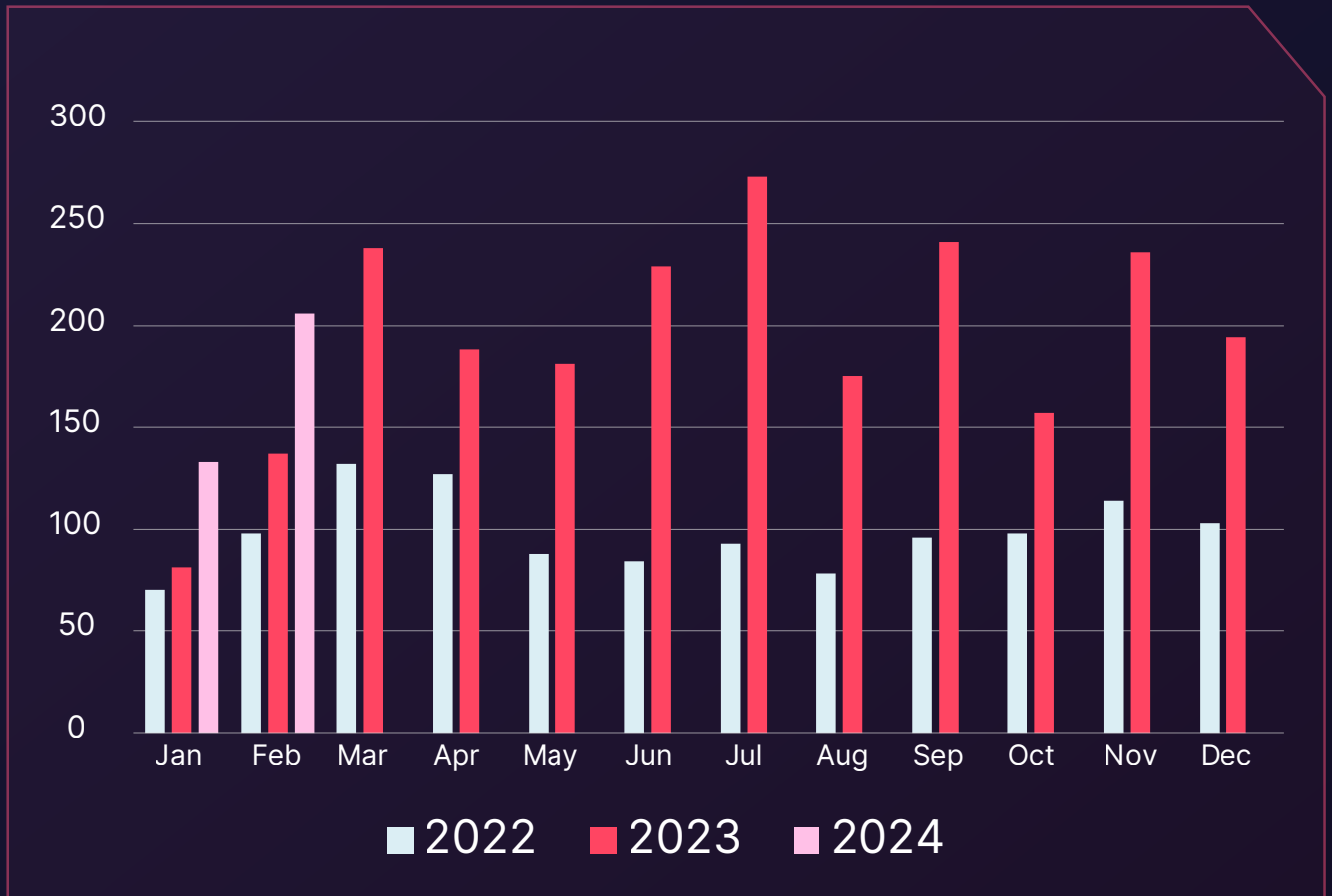
In the shadowy corridors of the cyber underworld, ransomware remains one of the most formidable threats to organizational security, with operators constantly evolving their tactics. This section delves into the ransomware-related discussions that pertain to cyber incidents related the United States, as tracked by SOCRadar's extensive monitoring over the last 26 months, from January 2022 to February 2024.

Our tools and analysts scour leak sites, blogs, and Telegram channels—common platforms for extortion and announcements by ransomware operators. Through comprehensive tagging, we categorize the data by organization, industry, and the country of the mentioned entities. This intelligence is shared within the Ransomware News channel of the SOCRadar platform.

The following subsections will explore the time distribution of these ransomware-related posts, the top industries targeted, the most active ransomware groups, and the types of shares—each within the United States context over the designated timeframe. It is crucial to understand that the data represents the number of mentions, not the actual number of attacks, and some organizations may be referenced multiple times. Consequently, this analysis should be seen as indicative of patterns rather than precise counts of incidents.

Chronology of Ransomware Discourse

▶ Temporal Patterns in Ransomware-Related Mentions



This bar graph depicts the month-by-month frequency of ransomware-related discussions connected to the United States, from January 2022 to February 2024.

Examining the provided data, we observe a notable escalation in the mention of ransomware incidents over the period in question. In 2022, the average monthly mentions hovered around 98.42, but by 2023, this average had almost doubled to 194.17. The first two months of 2024 have seen an even higher average of 169.5, despite the expected decrease in post-peak periods.

A stark increase is particularly evident in February 2024, with 206 mentions, which significantly exceeds any month from the previous years. This could be indicative of a new ransomware campaign or a heightened awareness and reporting of ransomware activities.

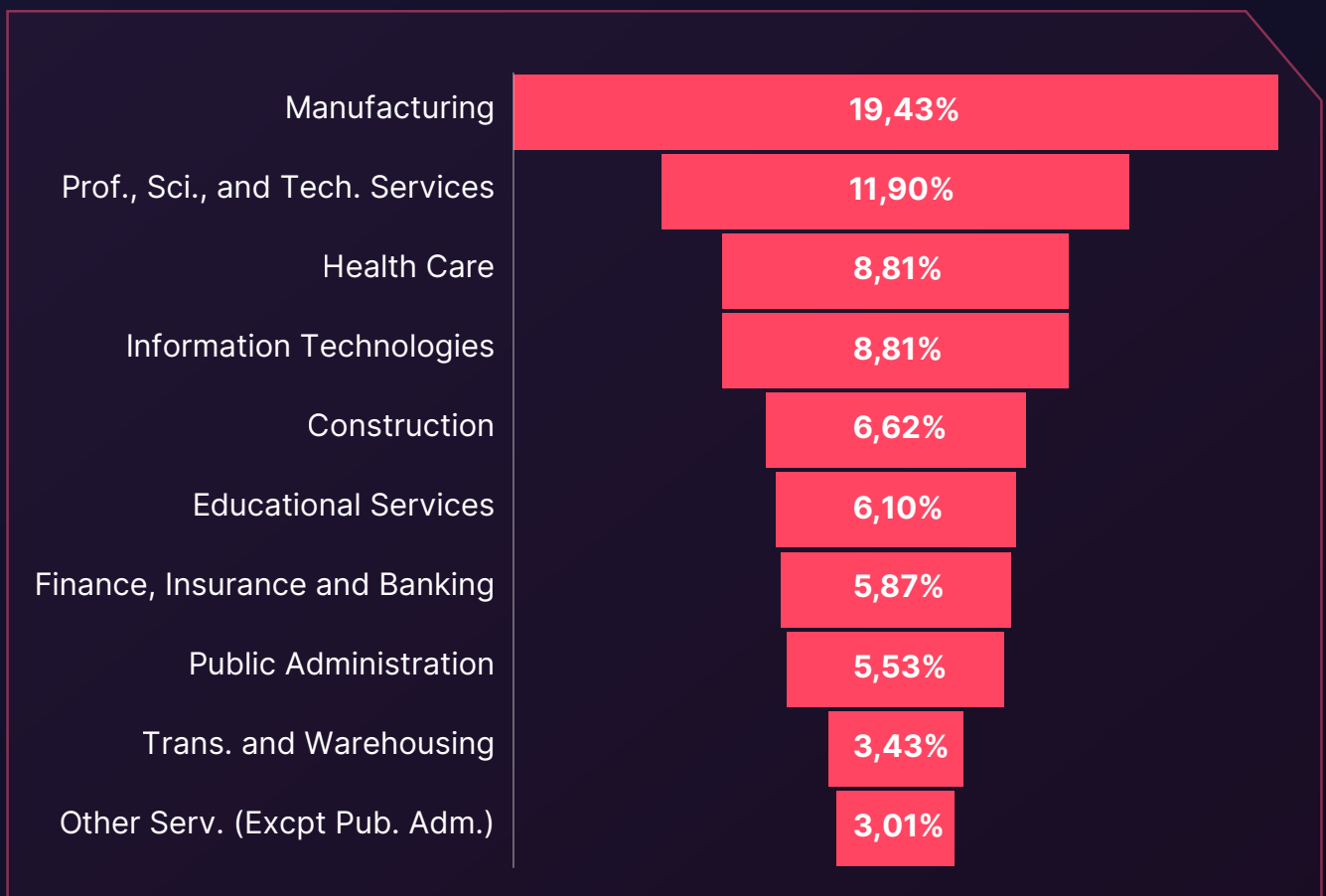
Comparing the dark web (from the previous section) and ransomware post dynamics over the same period, we discern distinct patterns in the frequency and trends of mentions. While the overall volume of dark web mentions pertaining to various cyber threats demonstrates considerable variability, ransomware-specific discussions reveal a clear upward trajectory. This contrast suggests differing operational tempos and possibly diverging interests among threat actors in these two realms.

In the dark web data, the highest concentration of mentions was observed in the latter half of 2023, particularly in November, which might reflect episodic events or campaigns specific to that time. However, in the ransomware discussions, we see a sustained increase across the entirety of 2023, culminating in a sharp rise in early 2024. This sustained growth in ransomware mentions could point to the growing prevalence and concern over ransomware attacks, indicating that they are becoming a more prominent part of the threat landscape, whereas the dark web mentions could be more reactive to specific incidents or trends.

This comparison underlines the importance of distinguishing between the general chatter on the dark web and the targeted conversations around ransomware, as each offers different insights into cybercriminal behaviors and potential threats. Understanding these dynamics is crucial for cybersecurity professionals as they tailor their defensive strategies to the specific nuances of each threat type.

Sectoral Priorities in Ransomware Narratives

► Industry Targets of Ransomware Conversation



Distribution of ransomware-related discussions by industry for the United States from January 2022 to February 2024, indicating which sectors were most frequently mentioned in the context of ransomware threats.

Upon comparing the top industries mentioned in the dark web context with those in ransomware narratives, we observe distinct sectoral focuses. In the ransomware space, the Manufacturing sector is most frequently mentioned, accounting for 19.43% of the discussions. This contrasts with the dark web discussions where Finance, Insurance, and Banking held the lead. The heightened attention towards Manufacturing could be due to the critical nature and interconnected supply chains within this sector, making it a lucrative target for ransomware attacks aimed at disrupting operations and demanding hefty ransoms.

The Professional, Scientific, and Technical Services industry comes second with 11.90%, followed by both Health Care and Information Technologies at 8.81%. These sectors are known for their sensitive data and reliance on uptime, which, if compromised, can have significant implications.

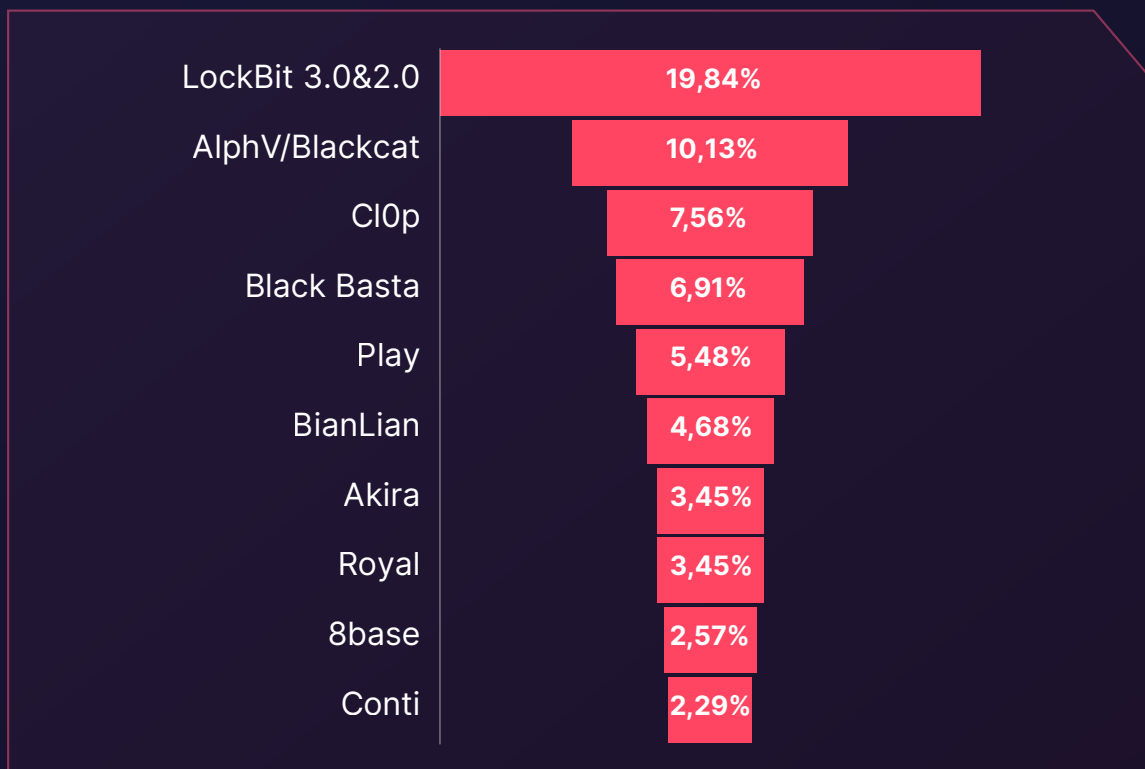
In contrast, sectors like Finance, Insurance, and Banking, which were significantly targeted in dark web mentions, appear less prominently in ransomware discussions with 5.87%, suggesting different operational tactics or threat focuses between the two domains. Public Administration also shows a lower proportion in the ransomware context with 5.53%, hinting at potentially differing security postures or attacker preferences.

The diversity in the targeted industries between dark web news and ransomware news points to a multifaceted threat landscape where threat actors may tailor their strategies according to the perceived vulnerabilities and potential payouts of each sector. This data is crucial for informing industry-specific cybersecurity strategies and defense mechanisms.



Dominance Dynamics of Ransomware Groups

► Prominence of Ransomware Groups



The table categorizes the most active ten ransomware groups targeting the United States by the percentage of mentions in ransomware-related posts from January 2022 to February 2024.

The data illustrates the landscape of ransomware groups that have been most active in terms of their mentions in the United States context. Notably, LockBit takes a significant lead with 19.84% of mentions, showcasing its dominance in the ransomware ecosystem not just in the United States, but globally during the period under review. This prominence can be attributed to the group's persistent activity and perhaps the impact of their operations.

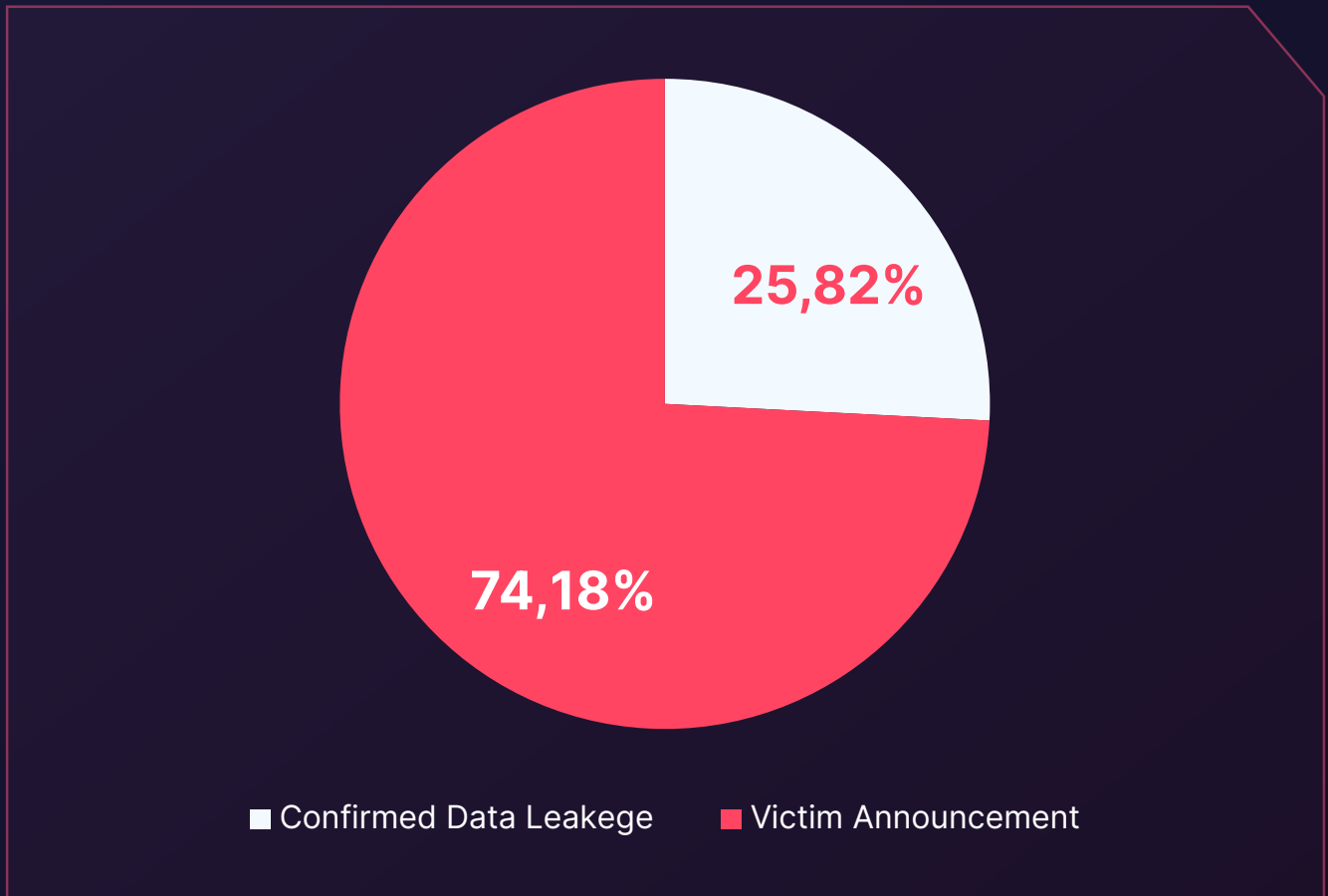
Following are AlphV/Blackcat and Cl0p, with 10.13% and 7.56% of mentions respectively, indicating their substantial but lesser presence compared to LockBit. Black Basta and Play are also among the more frequently mentioned groups, suggesting their active participation in ransomware campaigns during this timeframe.

Lesser-known groups such as BianLian, Akira, Royal, 8base, and Conti round out the list, each with a smaller share of mentions. Their presence reflects a diverse ecosystem of ransomware operators, each contributing to the cyber threat landscape with varying degrees of visibility and impact.

The dominance of LockBit underscores the group's significant role in shaping ransomware threats within the United States, and the necessity for focused cybersecurity measures to counteract this specific threat. The variety of active groups also underscores the complexity and multi-faceted nature of ransomware operations, necessitating comprehensive and adaptable defensive strategies.

Ransomware Operators' Intent

▶ Ransomware Operators' Communication Breakdown



The pie chart illustrates the proportion of ransomware-related posts that either confirm data leakage or make a victim announcement, indicating the operators' intentions in the United States from January 2022 to February 2024.

The data from the graph provides an insight into the intent behind ransomware operators' communications. A significant majority, 74.18%, of the posts are victim announcements, which include naming the organizations targeted by ransomware attacks, as a means of intimidation or a precursor to demanding a ransom.

In contrast, 25.82% of the posts confirm actual data leakage. This smaller proportion suggests that while the threat of data exposure is a common tactic for compelling victims to pay ransoms, the actual act of leaking data publicly is less frequently executed or announced. This could point to the use of data leakage threats as a bargaining chip in ransom negotiations, with the actual release of sensitive information being a last resort or occurring only after other extortion methods have failed.

The disparity between these figures emphasizes the psychological component of ransomware strategies, where the threat of damage is leveraged more than the act itself and underscores the need for robust incident response plans that address both the potential and the actualized risks of data exposure.

Navigating the Cyber Threat Landscape

Key Challenges for US Organizations

The digital era is a double-edged sword, offering vast opportunities for innovation and connectivity, while also presenting an expanding battlefield for cyber threats. As US organizations navigate this intricate landscape, understanding the prevailing and emerging dangers is critical for fortifying defenses and ensuring resilience against cyber adversaries.



Emerging and Persistent Cyber Threats

In recent years, there has been a notable increase in cyberattacks, with adversaries employing more sophisticated methods to exploit vulnerabilities. In 2023, several reports, including the Deloitte Cybersecurity Threat Trends Report and CrowdStrike's 2024 Global Threat Report, have pointed out significant trends and tactics that pose substantial risks to both public and private sectors in the United States.



Stealth and Speed in Attacks

Attackers are employing unprecedented stealth, with reports indicating that the fastest recorded eCrime breakout time was a mere 2 minutes and 7 seconds. This rapidity of attack execution underscores the need for organizations to implement real-time detection and response mechanisms to curb intrusions before they escalate.



Cloud Vulnerabilities

With the surge in cloud adoption, adversaries are increasingly targeting cloud infrastructures. The reports observed a 75% increase in cloud intrusions, with attackers often using valid credentials to fly under the radar, making these breaches particularly challenging to detect.



Identity-Based Threats

Identity threats have surged, facilitated in part by the advent of generative AI, which has enabled more convincing social engineering campaigns. Phishing, SIM-swapping, MFA bypassing, and stolen API keys have become common tactics for initial access. These methods underline the need for robust identity and access management systems.



Supply Chain Compromises

The exploitation of vendor-client relationships and the software supply chain has become a significant vector for attacks, allowing adversaries to maximize their impact by infiltrating multiple organizations through a single entry point.



Generative AI as a Tool for Adversaries

The potential misuse of generative AI technologies by adversaries is raising concerns. AI-driven techniques are not only used in sophisticated social engineering campaigns but are also feared to be instrumental in creating malicious software and tools to conduct more effective attacks.



Global Hacktivism

Amid the escalated conflicts like between Israel and Hamas, the cyber domain has emerged as a new battleground. Hacktivist groups supporting both sides have intensified their cyber activities. Various groups have targeted emergency systems, media outlets, and essential infrastructure with Distributed Denial-of-Service (DDoS) attacks and defacements. There are also reports of disruption claims, although these are often exaggerated. Notable groups like Anonymous Sudan, Cyber Av3ngers, and KillNet have been active, with some tied to state-sponsored activities. The use of cyber tactics reflects a growing trend in modern conflict, where digital disruptions serve as an extension of physical skirmishes.

To combat these threats, organizations are advised to prioritize ransomware prevention, enhance DDoS defense, strengthen access control for insider threat mitigation, secure email servers, and develop strategies to counteract hacktivism.

Control	Result
DNS (Any) Checked	✓ Passed
DNS Recursion	✓ Passed
Zone Transfer	✓ Passed
SlowLoris Checked	✓ Passed

The DoS Resilience Service in the SOCRadar Labs offers the capability to evaluate the resistance of your domain or subnet to DoS attacks, including but not limited to slowloris attacks.

Looking Ahead Cyber Threat Prospects for 2024

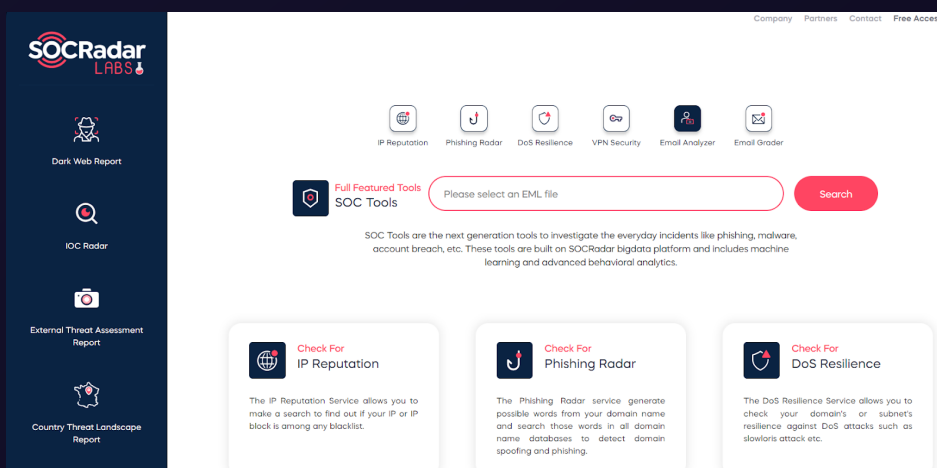
As the United States gears up for the 2024 elections, the cyber threat landscape presents an intricate web of challenges. Past elections, notably in 2020, have been marred by allegations of interference, with cyber tactics like phishing and misinformation campaigns taking center stage. With the emergence of generative AI, these threats are poised to become even more sophisticated, potentially blurring the lines between truth and fabrication to an unprecedented degree.

Generative AI and Phishing The New Frontiers in Election Security

Generative AI stands at the forefront of potential cyber threats to the 2024 elections. Its capacity to create convincing synthetic media, such as deep fakes, can be weaponized to create fraudulent narratives. Coupled with this is the risk of sophisticated phishing campaigns, which can now be turbocharged by AI, making them more personalized and harder to detect. These campaigns could target voters, political campaigns, and even election infrastructure, aiming to steal sensitive information or spread disinformation.

The intersection of generative AI and phishing embodies a critical threat vector. Such technology may be used to impersonate candidates or officials, leading to misinformation that could swing public opinion or undermine the credibility of the electoral process. Acknowledging and preparing for these novel threats is imperative to safeguard the integrity of democratic processes.

As we step into another election cycle, it's crucial to anticipate these potential cyber threats and bolster defenses. This includes educating the public on the risks of deepfakes, reinforcing the security of election infrastructure, and enhancing the ability to detect and respond to phishing attempts. By staying ahead of these advancements, the United States can strive to maintain the sanctity and security of its elections.

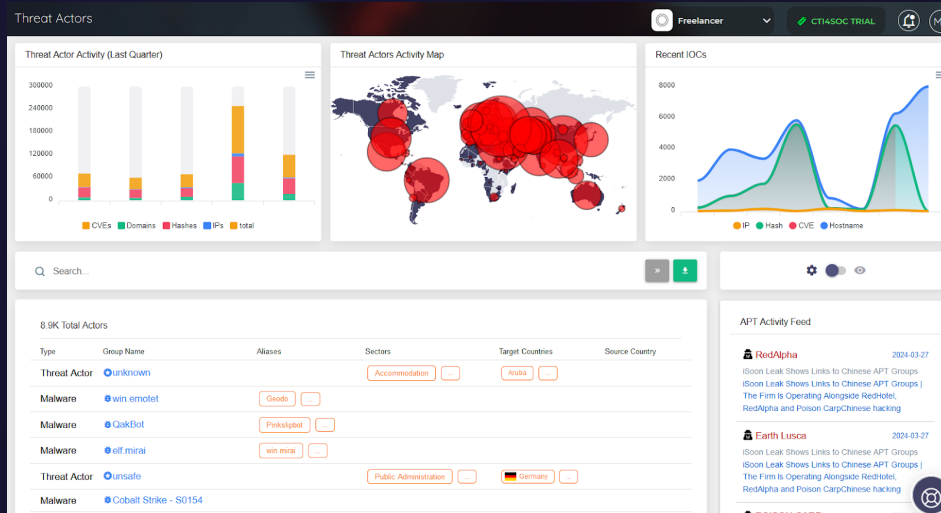


The screenshot displays the SOCRadar Labs website interface. On the left is a dark blue sidebar with the SOCRadar Labs logo and navigation links for Dark Web Report, IOC Radar, External Threat Assessment Report, and Country Threat Landscape Report. The main content area features a header with navigation links (Company, Partners, Contact, Free Access) and a row of service icons: IP Reputation, Phishing Radar, DoS Resilience, VPN Security, Email Analyzer, and Email Grader. Below this is a 'Full Featured Tools SOC Tools' section with a search bar and a 'Search' button. A descriptive paragraph states: 'SOC Tools are the next generation tools to investigate the everyday incidents like phishing, malware, account breach, etc. These tools are built on SOCRadar bigdata platform and includes machine learning and advanced behavioral analytics.' At the bottom, three service cards are visible: 'Check For IP Reputation', 'Check For Phishing Radar', and 'Check For DoS Resilience', each with a brief description of its function.

In the SOCRadar Labs, the Email Threat Analyzer service is available at no cost. It's designed to help determine whether an email might be a scam.

The Rise of Global Hacktivism

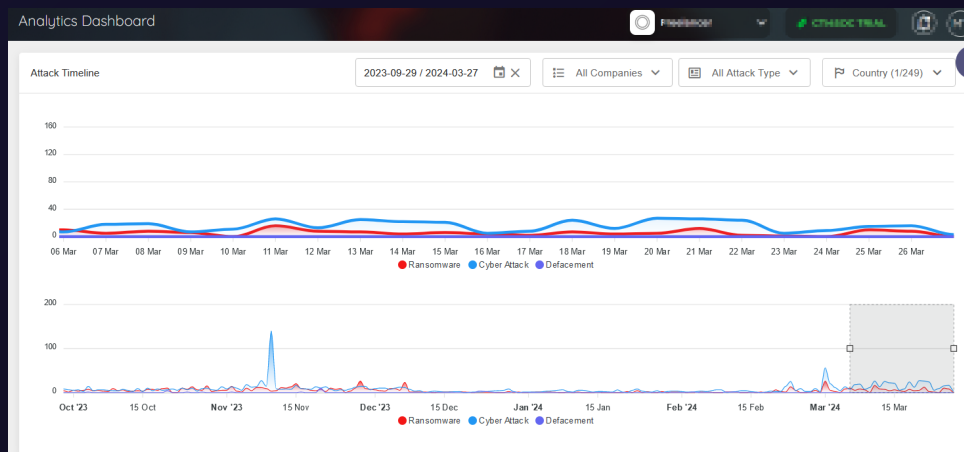
Global hacktivism is expected to rise, with ideological conflicts and international politics driving cyber activists. These digital crusaders are becoming increasingly sophisticated, coordinating attacks that are politically motivated and which can disrupt national and international affairs. With the US elections on the horizon, hacktivist groups might intensify their efforts to push their agendas, targeting political organizations, election infrastructures, and government agencies.



The Threat Actor Module from SOCRadar provides updates on threat actors and malware on a global, local, and industry-specific basis, keeping you informed.

The Threat to Supply Chains

The interconnectivity of the global supply chain presents a tempting target for adversaries seeking to inflict maximum disruption with a single strike. Supply chain attacks have the potential to compromise not just one entity but a multitude of businesses that rely on a single source for software or services. The SolarWinds attack serves as a stark reminder of the vulnerabilities within supply chain networks and the cascading effects that can arise from them. As we advance, the call for fortified supply chain defenses and thorough risk management strategies will be paramount.



In the SOCRadar platform, the Supply Chain Intelligence Analytics Dashboard enables monitoring of your third-party vendors or the entire ecosystem.

Conclusion

As we conclude this comprehensive examination of the cyber threat landscape that has unfolded over the recent years in the United States, it becomes evident that the digital domain remains an arena of high stakes and persistent threats. From the sophisticated ransomware attacks targeting crucial infrastructure to the subtle maneuvers of cyber espionage and the burgeoning risks posed by hacktivism and supply chain vulnerabilities, the landscape of cyber threats is as diverse as it is challenging. This report has not only cataloged significant incidents but also highlighted the evolving nature of cyber threats, underscoring the critical importance of adaptive and robust cybersecurity measures.

In light of these insights, the path forward requires a concerted effort across all sectors—public and private—to fortify defenses, foster cybersecurity awareness, and enhance resilience against the sophisticated tactics of adversaries. As the digital frontier continues to expand, so too must our collective commitment to securing it against the myriad threats that seek to undermine the integrity, confidentiality, and availability of our cyber ecosystem.

In the shadow of these challenges lies the opportunity for innovation, collaboration, and strategic foresight in cybersecurity practices. By learning from past incidents and anticipating future threats, particularly with the advent of generative AI and its implications for misinformation and phishing campaigns, stakeholders can navigate the complexities of the cyber realm with greater confidence and efficacy. As we look to the future, let this report serve as both a reflection on the lessons learned and a clarion call to action for safeguarding our digital world against the ever-evolving cyber threats of tomorrow.

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.

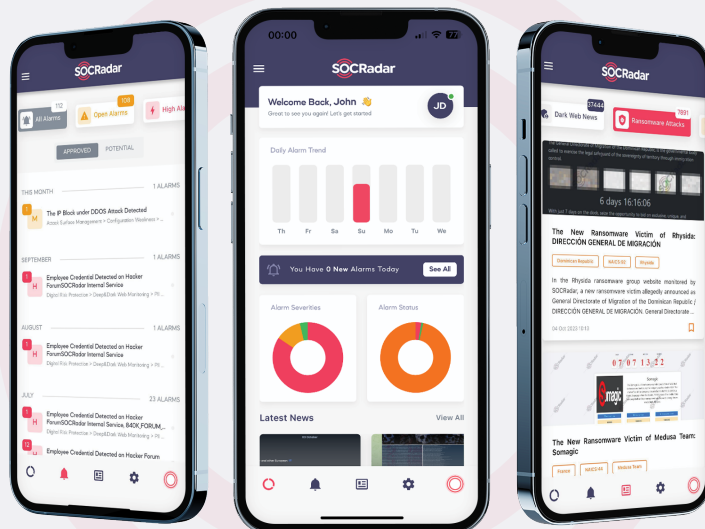
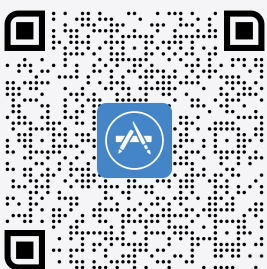
360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

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



socradar.io



Gartner
Peer Insights™

4.8/5
★★★★★