RANSOMWARE REPORT

Ransomware Readiness: How SMBs Can Prepare for the Rising Threat of Ransomware-as-a-Service, Initial Access Brokers, and Credential Theft

January 2024

eSENTIRE
Threat Response Unit

Executive Summary

Over the past several years, ransomware has evolved from straightforward “smash-and-grab” type attacks to complete dominance of the victim network, often resulting in network-wide encryption of files and systems. Accomplishing this takes time and resources but can yield far greater payouts from victims.

The modern ransomware landscape relies on a criminal “gig” economy to enable and scale cyberattacks. These services include malware obfuscation or encryption, certificates, malware-as-a-service, credentials, footholds within networks, and Ransomware-as-a-Service (RaaS) such as Lockbit.

For threat actors, including amateur actors, underground forums and IM channels provide plenty of opportunity (given the emergence of Ransomware-as-a-Service and affiliate business models) for entry into networks or high-value account credentials.

Unfortunately for network defenders, this has widened the scope of possible entry vectors they need to anticipate and defend. For example, consider the following scenarios:

1. Information stealing malware on an unmanaged system with enterprise credentials.
2. N-day vulnerability on edge device exploited prior to patching.
3. Employee’s VPN credentials are phished and the account isn’t enrolled in MFA.
4. Internet-facing RDP server compromised with password spray attack.
5. A user installs a stealthy RAT masquerading as legitimate software on a managed system.
6. Credentials and MFA tokens/cookies stolen using an Adversary-In-The-Middle (AiTM) phishing attack, allowing for MFA bypass.

Each scenario presents an opportunity for a threat actor to monetize credentials or network access. In most cases, these scenarios are opportunistic, meaning they are generally untargeted. However, the risk increases substantially when the undetected access granted by these attacks is used or sold.

As organizations improved their resilience to encryption attacks, adversaries began exploring a second extortion method: data theft and leak. This method involves stealing data prior to encryption, then threatening the release of data online. Non-payment often results in the publication of some, or all, of this data online as punishment.

In this report, we take the outside-in approach and examine the exposure ransomware victims had on underground forums and chats where access and credentials are traded. We look at victim attributes from public leak sites, then we expand this to two key markets used by adversaries to buy their way in: Initial Access Broker (IAB) auctions and credential shops and leaks.

Lastly, we also explore the business attributes of publicly known victims to answer questions, such as:

- What industries are most susceptible to ransomware attacks?
- What size of business, based on revenue and employees, are most susceptible?
- What ransomware groups pose the greatest risk?

Ransomware Victims: Who Is Affected?

Key Findings:

- Based on the data, most ransomware victims fit the criteria for small and medium-sized businesses (SMBs) by revenue and employee count.
- Manufacturing, Business Services, and Retail are the top affected industries between 2020 - 2023.
- Since 2020, the biggest cyber threat has been Lockbit, particularly for SMBs. Lockbit is a prolific Ransomware-as-a-Service (RaaS) threat that uses affiliates for attacks, making it challenging for organizations to anticipate multiple attack vectors.
- Compromised credentials pose a significant risk where remote access services aren't monitored or defended.

Ransomware has traditionally operated on a model of opportunistic extortion, with attackers casting a wide net to ensnare individual victims for one-time payments. However, the threat landscape has evolved significantly. Through the increasing use of Ransomware-as-a-Service (RaaS), we've witnessed the emergence of a more organized, business-like approach to these attacks so cybercriminals can maximize disruption and ransom potential.

Unfortunately, ransomware-as-a-service lowers the entry point for amateur threat actors to deploy ransomware. By essentially renting the malware (and **intrusion playbooks**), they can launch sophisticated cyberattacks that are scalable and often more devastating. This model has democratized the ability to execute ransomware campaigns, leading to a surge in both the frequency and sophistication of attacks, with profound implications for cybersecurity defense strategies.

Our Threat Response Unit (TRU) conducted threat research to analyze the relationship between an organization's annual revenue, industry, and number of employees and the likelihood of a ransomware attack. This data stems from publicly known victims listed on so-called "name-and-shame" sites operated by various ransomware groups between 2020 and 2023.

Figure 1 below shows the count of total ransomware victims based on their revenue.

The majority of ransomware victims were companies earning between $1 million and $25 million USD in annual revenue. Companies with annual revenues of $25 million to $50 million USD, $50 million to $100 million USD, $100 million to $250 million USD, and $250 million to $500 million USD round out the top five.

In total, between 2020 to 2023, organizations with revenue up to $500 million USD accounted for 77% of the victims in our dataset.

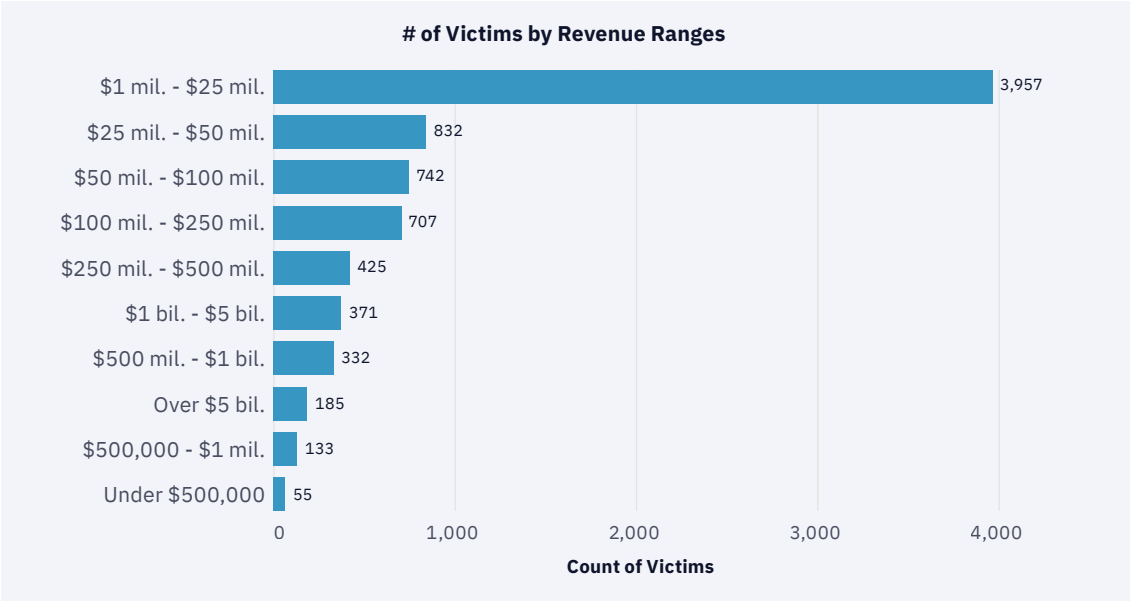

Figure 1: Ransomware victims named on leak sites, broken down by victim revenue.

Our data also shows historical trends indicating small-medium businesses (SMBs) that fall within the $1 million to $25 million USD revenue range are more susceptible to ransomware threats (Figure 2).

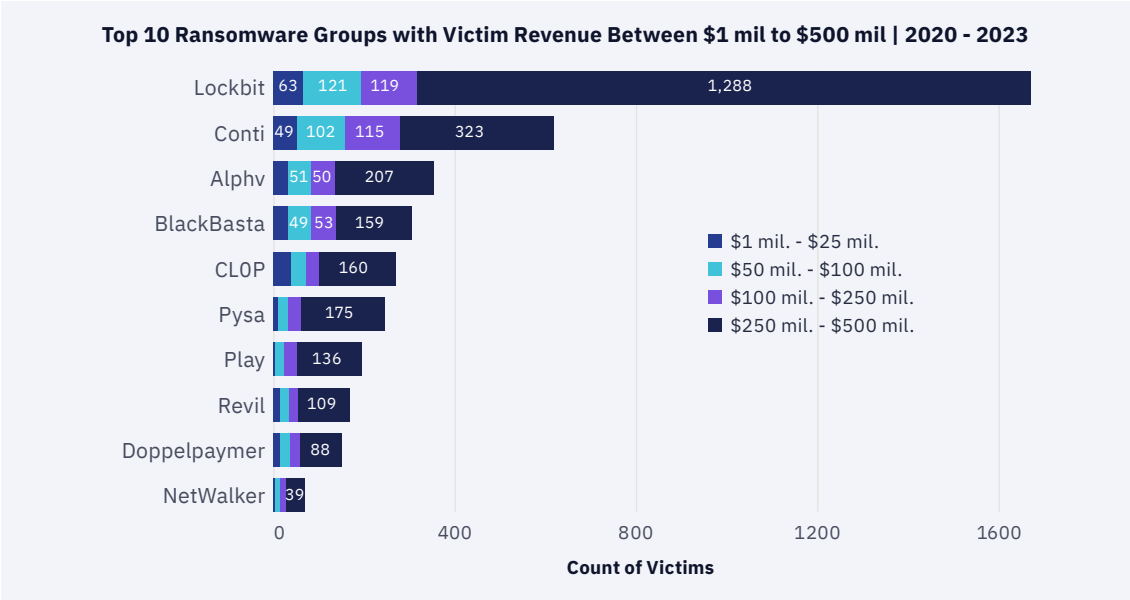

Figure 2: Top 10 ransomware groups targeting victims with revenue of $1 million - $500 million USD (2020 to 2023).

Our data shows that Lockbit is the most significant threat, followed by Conti, Alphv/BlackCat, and BlackBasta. In fact, in a June 2023 U.S. Cybersecurity and Infrastructure Security Agency (CISA) **security advisory**, the FBI estimated that between January 2020 and June 2023, the LockBit gang launched 1,700 attacks against U.S. organizations, many in critical infrastructure sectors.

Narrowing this view down to 2023, Lockbit continues to dominate followed by BlackBasta, Play, Alphv and CL0P (Figure 3).

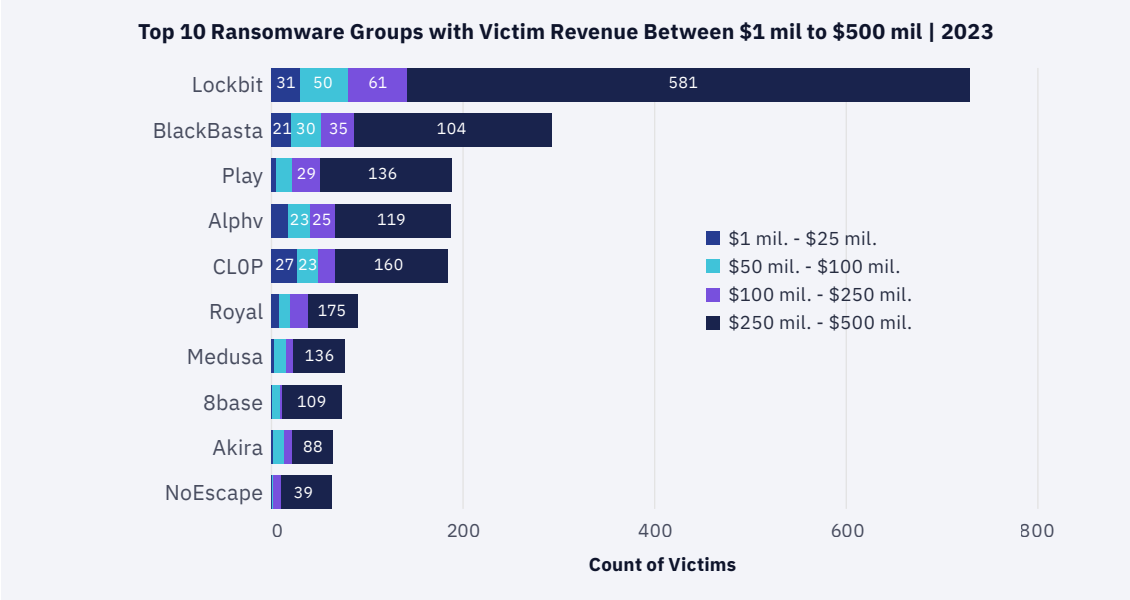

Figure 3: The top 10 ransomware groups targeting victims with revenue of $1 million - $500 million USD in 2023.

We also observed consistent trends around the most impacted industries (Figure 4); the top five victim industries are:

1. Manufacturing (18%)
2. Business Services (12%)
3. Retail (9%)
4. Construction (8%)
5. Education (5%)

The remaining five most targeted industries over 2020-2023 are Hospitality, Law Firms & Legal Services, Transportation, Finance, and Consumer Services.

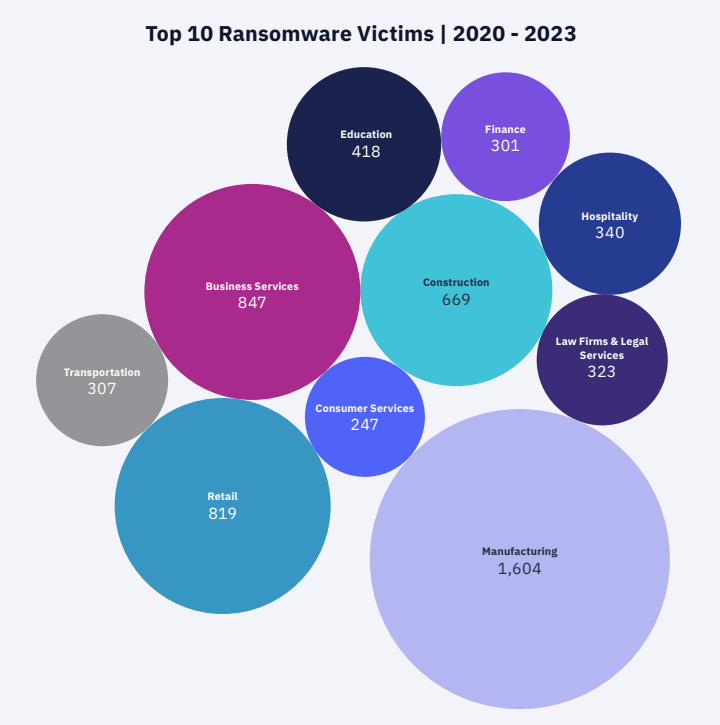

Figure 4: All-time victims grouped by industry.

It should be noted that both manufacturing and business services include a wide array of industry subtypes, which can affect this interpretation. For example, manufacturing includes thirty-two distinct sub-industries in this dataset, while Education has three. The top 3 sub-industries include:

Manufacturing

1. Industrial Machinery & Equipment
2. Building Materials
3. Food & Beverage

Business Services

1. Accounting Services
2. Custom Software & IT Services
3. Advertising & Marketing

Retail

1. Grocery
2. Home Improvement & Hardware
3. Consumer Electronics

One final attribute we examined for victims included the number of employees (Figure 5). When combined with revenue, there is a familiar pattern: businesses with revenue between $1 million and $25 million USD and under 100 employees account for nearly 40% of the victim pool.

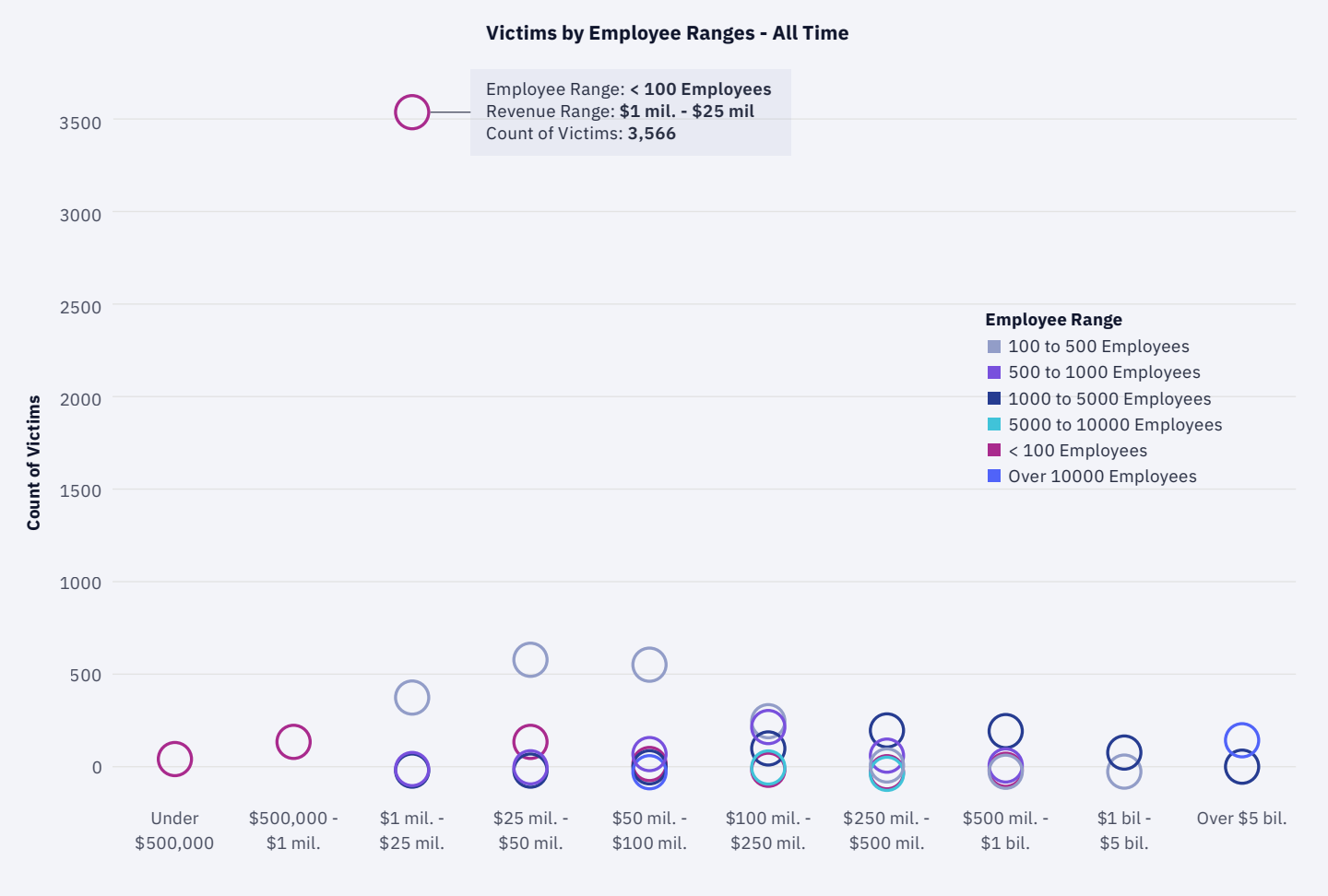

Figure 5: Relationship between victim employee count and revenue.

Initial Access Brokers (IAB)

Key Findings:

- Initial Access Brokers are a key contributor to the underground ransomware marketplace.
- IAB auctions are marketed using the victim's revenue, industry, country, and at times, employee count, which are key factors for evaluating future extortion payouts.
- Victim identities are deliberately obfuscated, but we found overlap with top industries affected by ransomware and possible victims.
- The exchange between the Initial Access Broker and the buyer takes time, so organizations must identify the source of compromise before the keys change hands.

As with the rise of ransomware-as-a-service, we also saw the rise of Initial Access Brokers – threat actors who specialize in gaining initial access into victim organizations and selling that access to other cybercriminals.

These sales tend to occur through initial access auctions, during which the brokers sell compromised access to a company's network or systems on underground forums or Dark Web marketplaces to the highest bidder (Figure 6).

The auction listings may include details such as the type of access (e.g., RDP or VPN), the industry or activity of the victim organization, the level of privileges obtained, the revenue of the company, the starting price, bid increments, and the buy it now price.

These auctions provide a way for threat actors to monetize access to compromised networks, which can be used for various malicious purposes, including ransomware attacks.

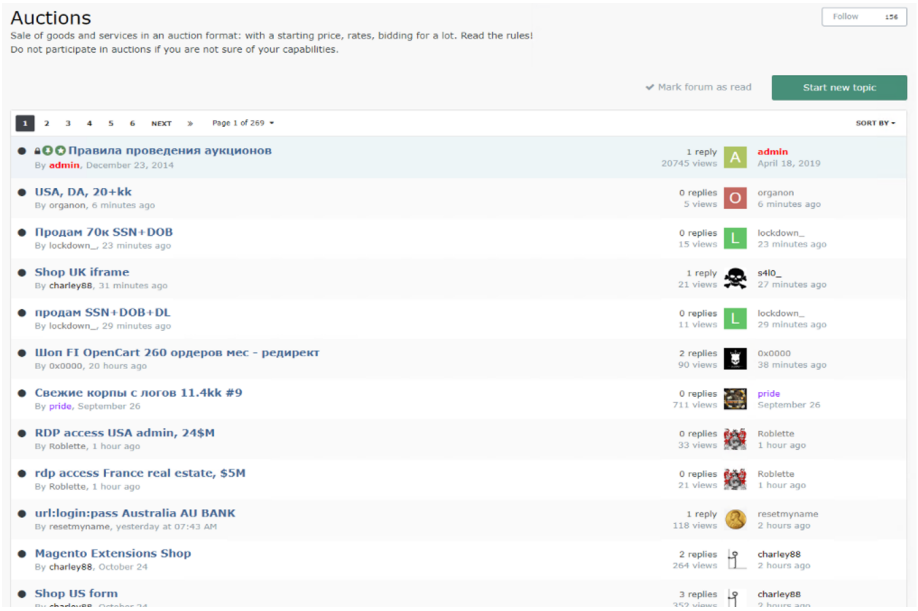

Figure 6: Exploit forums auctions.

These auctions commonly include the purported revenue of the victim organization to market their auctions to the highest bidder. For example, in October 2023, a threat actor auctioned privileged access to a US-based Telecommunications company with purportedly $380 million USD in revenue (Figure 7). Bidding started at $2,000 USD with the option to buy immediately for $5,000 USD.

Conversely, a UK-based commercial construction firm with $8.1 million USD in revenue began bidding at $800 USD with the buy-out set at $1,600 USD. These revenue numbers should be viewed skeptically, as they are provided by the seller and impossible to confirm without knowing victim's identity, especially since Initial Access Brokers are careful to include just enough details to market their access without divulging the real identity of the organization.

Figure 7: Example IAB auction for a US-based Telecommunications company with $380 million in revenue in October 2023. Access is Domain Admin level and through VPN.

Activity Over The Years

For our research, we analyzed and compared network-access auctions posted on a known Russian-language forum called Exploit; up until the end of 2023. We see a distinct increase in auctions beginning in 2021, followed by a 30% increase in 2022 (Figure 8).

This upward trend continued in 2023, with a 15% increase over the prior year. Vulnerabilities such as **CVE-2023-20198** or **CVE-2023-4966** which offer access to edge devices likely contributed to IAB auctions in 2023 and continue into 2024.

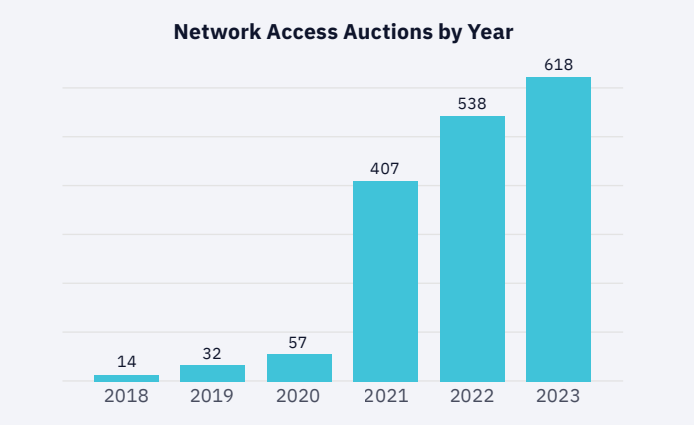

Figure 8: Initial Access Broker auctions identified on Exploit Forums.

We also evaluated whether there were any historical trends for the combined revenue and average revenue of victims (Figure 9).

Between 2021 and 2022, there was a 6% increase in the combined revenue for all businesses targeted but a 23% decline in average revenue for the same period.

This may suggest that while more large organizations are being targeted (raising the combined revenue), initial access for smaller businesses is being sold more often, possibly due to demand from increasingly agile extortion groups targeting smaller organizations.

On the other hand, between 2022 and 2023, both the combined revenue and average revenue for all businesses targeted decreased. This may indicate that attackers are increasingly targeting SMBs since they are less likely to have robust cybersecurity, making them easier targets even if the potential payout is smaller.

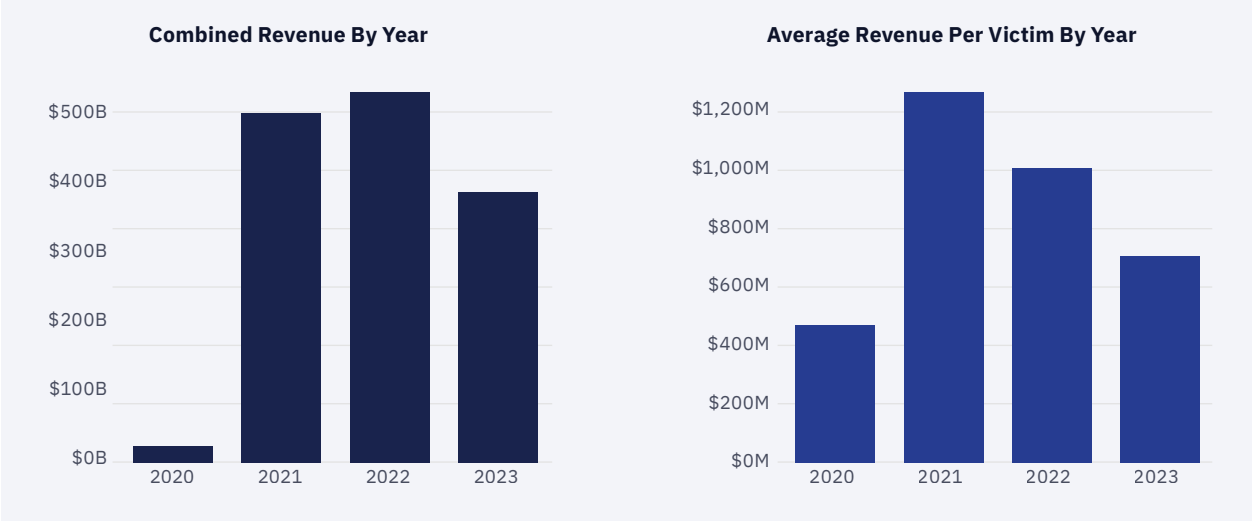

Figure 9: Combined revenue of victims (left) and average revenue of victims (right).

Lockbit, for example, likely has greater capacity to extort more victims for less revenue thanks to its affiliate model that enables a higher capacity for attacks. It's also possible this trend is affected by more auctioneers pushing company details to private messages or more clandestine avenues entirely when auctioning high-profile targets.

Initial Access Vectors

IAB auctions commonly include the method of access available to the buyer, such as:

- Email
- Secure Shell (SSH)
- Virtual Network Computing (VNC)
- Virtual Desktop Infrastructure (VDI)
- Virtual Private Network (VPN)
- Remote Desktop Protocol (RDP)

When looking at the breakdown of these access methods, RDP and VPN (or a mix of the two) seem to be the most common (Figure 10). RDP grants the buyer access to a system within the network via a graphical interface while a VPN provides access to internal network resources via the buyer's own system.

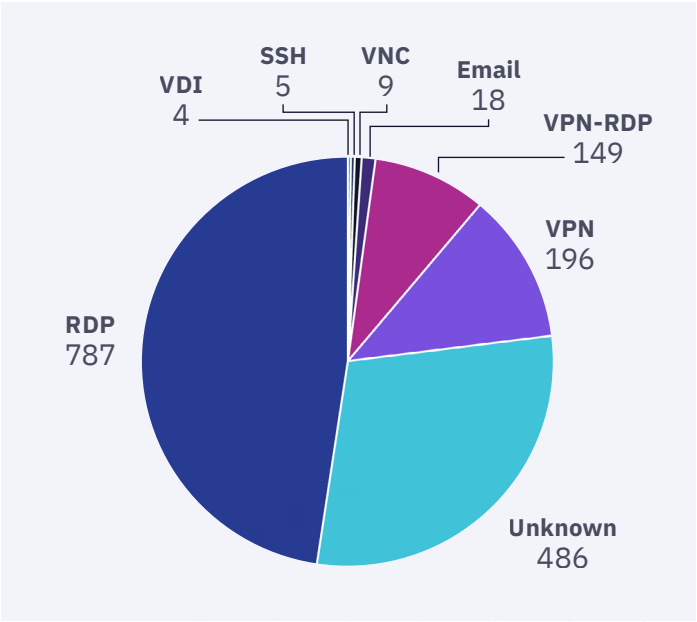

Figure 10: Purported access method offered in IAB auctions (2020 – 2023).

Regardless of the method, they grant threat actors access to internal network resources and a foothold from which to conduct cyberattacks, such as ransomware attacks. The preference for RDP and VPN access is further reflected by the average "buy-now" price for these auctions at $9,667 USD and $2,997 USD for RDP and VPN, respectively.

Therefore, we highly recommend implementing Multi-Factor Authentication (MFA) on remote access services as it increases the complexity for abusing compromised credentials. We also recommend restricting access to RDP servers to limit the exposure to brute force and exploit attacks.

Finally, it's also possible that "RDP" in these auctions refers generally to remote desktop access resulting from malware deployment on a server or desktop.

So, robust **endpoint monitoring and response** capabilities are a benefit here to prevent infection and identify compromise before it's too late.

Geographic Makeup of Victims

The geographical makeup of the IAB victims leans heavily towards organizations in the United States with 511 auctions. This is followed by Brazil (73), United Kingdom (62), Australia (60) and India (57) to round out the top five. Figure 11 plots the total auctions and average “buy-now” price (Blitz) by country. US organizations are not only the most numerous, but also demand the highest Blitz price.

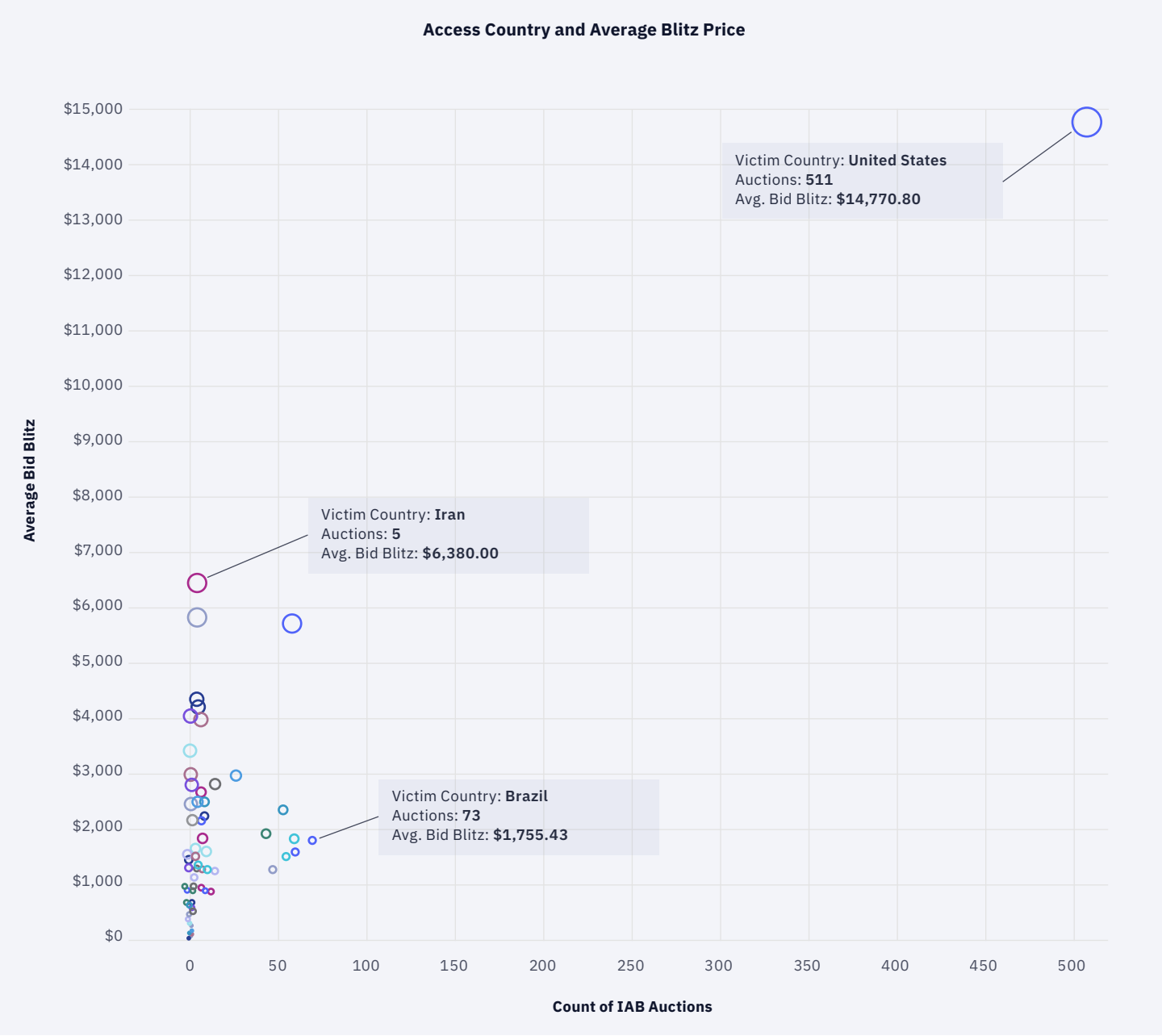

Figure 11: Comparison of average “buy-now” price and number of auctions identified by country (2020 – 2023).

Industry Makeup of Victims

Drilling down further, we can look at the industry breakdown of IAB victim organizations. Around 30% of auctions in our dataset included an identifier for the victim's industry although there is no common structure to how sellers offer this information. Some IABs copy and paste the industry identifier from B2B databases like ZoomInfo.

Others offer their own interpretation or choose to reveal it in private messages to conceal the identity of the victim from researchers. Thus, where available, we standardized the industry identifier so it could be joined and compared to other datasets.

Figure 12 shows the top ten victim industries across all countries by total count of auctions, including the access vector. For all three of the top targeted industries (i.e., Manufacturing, Business Services, and Retail), RDP is the most common initial access vector.

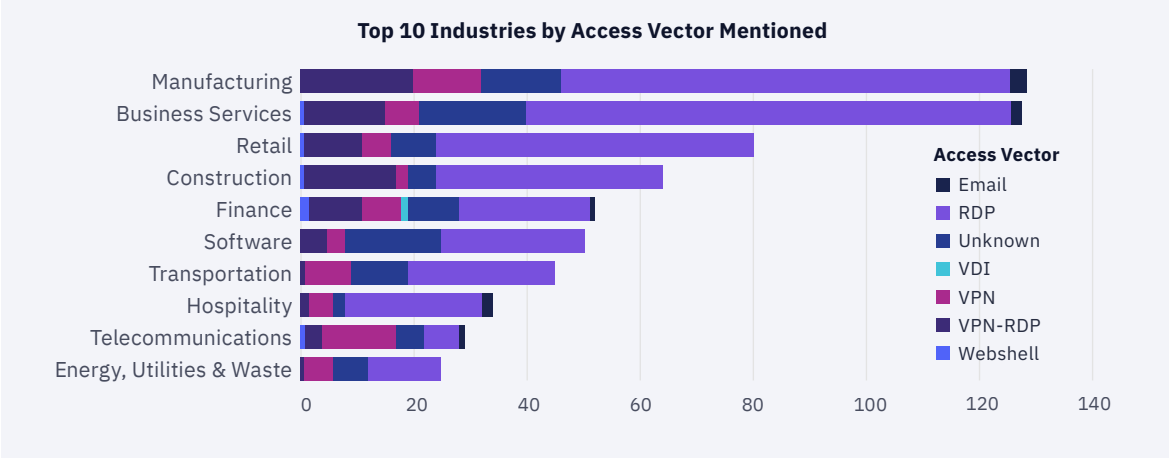

Figure 12: Top industries and access vectors (2020 – 2023).

Interestingly, the top IAB industries align closely with the top industries belonging to ransomware victims mentioned on data extortion leak sites (Figure 13 below). While the enriched IAB data is a sample of a broader access market which is difficult to quantify, it's an interesting correlation nonetheless and fits into a broader risk pattern for certain industries.

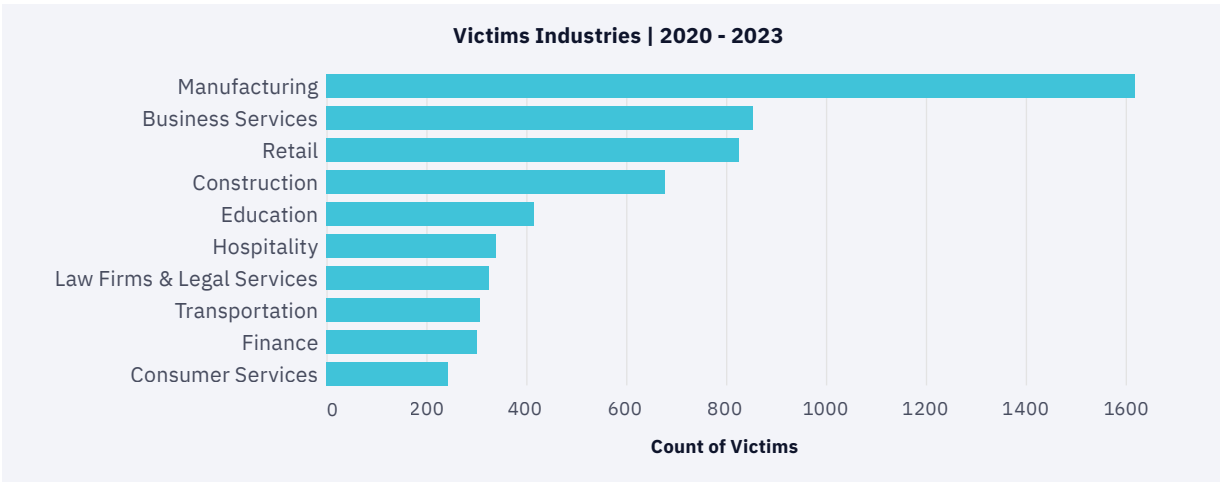

Figure 13: Ransomware victim industries, all time.

Tracing IAB Auctions to Ransomware Victims

Initial access auctions are purposely vague to avoid researchers or vendors tipping off victims before the sale. We assess these auctions are used by ransomware groups or affiliates to buy their way into networks to conduct extortion attacks.

To test this theory, we took five data points from IAB posts and compared them to victims mentioned on so-called ransomware name-and-shame sites. These include:

1. Matching Country
2. Matching Industry
3. Matching Sub-Industry (when available)
4. IAB auction within 30 days prior to leak by ransomware group
5. Revenue within $1 million USD

This resulted in a handful of matching IAB attributes and ransomware victims in Business Services, Construction, and Manufacturing (Figure 14).

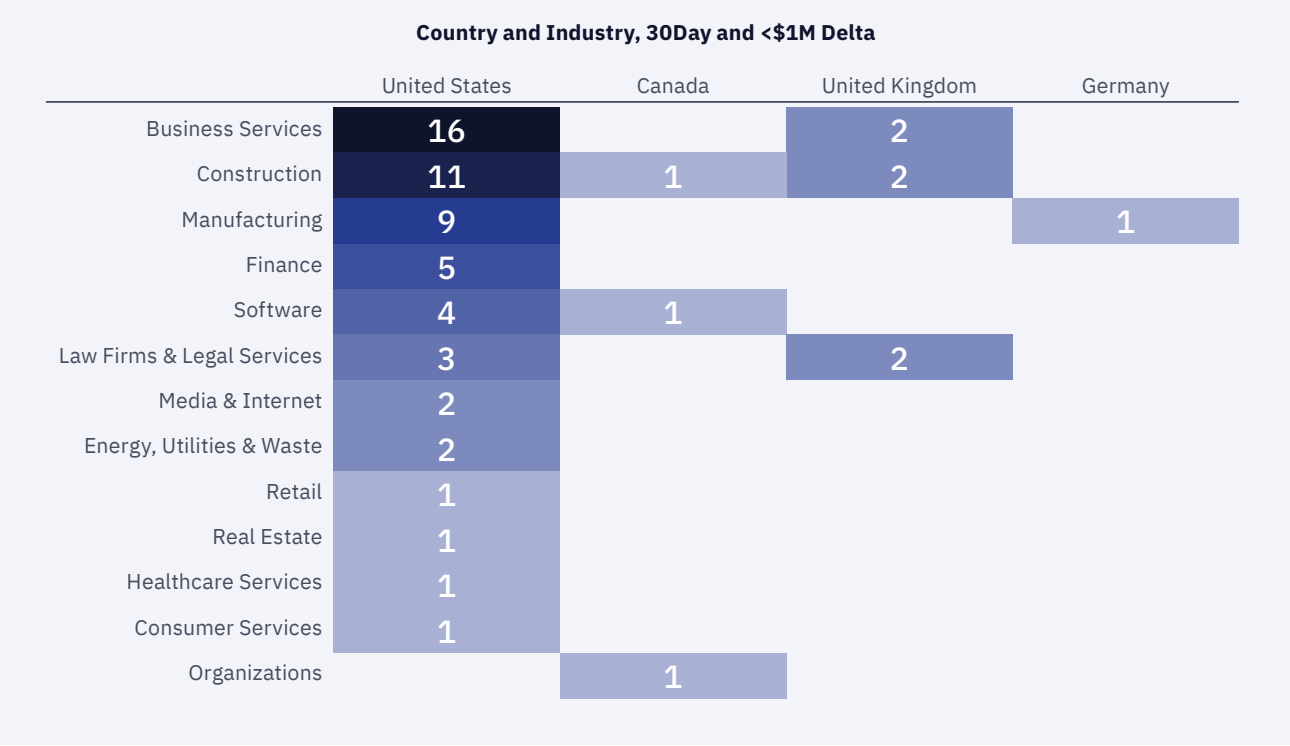

Figure 14: Possible correlation for IAB auctions and ransomware victims, within $1 million USD in revenue.

Expanding this to a revenue difference under $10 million USD yields significantly more matches (Figure 15).

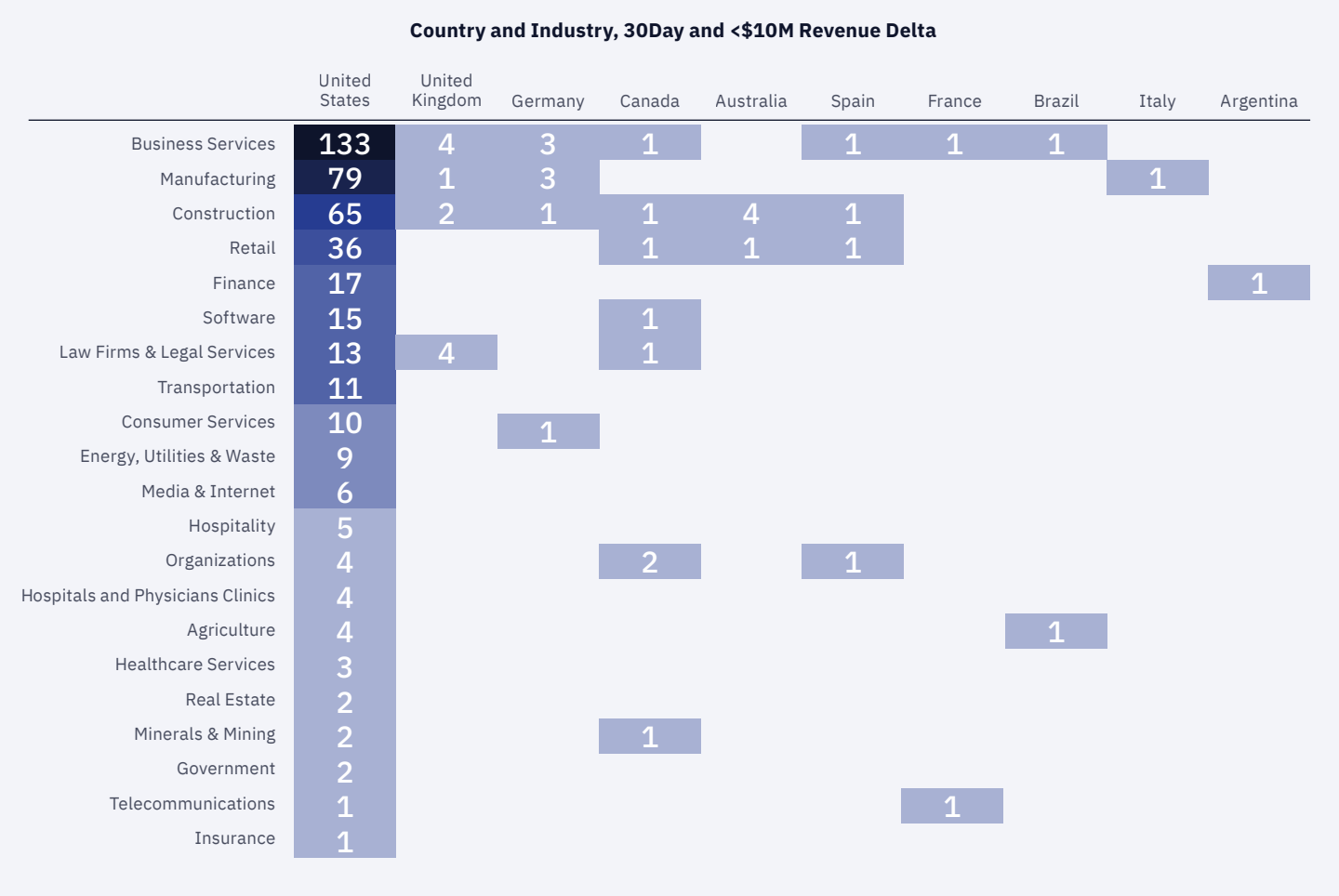

Figure 15: Possible correlation for IAB auctions and ransomware victims, within $10 million USD in revenue.

While it's not feasible to 100% match unnamed IAB victims with ransomware victims, the data fits a pattern that suggests certain industries (e.g., US-based Business Services, Manufacturing, Construction, Retail, and Finance) are more exposed or are simply more targeted by initial access threat actors either due to **geopolitical or purely financial** reasons. As a result, they're most likely to become ransomware targets compared to other industries.

Credential Exposure

Key Findings:

- Credentials are widely available across underground sources like fraud markets, leak sites, and Telegram channels. Fraud shops particularly offer a one-stop-shop for locating high-value credentials for network access, often for as little as $10 USD.
- Information stealing malware is a substantial source of credentials, including session tokens for bypassing MFA.
- There is a correlation between credential exposure and ransomware victims, wherein ransomware victims had 525 credentials (with passwords) exposed on underground sources on average.

The prevalence of ransomware (particularly ransomware-as-a-service) has driven demand for network access. Initial Access Brokers have emerged to meet this demand by selling access to networks primed for extortion.

Another means for gaining access includes compromised credentials for remote access services, email, or instant messaging platforms. These credentials are surprisingly trivial to acquire; shops like Russian Market or 2Easy offer logs from thousands of compromised systems for as little as $10.

These shops make it simple to identify credentials of interest, usually allowing users to search for specific technologies or services prior to purchasing.

Figure 16 shows the volume of sales on underground fraud shop Russian Market between January 2021 and August 2022.

Figure 16: Russian Market sales between January 2021 and August 2022. Breakdown of information stealer sources for credentials (insert).

These logs, often supplied by infostealers such as the **Redline Stealer malware**, include nearly every saved credential on the system (i.e., credentials stored in browsers, for crypto wallets, RDP, and VPN), to be exfiltrated and sold on the markets.

These stolen credentials include not only username/password sets, but also cookies which can be used to hijack legitimate sessions and bypass Multi-Factor Authentication (MFA) requirements.

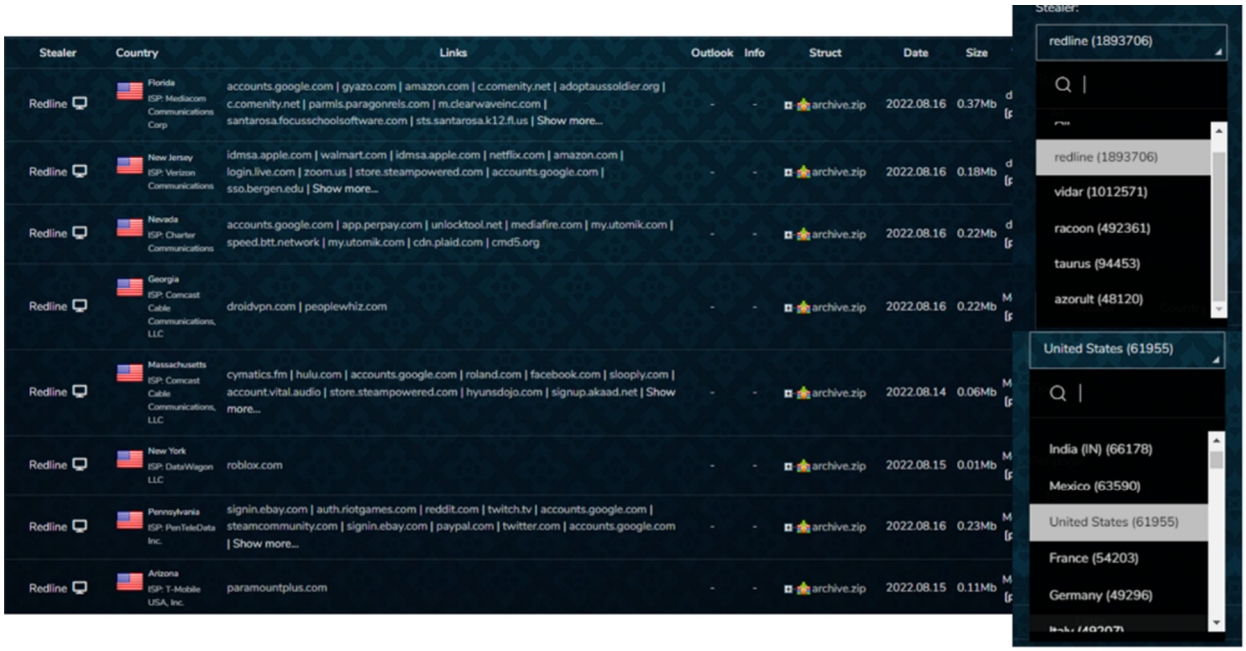

Figure 17: Russian Market panel. Read our full Redline Stealer malware analysis for more details.

Infostealer-sourced credentials are also widely distributed and sold on Telegram, a popular instant messaging platform. Figure 18 shows a post to a Telegram group from October 2023 selling monthly access to over 200,000 logs for $120 USD.

What's more, the link between information stealers, fraud markets, and ransomware attacks has been **documented previously**. Remote access to a system or network with a keychain full of credentials is a very powerful starting position for any intrusion.

As such, we examined known ransomware victims and their exposure to stolen credentials pertaining to information stealers (Figure 19). This was a relatively narrow search, considering it focused solely on the stealer logs distributed on underground forums or channels containing email addresses tied to these organizations.

We identified 5038 unique accounts tied to 799 organizations or approximately 16% of the ransomware victims in our dataset. While this is a relatively small percentage of victims, we assess that the number is likely higher considering the tight scope of our sample data.

Figure 18: Telegram group selling credential logs.

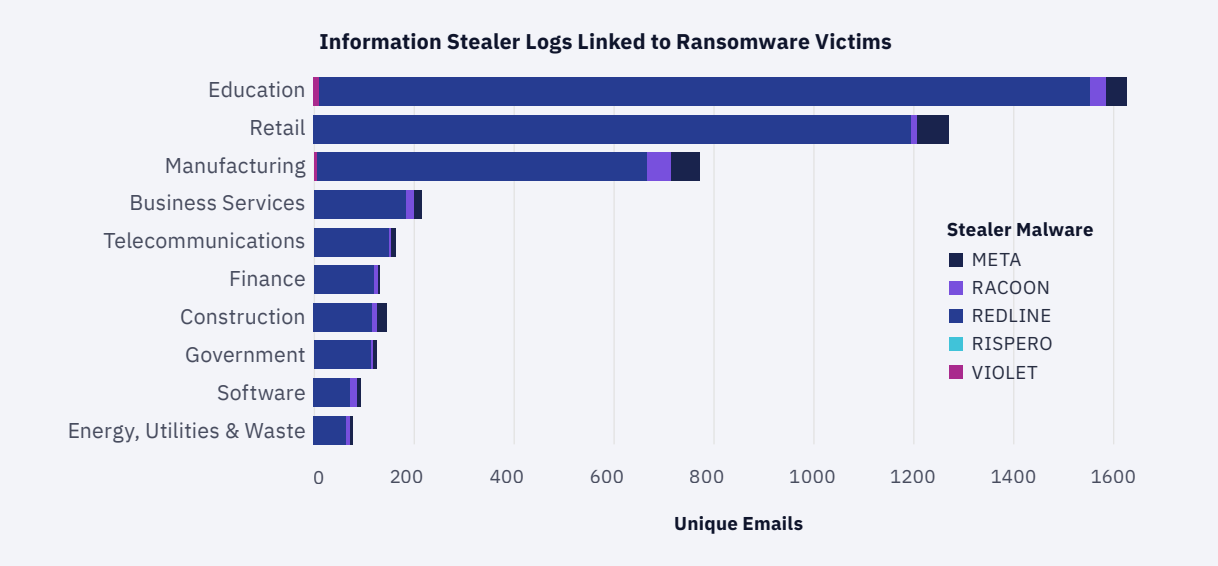

Figure 19: Breakdown of information stealer logs containing identifiable account names tied to ransomware victims identified on name-and-shame leak sites between 2020 and 2023.

Our threat research shows that the education industry was disproportionately represented, likely due to an abundance of student logins found in stealer logs. These logins represent less of a risk for network takeover than that of a regular employee assuming proper access controls are in place. A similar conclusion can be made about businesses in retail with respect to corporate and non-corporate credentials mixed together.

However, it still presents an opportunity for threat actors keen on targeting **higher education for cybertheft**. Login credentials for accounts belonging to businesses in manufacturing were also prevalent. What's of greater concern is that these credentials are more likely tied to real employees when compared to Education or Retail given the nature of these businesses.

Expanding this analysis, we looked at all credential leaks where the leak occurred within 30 days prior to the ransomware event.

Approximately 25% of ransomware victims had credentials exposed within 30 days of their identity disclosure on ransomware leak sites.

On average, these organizations had 23 credentials (username/email + password) exposed during this time. This number jumps to on average 525 credentials exposed at any time prior to this disclosure. We assess that the exposure of these credentials is indicative of a significant risk to organizations as these credentials can be leveraged by attackers to move laterally and deploy ransomware in compromised environments.

As we saw with infostealer logs, industries where employees and customers shared a common login domain are overly represented (e.g., Education, Real Estate and, in some cases Retail).

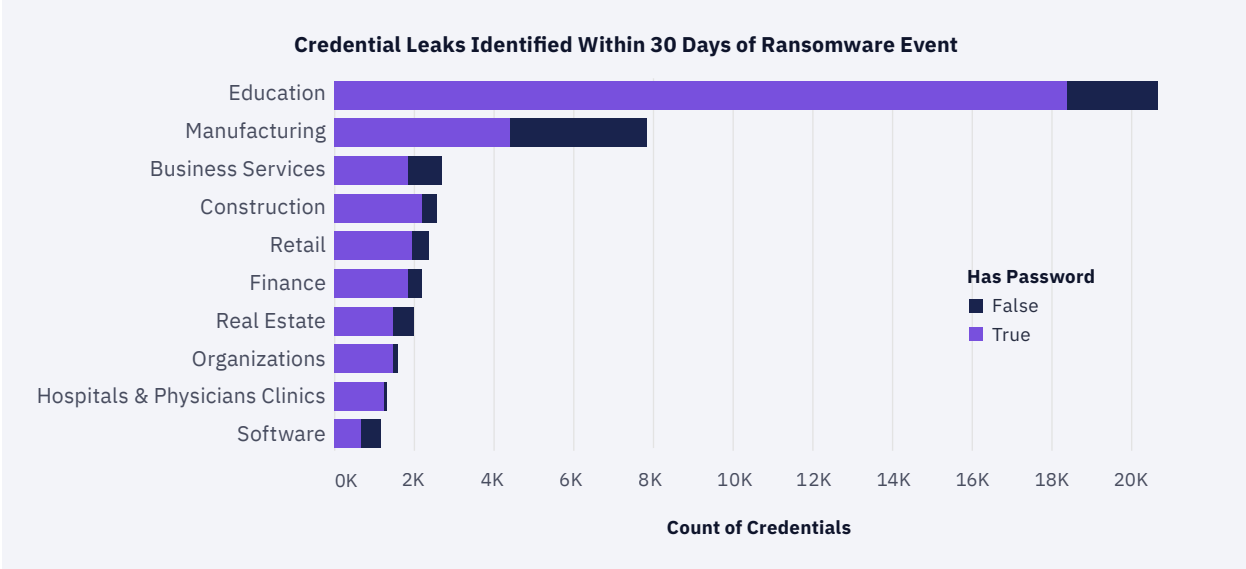

Figure 20: Credential exposure of ransomware victims grouped by industry within 30 days prior to publication on name-and-shame leak sites.

For example, Education, with only 6% of total victim organizations, represented 29% of total credentials linked to victims found on the underground. Comparatively, Manufacturing victims made up 21% of total victims and 16% of total credentials. Manufacturing poses a concern relative to other industries, with a high count of exposed credentials and unique victim organizations.

Again, we see that the Education sector is unevenly represented and it's less likely the high count of exposed credentials is representative of real risk to these organizations (given they are likely tied to student accounts). Exposed credentials across other sectors are more evenly distributed, suggesting a relatively high number of businesses victimized by ransomware had credential exposure.

The delta between the number of victims and total credentials provides an estimate of whether a certain industry is over-represented by organizations with many accounts (likely belonging to customers or non-employees).
The table below shows the top 10 victim industries by percentage of overall exposed credentials.

Industry	% of Total Orgs	% of Total Credentials	Difference
Education	6	29	23
Manufacturing	21	16	-5
Business Services	11	9	-2
Retail	10	6	-4
Construction	10	6	-4
Government	3	5	2
Finance	4	5	1
Software	3	4	1
Real Estate	3	4	1

Conclusion and Recommendations

Ransomware continues to be one of the top cyber threats faced by businesses, and one that remains profitable for adversaries. Understanding that ransomware attacks disproportionately impact and target small and medium-sized businesses (SMBs) puts security leaders in these organizations on notice that they could face more risk compared to other organizations, especially within the manufacturing, business services and retail industries.

Moreover, it's clear that the Lockbit Ransomware-as-a-Service (RaaS) threat is more acute for SMBs and can be more challenging to defend against given how it leverages affiliates and multiple attack vectors.

Network access is in demand, and IAB auctions are likely actively marketing the revenue, industry, country, and employee count for the targeted organizations, which help attackers estimate future extortion payouts. Security leaders must also understand that ransomware likely remains the top method of monetizing network access and skilled adversaries have **shifted** from fraud to extortion attacks.

What's more, information stealing malware is a substantial source of user credentials, including session tokens for bypassing MFA. These credentials are made widely available across the Dark Web through underground marketplaces, leak sites, and Telegram channels.

However, the exchange between the Initial Access Broker and the buyer takes time, so it's critical for organizations to identify the source of compromised credentials before the keys change hands to head off ransomware and extortion attacks. Our data shows a clear correlation between credential exposure and ransomware victims, so monitoring the Dark Web is critical to ensure that your employees' credentials aren't exposed on underground sources.

The challenge faced by organizations, particularly those with limited budgets, is anticipating attacks from multiple vectors, then withstanding the ones that get in. Security leaders should leverage the research presented in this report to educate themselves on the ransomware risks their organizations face and inform their cybersecurity strategies based on these recognized risks.

Based on the threat research presented in this report, our recommendations for reducing the risk of a ransomware attack and building resilience include:

Understand, Prepare, and Predict Cyber Threats

- Ensure your phishing and **security awareness training program** covers both email and browser-based threats.
- Secure your edge devices/services:
  - Apply security patches or mitigations as soon as possible.
  - Prioritize actively exploited vulnerabilities, even on internal systems.
  - Restrict access to management interfaces.
  - For file sharing services/devices, consider restricting access even when fully patched and reduce the retention on historical data to the minimum required.
- Secure all remote access services:
  - Place remote access services behind VPN and/or restrict access.
  - Require Multi-Factor Authentication (MFA) on all accounts.
- Reduce the impact of compromised credentials:
  - Require Multi-Factor Authentication (MFA) on all accounts.
  - Limit access to network resources to managed and compliant systems.
  - Deactivate/refresh authentication sessions in the event of account compromise.
- Protect endpoints from malware:
  - Engage an **Endpoint Detection and Response (EDR)** provider that offers anti-malware and response capabilities.
  - Keep systems up to date with the latest patches.
- Implement a **Dark Web Monitoring** service so your team can actively monitor for leaked employee credentials or even endpoint sales resulting from information stealing malware.
- Engage an **Incident Response (IR) Readiness** service to take a proactive approach to quickly resolve an attack, minimize business disruption, and reduce your recovery costs.

Detect, Investigate, Disrupt, and Contain Cyberattacks

- Centralize logging for all edge devices.
- Monitor log-on activity for remote access services, such as VPN/RDP.
  - Immediately revoke illegitimate sessions and attempt to identify the source of compromise.
- Remediate malware infections as quickly as possible.
  - Isolate systems and lockout accounts while investigation takes place.
  - Investigate account activity on other systems during the compromise window.
  - Remediation should include returning the system to a known good state, revoking active sessions, and resetting compromised credentials post-cleanup.

Eradicate Threats and Return to Standard Operations

- Identify the type of ransomware and/or the threat actors behind the attack, if possible, to determine if there is a possible decryption key already available.
  - If you don't have the expertise to conduct this investigation in-house, engage an external **Incident Response provider** that also has Digital Forensics capabilities to lead the charge.
- Create, maintain, and exercise a strong cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.
- Review all your current Incident Response plans around restoring applications, platforms and networks following an event, including:
  - Business Impact Analysis
  - Business Continuity Plan
  - Disaster Recovery Plan
  - Incident Response Plan

Protect Your Employees and Brand Reputation with eSentire's Dark Web Monitoring Services

Even if your organization has the right tools, it can still be difficult to inform decisions based on vast data living in Dark Web networks without real-time monitoring and correlation for improved threat context. Moreover, if your team is unable to correlate what sensitive data has been leaking, it's challenging to know where to look for on the Dark Web with respect to threats and future risks that can potentially impact your organization.

Our Dark Web Monitoring service extends visibility beyond your on-premises and cloud environments to detect compromised user credentials, corporate sensitive data, and early indicators of potential cyber threats to protect your brand, executive team, and employees. 24/7 monitoring across the Dark Web identifies early indicators of potential cyber threats, IOCs, and evolving tactics, techniques, and procedures (TTPs) that threat actors rely on to conduct sophisticated cyberattacks.

In addition, we provide contextual awareness into known and unknown threat actor groups, for deeper threat investigations, by observing forum discussions, recognizing communications patterns used within conversations, and using this intelligence to build a timeline to inform our threat response actions.

More specifically, you can benefit from:

- Enhanced visibility and alerting on compromised credentials, mentions by Initial Access Brokers (IABs), or discussions of a targeted cyberattack — including 24/7 monitoring for leaked credentials of your top executives and key personnel.
- Identification of potential phishing campaigns, domain infringement practices, and other malicious activities.
- Proactive monitoring of third-party and supply chain vendors to manage and reduce supply chain risk.
- Identification of employees (or other insiders) who are acting with malicious intent to violate security policies or sell their credentials/access on the Dark Web.

Plus, eSentire MDR customers can also leverage the eSentire Threat Response Unit (TRU) and the eSentire Cyber Resilience Team for regular reports on relevant Dark Web alerts, get informed on industry-specific risk areas, participate in live TRU intelligence briefings —and more.

We are recognized globally as the Authority in Managed Detection and Response because we hunt, investigate, and stop known and unknown cyber threats before they become business disrupting events. We were founded in 2001 to secure the environments of the world's most targeted industry—financial services. Over the last two decades, we have scaled our cybersecurity services offering to hunt and disrupt threats across every industry on a global scale.

With two 24/7 Security Operations Centers (SOCs), hundreds of cyber experts, and 2000+ customers across 80+ countries, we have scaled to deliver cybersecurity services across highly regulated industries with a proven track record of success in securing organizations.

Ready to get started?

Connect with an eSentire Security Specialist to learn how eSentire Multi-Signal MDR, powered by our XDR Cloud Platform, can help you reduce cyber risk and prevent ransomware attacks from disrupting your business.

CONTACT US

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US 1-866-579-2200

eSENTIRE