SOCRadar®
Your Eyes Beyond

U.S. DARK WEB REPORT

socradar.io

Table of Contents

Dark Web Mentions and Ransomware Trends

In today's digital age, the vast expanse of the internet houses the information we see daily and a parallel realm known as the dark web. This secretive part of the digital universe is frequently associated with illicit activities, ranging from drug trafficking to cybercrimes. Central to our report's scope are two intertwined aspects: dark web mentions relevant to U.S. entities and the surge in ransomware campaigns against them.

The first section, "Dark Web Radar," provides insights into the frequency with which U.S. industries are discussed on the dark web. These mentions can indicate potential threats, vulnerabilities, or the cyber underworld's interests. They serve as a temperature check, highlighting industries that may be particularly interesting to cyber criminals, from the value of their data to potential weaknesses in their cyber defenses.

In tandem, the second section, "Ransomware Trends," narrows its lens on one of the most formidable cyber threats facing U.S. organizations: ransomware attacks. These are not just cybercrimes; they are targeted, damaging, and often have significant financial implications. By analyzing mentions of ransomware groups targeting U.S. entities and their specific industry preferences, we aim to shed light on the shifting landscape of cyber threats and the industries most at risk.

Together, these sections offer a comprehensive glimpse into the darker corridors of the internet and the looming threats that U.S. organizations must navigate. As we delve into the specifics, stakeholders must remember that awareness and understanding are the first steps in crafting robust defenses against these cyber adversaries.

Executive Summary

This report aims to illuminate the pressing cyber threats from the dark web, focusing on how U.S. industries are perceived and targeted. The hope is that with better insight, organizations can fortify their defenses and stay one step ahead of cyber adversaries.

Dark Web and Ransomware Evolution

- Persistent growth in ransomware mentions on dark web platforms and Telegram channels.
- A sharp increase in 2023 suggests an enhanced focus on targeting U.S entities.

Ransomware Mentions Yearly Comparison:

- **2022:** Total mentions stood at 1,079.
- **Up to September 2023:** Mentions surged to 1,514; a grow th of approximately 40.3%.
- Monthly average mentions in 2022 were 89.92; in 2023, this rose by 87.1% to an average of 168.22.

Target Analysis:

- Ransomware gangs prioritize industries where interruptions lead to immediate financial loss.
- Due to its dependency on continuous operations, manufacturing stands out as a prime target.

Industry Targets Distribution:

- A diverse range of industries, including Professional, Scientific, and Technical Services, Healthcare, Information Technologies, and Education, is on ransomware groups' radar.
- The strategy emphasizes diversity, ensuring many opportunities and points of leverage.

Impact of Freely Shared Data:

- Accessibility to varied datasets on the dark web enables gangs to expand their targeting.
- Detailed organizational insights allow for more sophisticated victim assessment.

Top Ransomware Groups (2022-2023):

- LockBit 3.0 & 2.0 lead with 20.09% (521 posts) of total mentions.
- Other notable groups: AlphVM Blackcat (10.57% or 274 posts) and Cl0p (9.56% or 248 posts).

Ransomware Announcement vs. Data Exposure:

- 71.50% (1,854 posts) were victim announcements, while 28.50% (739 posts) showcased actual data exposure.
- Roughly 40% of the announced victims might not have paid the ransom, restored data from backups, or accepted data loss.

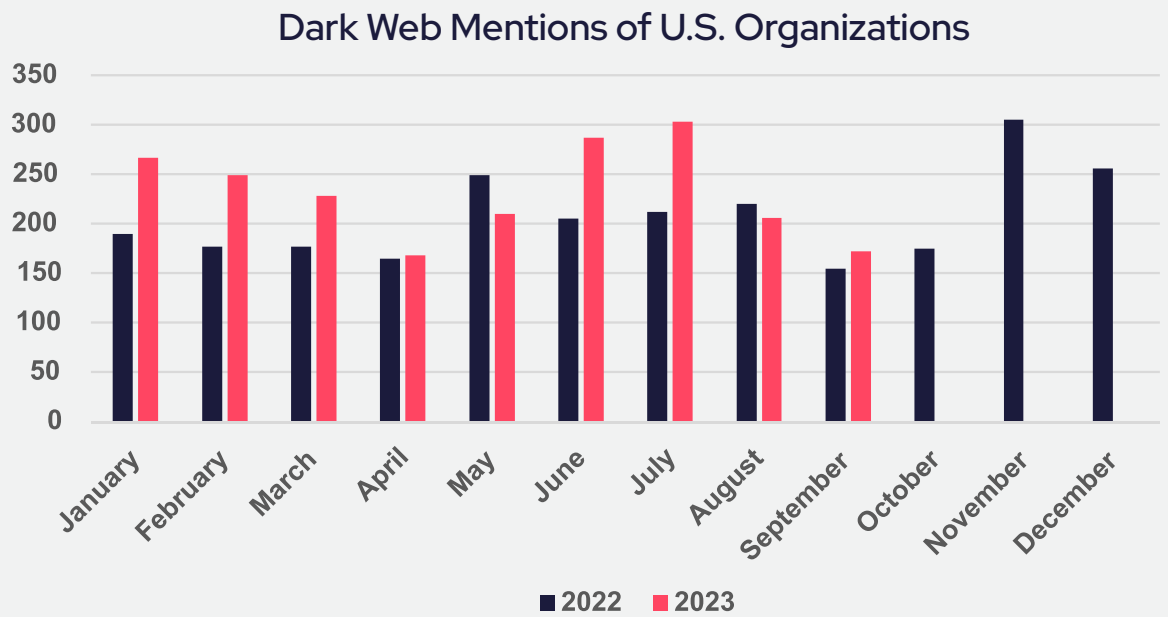
Comparison of Industry Mentions (Dark Web vs. Ransomware Activities):

- Banking, Finance, and Insurance: 16.48% on Dark Web, but only 6.56% in ransomware contexts.
- Manufacturing: Lesser dark web mentions (5.53%) but higher ransomware focus (16.89%). E-commerce is notably mentioned (11.80%) on the dark web but not in the top 10 for
- ransomware.

Dark Web Radar

Dark Web Mentions of U.S. Organizations (2022 - 2023)

As cyber threats continue to evolve and the digital landscape expands, tracking mentions of organizations on the dark web has become an imperative task for security professionals. This data provides a month-by-month breakdown of mentions related to U.S. organizations on the dark web for 2022 and the first nine months of 2023.



Monthly breakdown showcasing the number of mentions related to U.S. organizations on the dark web. The data indicates a rising trend in mentions from 2022 to the first nine months of 2023, emphasizing the need for continuous vigilance.

Total Mentions in 2022: 2,486
Total Mentions in 2023 (Jan-Sep): 2,090
Average Monthly Mentions in 2022: 207.17
Average Monthly Mentions in 2023 (Jan-Sep): 232.22

Insights:
The data highlights several noteworthy trends:

1. **Increase in Monthly Average:** There's a notable increase in the average monthly mentions from 2022 to 2023. While 2022 saw an average of 207.17 monthly mentions, the first nine months of 2023 experienced an average of 232.22 monthly. This suggests a rising interest or heightened activity around U.S. organizations in dark web forums and platforms.

2. **Notable Spikes:** Months like May 2022 and July 2023 witnessed more mentions than the surrounding months. Such irregularities can hint at specific campaigns or events that might have prompted increased chatter.

Dark Web Radar

November 2022

The spike in dark web mentions of U.S. organizations in November 2022 being close to the holiday season certainly presents a potential connection. Here's why:

- *Holiday Shopping & Increased Online Transactions:* The months leading up to the holiday season, especially starting from Black Friday in November, see a surge in online shopping. Threat actors are well aware of this trend and may ramp up their activities to exploit increased online transactions, potentially leading to more mentions and discussions on the dark web.

- *Seasonal Phishing and Scam Campaigns:* During the holiday season, there's an uptick in phishing campaigns and scams that mimic popular shopping sites, charity donations, and delivery notifications. These could increase chatter and exchange of tools, tactics, and data in dark web forums.

- *End-of-Year Activities:* Organizations may be closing their financial books, making more significant financial transactions, or rolling out end-of-year promotions, which can attract the attention of threat actors.

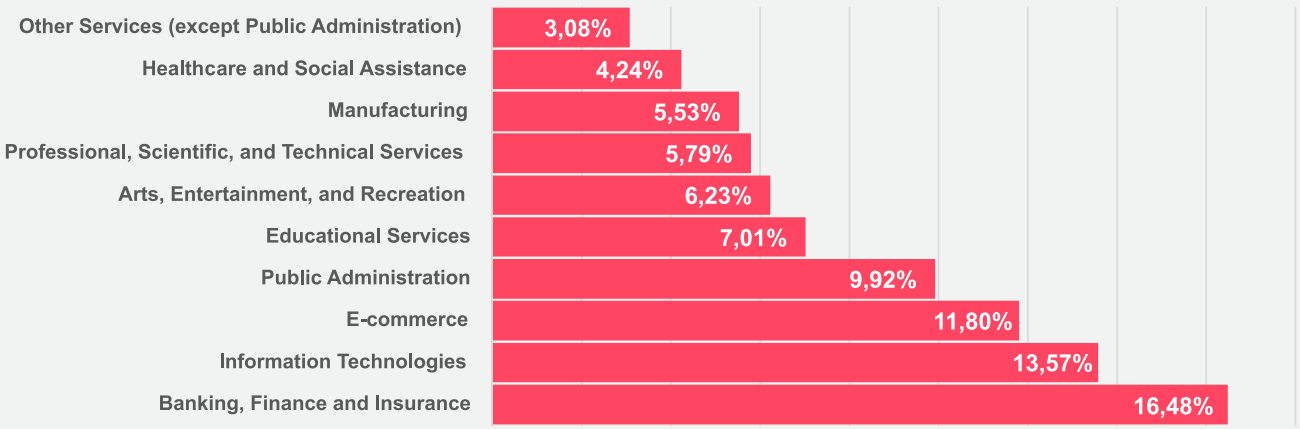
- *Potential for More Vulnerabilities:* With the rush to roll out holiday promotions, companies might hastily deploy software or online platforms, potentially introducing vulnerabilities. Threat actors could discuss these vulnerabilities on the dark web.

While the holiday season's onset could contribute to the spikes in mentions, it's crucial to approach such hypotheses cautiously. Correlation doesn't necessarily imply causation. It would be ideal to further analyze the data, delve into the content of the mentions, and consider other potential external factors to draw a more informed conclusion.

Dark Web Radar

Top 10 U.S. Industries Under the Spotlight

When analyzing dark web mentions by industry, it's crucial to recognize the interconnectedness of today's business world. Many mentions often span multiple industries due to the multifaceted nature of the entities being discussed or the range of their operations.



This chart showcases the volume of dark web mentions across various industries targeting U.S. organizations. Note that some mentions span multiple industries, which may lead to overlaps in the counts. The descending order highlights the industries most frequently discussed, illuminating potential risk areas.

Banking, Finance, and Insurance: Holding the leading position, the Banking, Finance, and Insurance industry represents 16.48% of the total mentions, equating to 754 posts. This prominence isn't surprising given the sensitive nature of financial information and the high data value within this industry. Successful cyber attacks on this industry can yield significant financial gains for threat actors and will likely draw extensive attention within dark web communities.

Information Technologies: Coming in second, the IT industry was mentioned in 13.57% of the posts, summing up to 621. This industry is a pivotal target for cybercriminals due to the vast amount of data and interconnected systems they manage. A breach could open doors to other industries, given the extensive client lists and partnerships IT companies usually maintain.

E-commerce: With the rise of online shopping, especially during recent years, e-commerce platforms have become lucrative targets. The industry holds 11.80% of the total mentions, translating to 540 posts. These platforms handle financial transactions and store vast amounts of personal consumer data, making them tempting targets.

Dark Web Radar

Public Administration: Given the potential for political motives, information leverage, and the vast array of services they provide to the public, it's understandable that Public Administration is mentioned in 9.92% of the posts, which is 454. Successful attacks on public systems can cause disruptions on a large scale, from public utilities to government services.

Educational Services: Institutions under this category, which garnered 7.01% mentions (321 posts), have become increasingly targeted. These entities often handle sensitive information, including research data, personal student records, and financial details, but may lack robust cybersecurity defenses due to budget constraints.

For the remaining industries, like (Arts, Entertainment, and Recreation; Professional, Scientific, and Technical Services; Manufacturing; Healthcare and Social Assistance; and Other Services) each have their vulnerabilities and attractiveness as targets. These industries, despite having varied operations, are interconnected in many ways and often rely on similar technological frameworks. Hence, a breach in one can provide insights or access to others, further emphasizing the need for robust cybersecurity measures across all industries.

It's essential to note the continuously evolving landscape of cyber threats. As specific industries bolster their defenses, threat actors might pivot to what they perceive as weaker targets. This adaptability underscores the importance of a proactive cybersecurity approach for all industries.

Key Observations:

- *Financial and IT Industries Lead the Pack:* The dominance of the Banking, Finance, and Insurance industries, followed closely by Information Technologies, reflects the potential gains and impacts of these industries. Their data-rich environments make them prime targets.

- *Diversity in Targets:* The range of industries, from E-commerce to Arts and Telecommunications, indicates a broad spectrum of interests among threat actors. This could be attributed to diverse motives, from financial gains to data theft or geopolitical reasons.

- *Multiplicity of Tags:* The data considers discussions that might have been labeled under single or multiple tags. This reflects threats' complexity and multifaceted nature, where a single mention might pertain to various industry vulnerabilities.

Considering these findings, U.S. organizations across all industries must prioritize cybersecurity. It's evident that no industry is exempt from the interest of dark web users, so a proactive approach to threat intelligence is crucial.

Dark Web Radar

Analysis of Mentioned Purposes in the Dark Web: 2022 vs. 2023

In examining the purpose of mentions related to U.S. organizations within dark web forums and channels, we tag the post with distinct categories to provide insights into the activities and intentions of threat actors.

Purpose	2022	2023
Buying	1.17%	0.00%
Hack Announcement	0.36%	1.44%
Partnership / Cooperation / Offer	0.56%	0.14%
Selling	57.04%	49.67%
Sharing	40.83%	48.61%
Target Attact	0.04%	0.14%

Distribution of Purposes for Mentions in the Dark Web (2022 – 2023). The data for 2023 is available only for the first nine months.

Analyzing the purposes for which U.S. organizations were mentioned in dark web forums and channels in 2022 and 2023, several trends are notable.

- *Selling Activity:* The predominant category, mentions related to selling, experienced a decrease in 2023, going from 57.04% to 49.67%. One plausible explanation for this decrease could be the saturation effect of the rise in shared data. As more information becomes free, the uniqueness and value of data available for sale can diminish, thus reducing selling activity.

- *Sharing Activity:* Sharing-related mentions, on the other hand, saw a slight increment, moving from 40.83% in 2022 to 48.61% in 2023. The surge in sharing could potentially contribute to market saturation, where an abundance of freely available information reduces the demand for purchased data.

- *Hack Announcements:* A significant uptrend was observed in hack announcements, growing fourfold from 0.36% in 2022 to 1.44% in 2023. Despite the relatively low overall numbers, this increase indicates a growing inclination towards publicly declaring hacks or breaches.

Dark Web Radar

- *Buying Activity:* There's a notable cessation of buying activity in 2023. This could be interpreted in several ways. Given that a considerable amount of data is being shared freely, it might render buying redundant for many users. Why purchase data when a vast amount is being shared for free and selling activity is also high?

  Furthermore, this could indicate a higher degree of self-sufficiency among dark web users, who might now have the tools and resources to obtain the data they need without relying on purchases. It might also hint at a decreased trust in buying data, perhaps due to concerns about the quality, relevance, or authenticity of data being sold. Moreover, the decline in both selling and buying could compel sellers to scout for fresh markets. The recent sightings of some threat actors on the clear web might serve as an early indication of this transition.

- *Partnership and Target Attack:* These categories exhibited minor variations between the two years. The relatively low percentages in "Partnership/Cooperation/Offer" and "Target Attack" are noteworthy, with the latter suggesting that even a slight presence of targeted attacks can bear considerable consequences.

The insights provided by this data, even though limited to the first nine months of 2023, offer a valuable perspective into the evolving dynamics and patterns of mentions of U.S. organizations on the dark web. The observed trends underscore the importance of continual vigilance and adaptive strategies to address the shifting nature of threats from dark web activities.

Dark Web Radar

Active Post Owners in 2023: An Analysis of Dominant Behaviors

When we delve into the top active post owners of 2023, a distinct pattern emerges:

Post Owner	Posts	Activity Type	Content Focus
Chucky	106	Sharing	Data/Database
nixploiter	86	Selling	Access
Osiris	52	Sharing	Data/Database
FentanylTroia	52	Selling	Data/Database

Top Active Post Owners in 2023: Activity Type and Content Focus.

The data shows that sharing activities, especially those related to databases and data sets, dominate the list of top contributors. While selling is not absent from the top ranks, it's considerably less frequent when compared to sharing.

The Sharers vs. Sellers Dichotomy:

A notable observation is the prevalence of consistent identities among sharers when we look at top posters. This can be attributed to the desire of these actors to build reputation and credibility within the dark web communities. A good reputation as a sharer can lead to increased trust, more followers, and even potential collaboration or information exchanges with other actors.

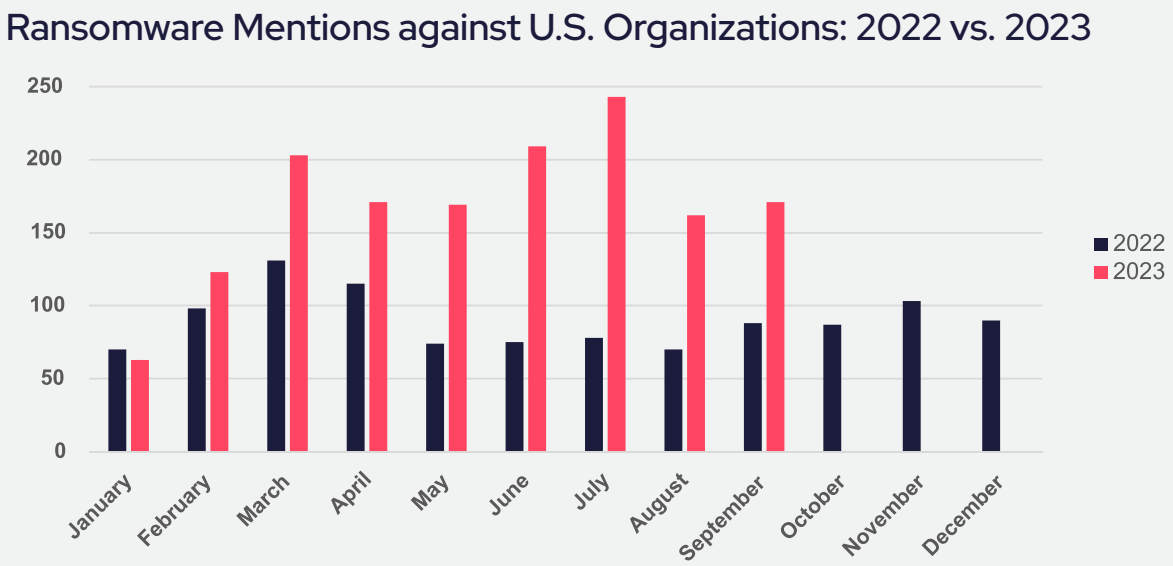
On the flip side, the dynamics for sellers seem to be fundamentally different. Given the heightened risks associated with selling, especially items or services that attract significant legal attention, sellers may adopt strategies to mitigate these risks. One such strategy could be the use of multiple pseudonyms or aliases. By continuously changing their online identity, sellers make it more challenging for law enforcement and cybersecurity researchers to profile or track their activities.

However, comparing the average posts per owner, there's a minimal difference (2.13 vs. 2.10). It appears only the pack leaders adopt a distinct strategy.

Ransomware Trends

Ransomware Mentions: An Analysis of Trends

The dark web, a nefarious component of the digital realm, is persistently evolving. With a focused lens on ransomware groups targeting private and public U.S. organizations, the data extracted from mentions on the groups' websites and Telegram channels paints a disturbing picture of the cyber threat landscape.



This bar graph illustrates the month-by-month mentions of ransomware groups targeting U.S. entities on the dark web, highlighting a concerning uptick in 2023.

Yearly Comparison

Even with 2023 not yet concluded, the mentions of ransomware groups targeting U.S. entities show a marked escalation.

- **Total Mentions:**
  2022 witnessed a total of 1,079 mentions.
  By September 2023, this number had already touched 1,514, representing an increase of about 40.3% from the previous year.

- **Average Monthly Mentions:**
  For 2022, the monthly average was 89.92 mentions.
  In contrast, the average for the first nine months of 2023 stands at a significantly higher 168.22, indicating an 87.1% growth.

Implications and Interpretations

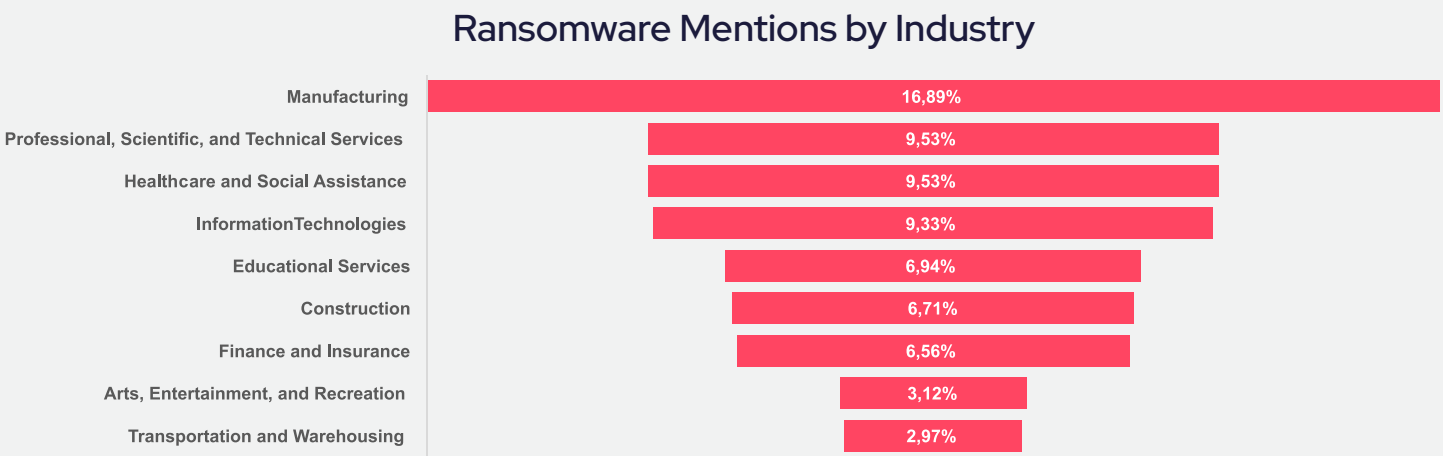
The evident uptick in mentions of ransomware groups on the dark web suggests several alarming possibilities: an enhanced interest in targeting U.S. organizations, more significant collaboration amongst groups, or a higher rate of successful cyber attacks. Entities in the U.S. should bolster their cyber defenses in response to this emerging data.

Moreover, the consistent escalation in the initial months of 2023 might signify a more systematic and concerted effort among ransomware groups. While there seems to be a moderate decline post-July, it's still premature to ascertain if this trend will continue or shift in the remaining months.

Ransomware Trends

Ransomware Targets: A Focus on Operational Continuity

A defining pattern emerges when assessing the industries most frequently targeted by ransomware gangs – emphasizing operational continuity. Particularly, industries where a brief halt in operations can lead to substantial financial losses are at the top of the list. This criterion elucidates the particular focus on the manufacturing industry. When production ceases, even momentarily, companies start to bleed funds, intensifying the urgency to address the ransomware situation.



The graph highlights the percentage distribution of ransomware mentions by industry on dark web platforms and Telegram channels. It emphasizes the strategy of ransomware gangs to target industries where operational continuity is paramount.

Beyond manufacturing, the diversity of industries on ransomware gangs' radar is worth noting. The Professional, Scientific, and Technical Services industry, with a 9.53% mention rate, underscores the digital dependency and wealth of sensitive data inherent to these fields. Breaching such industry can provide a ransomware gang with data of high intrinsic value and the potential for reputational leverage against victimized entities.

The Healthcare and Social Assistance industry are an equally significant target. The sensitivity and critical nature of healthcare data, coupled with the life-saving operations these institutions carry out, make them desirable marks. Any disruption to healthcare operations can be a matter of life and death, giving ransomware gangs a potent hand to play in negotiations.

Information Technologies isn't just the backbone of many modern operations but also a meta target. Successful attacks against IT companies can open the doors to many other victims relying on the IT provider's services or products.

While perhaps less immediately intuitive as targets, Educational Services and Construction have their own vulnerabilities. Campuses are ripe with personal data, research, and intellectual property, while construction operations depend highly on timelines; any disruption can result in contractual penalties and lost revenue.

The remaining industries, from finance to transportation, underline a broader strategy: diversity. Ransomware gangs diversify their targets to ensure consistent opportunities and leverage points. No industry is genuinely safe; the approach is multifaceted and ever-evolving, with an evident focus on exploiting each industries' unique vulnerabilities and operational pressures.

Ransomware Trends

Impact of Freely Shared Data on Ransomware Targets

The proliferation of freely shared data on the dark web may be a significant factor in the diverse target selection of ransomware groups. With a rich and varied dataset at their fingertips, cybercriminals can perform more sophisticated target assessments, identifying potential vulnerabilities across various industries. This accessibility to such data allows ransomware groups to cast a wider net, ensuring they always have a pipeline of potential victims.

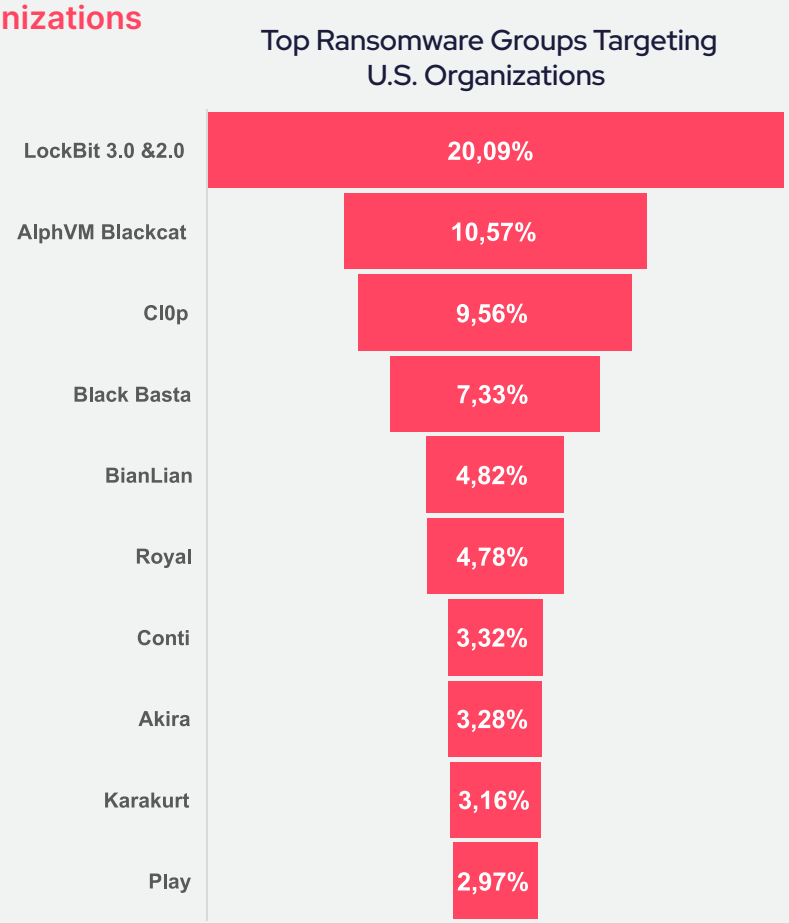
The data can offer insights into an organization's financial capacity and operational vulnerabilities and highlight lucrative connections that can be exploited. For instance, if an IT firm's data reveals links to several major clients in various industries, this could make the IT firm a more attractive target since breaching it could provide a gateway to multiple victims. Similarly, suppose a manufacturing company's data uncovers that they have contracts with government entities or large corporations. In that case, it might become a priority target due to the potential for high ransom payouts.

Thus, while operational continuity and the potential for immediate financial loss (like in the manufacturing industry) remain strong motivators for ransomware gangs, the easy availability of varied data sets further widens their horizon, pushing them to diversify their attacks even more. This diversity increases their chances of a successful breach and amplifies their potential payoff, making every industry, regardless of its nature, a potential target.

Ransomware Groups Targeting U.S. Organizations

The complexity of the dark web means that many ransomware groups actively operate and target organizations of various sizes and industries. The data for 2022 and the first nine months of 2023 reveals the top 10 ransomware groups that have displayed a significant focus on public and private U.S. organizations. In total, there have been 2,593 posts made by these groups concerning U.S. entities

Top Ransomware Groups Targeting U.S. Organizations (2022-2023). A comprehensive breakdown of the leading ransomware groups targeting U.S. organizations from 2022 to September 2023, based on the number of their mentions and posts.



Ransomware Trends

LockBit 3.0 & 2.0 takes the lead, accounting for an impressive 20.09% (521 posts) of the total mentions. The prevalence of this group highlights its aggressive campaign against U.S. organizations. Its successor and predecessor versions seem to be involved in this targeting, suggesting a consistent and determined approach to victimizing entities in the region.

AlphVM Blackcat follows with 10.57% (274 posts) of the mentions, solidifying its position as another significant player in the cyber underworld regarding ransomware attacks on U.S. soil. The third on the list is **Cl0p,** capturing 9.56% (248 posts) of the mentions. Their activity underscores a strategic focus on the U.S. as a profitable region for their ransomware operations.

Other groups like **Black Basta** and **BianLian** also mark their significant presence with 7.33% (190 posts) and 4.82% (125 posts), respectively. The diversity in the list, with groups like **Royal, Conti, Akira, Karakurt,** and **Play** also making appearances, reflects the wide-ranging threats that U.S. organizations face. These groups collectively underscore the immense cyber threat landscape and the dynamic nature of ransomware campaigns against U.S. entities. Implications and Analysis

The consistent and dedicated focus of these groups on U.S. targets indicates some organizations' perceived profitability and potentially weaker cyber defenses. It is also worth noting that the diversity in target selection might be influenced by the freely shared data observed in the previous sections of this report. This emphasizes the need for organizations to continuously enhance their cybersecurity posture, maintain awareness of the current threat landscape, and implement proactive measures to mitigate such threats.

Ransomware Trends

Ransomware Attack Announcements vs. Data Exposure

In the period from 2022 to September 2023, there were a total of 2,593 posts by ransomware groups concerning U.S. organizations. Among these, a striking disparity is observed between two types of shares: victim announcements and data exposures.

Victim announcements, wherein cybercriminals publicly acknowledge their successful infiltration of an entity, make up a significant portion, accounting for 71.50%, or 1,854 posts. Conversely, posts showcasing actual data exposures — where sensitive or proprietary information is unveiled — constitute 28.50% or 739 posts.

This data allows us to draw some preliminary inferences about victim behavior following a ransomware attack. Making a careful and rudimentary estimation, if we were to view the 1,854 victim announcements as a rough representation of the total number of victims (with the understanding that the actual number might be higher, given that some victims might negotiate directly without a public post or might convince the ransomware groups to retract the posts), and juxtapose this with the 739 data exposure instances, it suggests that nearly 40% (calculated as 100% x 739/1854) of the announced victims potentially did not yield to the ransom demands. This could mean that these organizations either managed to restore their data from backups, sought assistance from law enforcement or cybersecurity firms, or accepted the loss and did not pay the ransom.

However, it's important to underscore the speculative nature of this analysis. Many factors can influence a victim's decision to pay, including the criticality of the exposed data, the organization's cyber insurance policy, and the amount of the ransom demand, among others.

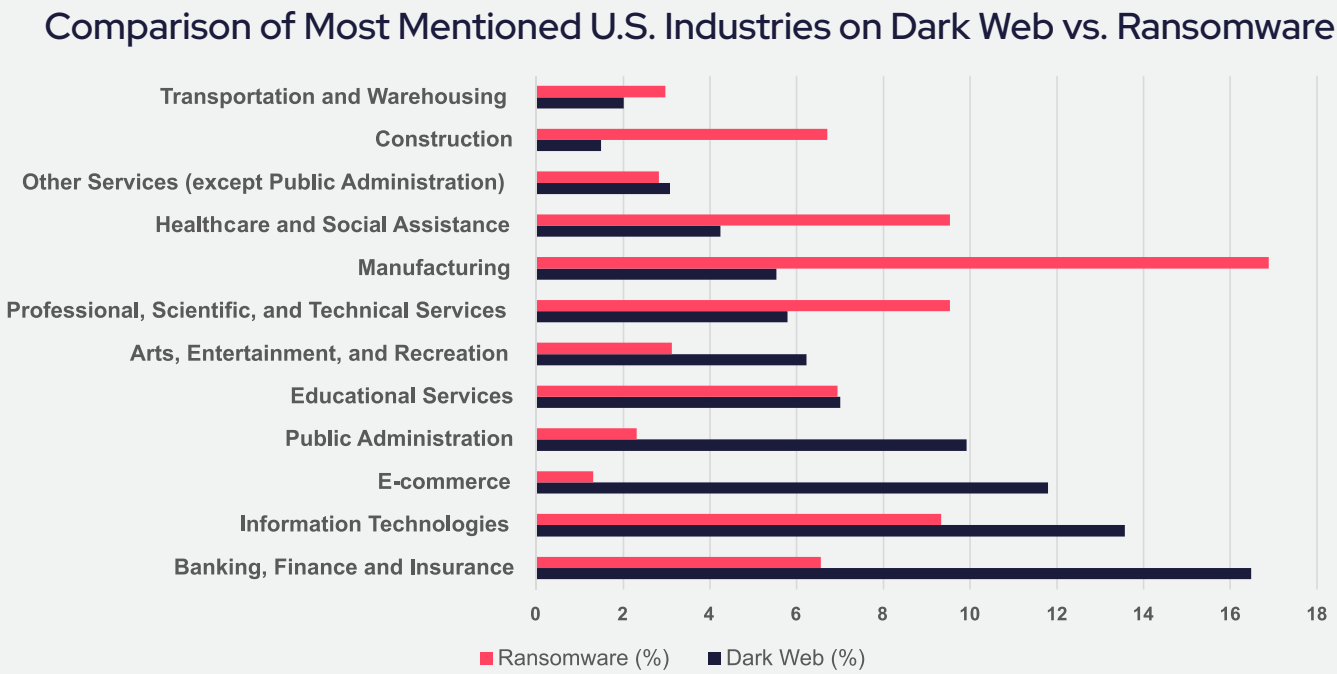
Ransomware Share Types (Jan 2022 - Sep 2023)

Share Type	Percentage	Number of Posts
Data Exposed	28.50%	739
Victim Announcement	71.50%	1,854

A breakdown between ransomware groups' victim announcements and actual data exposure posts, revealing insights into victim responses post-compromise.

Ransomware Trends

Comparison of Industry Mentions: Dark Web vs. Ransomware Activities (2022-2023)



This chart contrasts the frequency of mentions of various U.S. industries on the Dark Web with those specifically in ransomware contexts from 2022 to 2023.

Ransomware Share Types (Jan 2022 - Sep 2023)

1. **Banking, Finance and Insurance:**
   - *Dark Web:* 16.48%
   - *Ransomware:* 6.56%
   - *Observation:* The Banking, Finance, and Insurance industry is frequently mentioned on the dark web. The strict regulations requiring more backups in this industry might make it more resilient against ransomware attacks and long negotiations. As a result, ransomware groups might find it less appealing compared to other industries, such as manufacturing.

2. **Information Technologies:**
   - *Dark Web:* 13.57%
   - *Ransomware:* 9.33%
   - *Observation:* The IT industry is significantly mentioned in both contexts, indicating its vulnerabilities and potential value for general dark web activities and ransomware operations.

3. **Manufacturing:**
   - *Dark Web:* 5.53%
   - *Ransomware:* 16.89%
   - *Observation:* While Manufacturing is not as predominantly mentioned on the dark web, it tops the list in the context of ransomware. As discussed earlier, the need for operational continuity in this industry may make it an attractive target for ransomware groups.

Ransomware Trends

4.Public Administration:
- *Dark Web:* 9.92%
- *Ransomware:* Not in the top 10
- *Observation:* This industry has significant mentions on the dark web, but it's not a primary target for ransomware groups, indicating different types of threats prevalent for this industry.

5. Educational Services:
- *Dark Web:* 7.01%
- *Ransomware:* 6.94%
- *Observation:* Educational institutions are consistently targeted, probably due to the valuable data they possess and potential vulnerabilities in their systems.

6. Arts, Entertainment, and Recreation:
- *Dark Web:* 6.23%
- *Ransomware:* 3.12%
- *Observation:* This industry, while relevant, does not seem to be a primary target for ransomware groups, suggesting other forms of cyber threats or general interest.

7. Professional, Scientific, and Technical Services:
- *Dark Web:* 5.79%
- *Ransomware:* 9.53%
- *Observation:* This industry has a considerable focus in the ransomware context, possibly due to the high-value data and intellectual property they might possess.

8. Healthcare and Social Assistance:
- *Dark Web:* 4.24%
- *Ransomware:* 9.53%
- *Observation:* The health industry, vital for public welfare, sees a heightened focus from ransomware groups, likely due to the critical nature of their operations.

9. E-commerce:
- *Dark Web:* 11.80%
- *Ransomware:* Not in the top 10
- *Observation:* E-commerce has significant mentions on the dark web, indicating a diverse set of threats but not specifically from ransomware.

10. Other Services (except Public Administration):
- *Dark Web:* 3.08%
- *Ransomware:* 2.82%
- *Observation:* This broad category sees a consistent but lower mention in both contexts.

Ransomware Trends

11. Construction:

- *Dark Web:* Not in the top 10
- *Ransomware:* 6.71%
- *Observation:* The construction industry doesn't prominently in general dark web mentions. However, it is a notable target for ransomware groups, indicating industry-specific vulnerabilities or perhaps the value of business disruption in this industry.

5. Transportation and Warehousing:

- *Dark Web:* Not in the top 10
- *Ransomware:* 2.97%
- *Observation:* Like the construction industry, Transportation and Warehousing don't seem to have widespread mentions on the dark web. Yet, they make it to the ransomware list, suggesting that while the industry might not be a hotbed for diverse cyber threats, it remains on the radar for ransomware attackers, possibly due to logistical importance and the cascading impact of disruptions.

The focus of dark web and ransomware-specific mentions varies, underscoring the importance of understanding industry-specific threats. While some industries are universally targeted due to their inherent value, others may be more attractive to specific types of cybercriminals or based on current trends and opportunities in the cybercrime landscape.

Conclusion

The landscape of ransomware activities has seen significant growth, particularly in 2023, with a pronounced focus on U.S. entities. This growth is facilitated by the abundant availability of diverse datasets on the dark web, providing malicious actors with strategic information to tailor their attacks. While ransomware gangs display a diverse range of target industries, there's a clear emphasis on those where operational interruptions yield immediate financial implications, like manufacturing. Interestingly, while specific industries like e-commerce are frequently mentioned on the dark web, they do not correlate with the top ransomware targets, indicating varied interests and agendas within the darker corners of the internet. Understanding these shifting dynamics is paramount for organizations looking to bolster their cyber defenses as ransomware continues to evolve.

Who is SOCRadar®?

Your Eyes Beyond

As an Extended Threat Intelligence (XTI) platform and inventor of the concept, SOCRadar's approach effectively integrates Threat Intelligence, Digital Risk Protection, and External Attack Surface Management (EASM). Adapting proactive security with a hacker mindset, we aim to help security teams to detect blindspots before attackers.

The shortage of cybersecurity experts is a growing problem worldwide. All companies around the world must use resources efficiently to provide adequate cyber security with their limited resources. Automated security solutions offer precisely the opportunity that corporations are looking for. With its AI-powered automation technology. **With providing protection against threats for more than 12.000+ companies from 157 countries, SOCRadar has become an extension of SOC teams from every industry.**

SOCRadar provides extended cyber threat intelligence (XTI) that combines: **"Cyber Threat Intelligence, Digital Risk Protection, and External Attack Surface Management Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

12.000
Free Users

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 12 MONTHS FOR FREE

Gartner Peer Insights. Customer First

Gartner Peer Insights™ 4.9/5 ★★★★★

Contact Us info@socradar.io +1 (571) 249-4598 651 N Broad St, Suite 205, Middletown, DE 19709