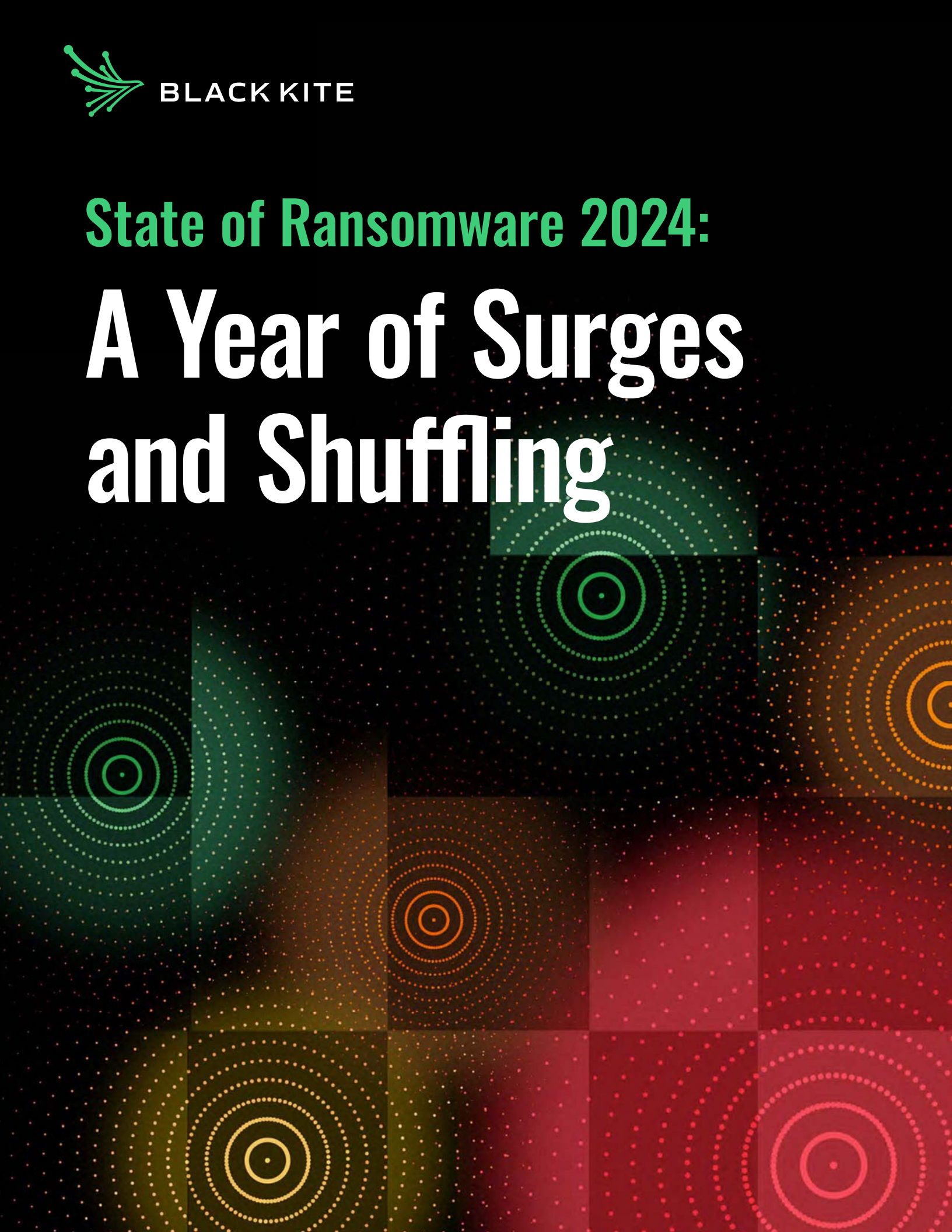




BLACK KITE

**State of Ransomware 2024:**

# **A Year of Surges and Shuffling**





# Table of Contents

<b>Introduction</b>	<b>3</b>
<b>Executive Summary</b>	<b>4</b>
<b>Ransomware Reckoning: The Surge and Shuffle</b>	<b>5</b>
<b>Ransomware Group Dynamics: The Shifting Power</b>	<b>8</b>
<b>Case Studies: Operational Disruptions in the Ransomware Echelon</b>	<b>11</b>
<b>The Affiliate Chess Game: Ransomware’s Recruitment Rush</b>	<b>13</b>
<b>Spotlight: Change Healthcare Incident</b>	<b>15</b>
<b>The Alarming Trend of Quick Succession Ransomware Attacks</b>	<b>18</b>
<b>Affiliate Dynamics: The Ransomware Crossover</b>	<b>19</b>
<b>The Affiliate Marketplace</b>	<b>20</b>
<b>Opinion: Dr. Ferhat Dikbiyik</b>	<b>21</b>
<b>The Global Ransomware Marketplace: Victim Profiling and Strategic Targeting</b>	<b>22</b>
<b>Manufacturing Sector: A Ransomware Hotspot</b>	<b>26</b>
<b>Evaluating the Bounty: Ransomware Targets by Financial Footprint</b>	<b>31</b>
<b>Crafting a Corporate Veil: The Dichotomy of Ransomware PR</b>	<b>37</b>
<b>Case Study: A Look at Ransomware’s Impact on US Essential Industries</b>	<b>38</b>
<b>Rethinking Ransomware: From Reaction to Prevention</b>	<b>40</b>
<b>Understanding Ransomware Susceptibility</b>	<b>43</b>
<b>How RSI™ Helps to Mitigate Ransomware Risk</b>	<b>45</b>
<b>Prevention and Minimizing Ransomware Risk</b>	<b>46</b>
<b>Mitigating Third-Party Ransomware Risk</b>	<b>47</b>
<b>Conclusion</b>	<b>48</b>
<b>Methodology</b>	<b>46</b>
<b>Black Kite Research &amp; Intelligence Team</b>	<b>50</b>



# Introduction

In recent years, the digital landscape has been marred by a growing and pervasive threat: **ransomware attacks**.

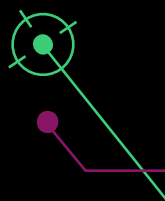
Once considered a sporadic nuisance, these malicious incursions have evolved into sophisticated operations, orchestrated by organized cybercrime syndicates with chilling efficiency. As businesses and individuals increasingly rely on interconnected systems and digital infrastructure, the stakes of these attacks have never been higher.

In our continued monitoring of ransomware activity by the Black Kite BRITE team, we've uncovered a startling observation: The sophistication of ransomware groups rivals that of any tech startup. A number of these criminal organizations offer services like customer support for victims to help streamline the process of payment. They have legions of employees, or affiliates, for whom they have recruitment strategies and the groups have go-to-market-like strategies where different groups have preferential victim profiles. Each group has a preferred set of tactics or strategy for perpetrating their crimes.

Our research also confirms that gone are the days when these groups would mostly target resource-rich organizations. Back then, there stood an unwritten code: Do not target organizations that offer critical human services. This is no longer the case, and we are seeing a stark rise in the number of attacks against healthcare related organizations.

This research report delves into the alarming rise of ransomware incidents, shedding light on the evolving tactics of cybercriminals, how they operate and the profound impact these attacks have on victims worldwide.

We hope you find the information in this report as enlightening (and fascinating) as we do.



# Executive Summary

In a digital landscape where threats constantly evolve and adversaries grow more cunning, understanding the dynamics of ransomware attacks is critical. By shedding light on the tactics, motivations, and consequences of these nefarious operations, this report aims to empower organizations with the knowledge and insights needed to bolster their cybersecurity defenses and mitigate the risk of falling victim to ransomware extortion.

**The last year saw a massive increase in ransomware attacks, increasing from 2,700+ in the previous twelve months to almost 4,900 businesses in the last twelve months.** This highlights the increased persistence of these groups as well as the incredible effectiveness of their tactics.

**We saw the rise and fall of specific groups that left voids for newer or up-and-coming syndicates to fill.** This year also saw more evidence that affiliates are moving between ransomware groups to maximize their own profits.

**Another alarming trend this report surfaces is the prevalence of repeat victims.** Our data indicates that 104 companies were victimized by two groups while three companies were targeted by three groups. These repeat attacks come in rapid succession to the first, indicating the ransomware groups are monitoring other attacks so they can strike while a victim is still weak.

**Geographic targeting remains a consistent way for ransomware syndicates to profile victims.** 47% of reported ransomware victim companies were located in the **United States**.

**Other countries with a large number of attacks are the United Kingdom, Canada, Germany and Italy**— all countries with prosperous economies, suggesting the attackers are looking to maximize profits.

**Industries most hurt by operational disruption topped the list in terms of number of ransomware attacks.** Manufacturing leads the pack with professional services and healthcare close behind.

Based on the ransomware groups' most common motivation of maximizing profits, one would assume that larger organizations would bear the brunt of attacks. However, the data does not support this hypothesis. **In fact, a significant 31% of ransomware victims, in our study, are organizations with less than \$20 million in annual revenue.**

Overall, the data in this report highlights the importance of proactive measures rather than incident response when it comes to managing ransomware risk. Being able to recognize trends in how ransomware groups behave allows us to identify ransomware risk factors and create mitigation plans.



**For example, Black Kite's Ransomware Susceptibility Index<sup>®</sup> (RSI<sup>™</sup>) can see that the companies with a value above 0.8 on a 0-1 scale are 27 times more likely to experience a ransomware attack than the companies with a value**

Having this type of information and understanding a company's RSI<sup>™</sup> value can mean the difference between business disruption and smooth business operations.

## RANSOMWARE RECKONING:

# The Surge and Shuffle

We are seeing an unrelenting rise in ransomware attacks in a world where cyber adversaries function like shadow enterprises.

The number of victims has doubled, marking an alarming climb from the previous year, from last year's 2,700+ to almost 4,900 businesses caught in the digital crosshairs. This year's storyline sees ransomware as a service (RaaS) operators playing kingmaker, as former allies turn competitors. The stage is set: New actors enter, old ones exit, and the game of digital dominance evolves. It's a relentless pursuit of power where only the adaptable survive.

This section peels back the layers of the ransomware rampage, revealing the rise and fall of the infamous, silent takedowns and the new faces of cyber threats.

**Buckle up — it's a wild ride through the dramatic shifts and data that reshaped the ransomware realm.**

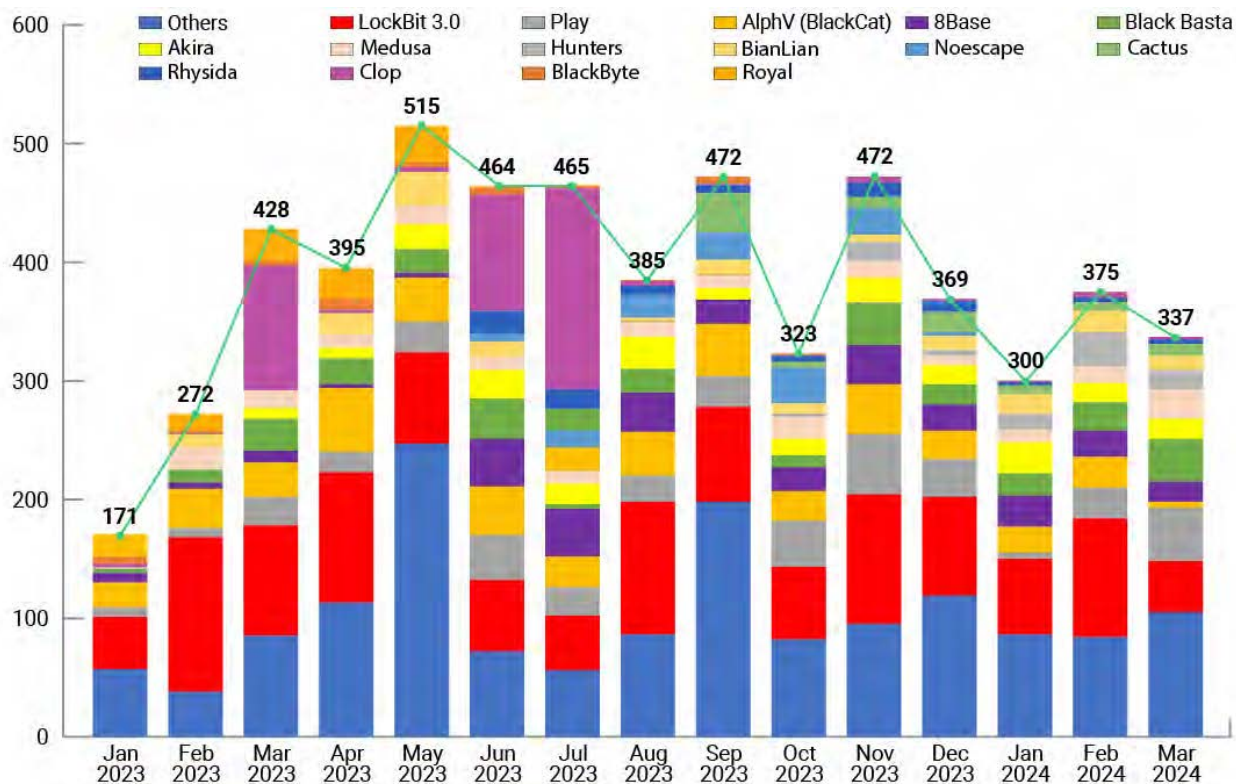
# From Gradual Increase to Exponential Growth

The narrative of ransomware in the past year has transitioned from moderate increases to exponential growth. Data from early 2023 indicates victim numbers below the two-hundred mark per month. However, subsequent months witnessed a considerable surge, highlighting an expanding threat landscape. For a comprehensive analysis, the chart below includes figures from the first quarter of 2023, ensuring a full view of the year's progression.

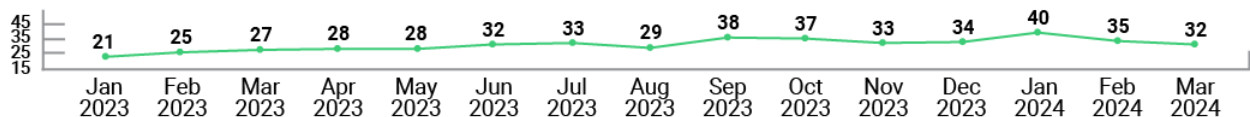
# Attacks Double Year Over Year

Focusing on the same annual quarters in 2022, 2023, and 2024, there's a remarkable trend: **Victim counts have nearly doubled each year, with this year's count reaching 4,893, up from 2,708 the previous year.** This trend indicates not just an escalation but an acceleration of attacks, signaling an evolving and more aggressive ransomware environment. The data serves as a critical metric of cybersecurity challenges, calling for strategic responses in threat mitigation.

### Number of Ransomware Victims Announced



### Number of Ransomware Gangs that Announced at Least One Victim

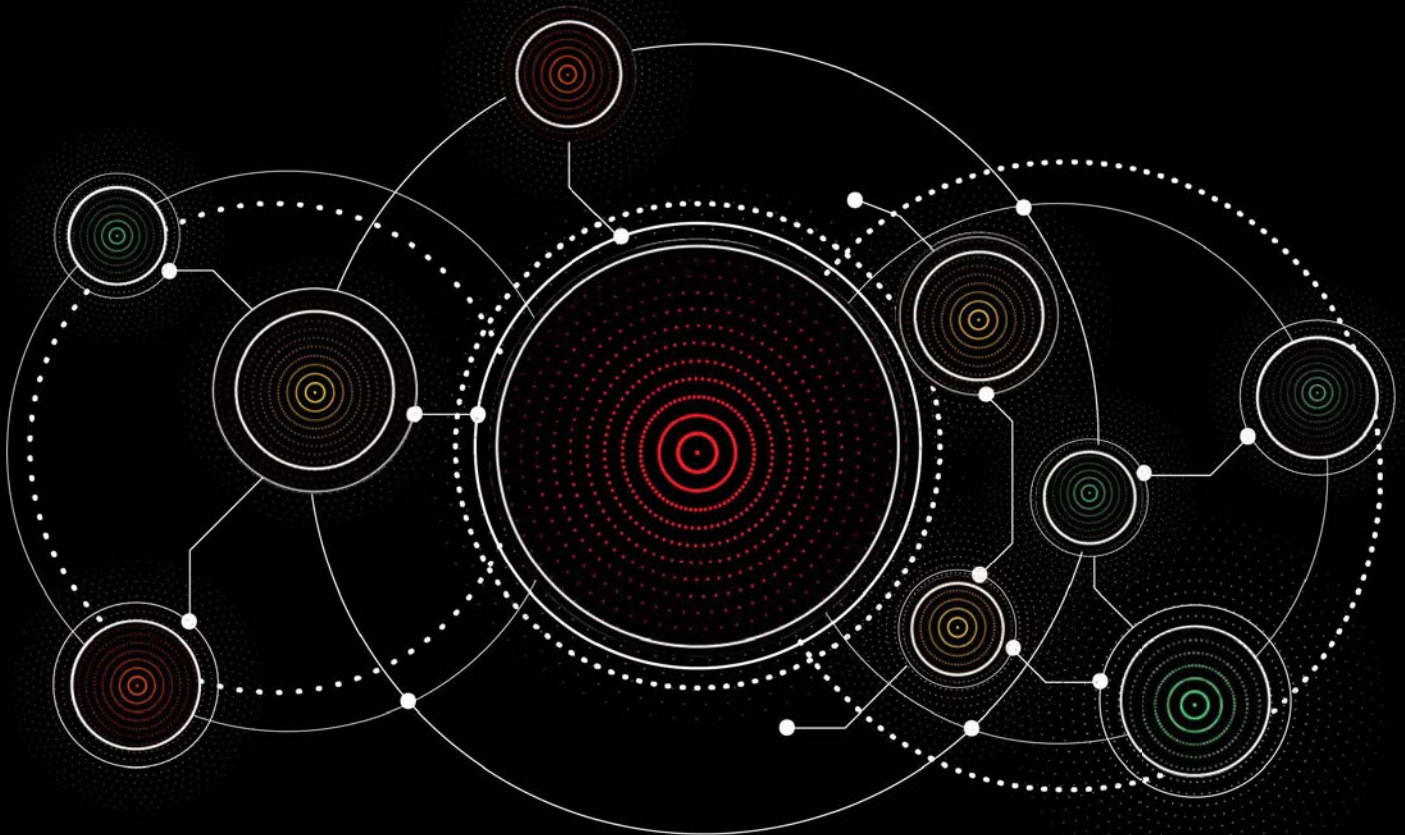


# Notable Ransomware Operator Activity

The ransomware landscape in the past year has been dynamic, characterized by significant incidents that have both escalated the threat level and signaled a shift in cybercriminal activities. **Here's a closer look at the pivotal moments that stood out:**

- **ClOp's** aggressive campaigns in March 2023, exploiting GoAnywhere MFT servers, set off a cascade of activity.
- **ClOp** continued to capitalize on vulnerabilities, moving to exploit MOVEit MFT servers in the mid-year.
- **Malas**, entering the fray in May 2023 and targeting Russian companies, made a short but impactful appearance.
- **AlphV**, previously second in infamy, suffered an operational shutdown by the FBI in late 2023, an event that saw their online presence dismantled.
- **LockBit's** foothold wavered following law enforcement interventions in early 2024, leading to an exodus of their affiliates.
- The disruption of **AlphV** and **LockBit** has not cooled the ransomware arena but instead ignited a frenzy of activity as groups vie for dominance and attempt to fill the void left behind.

The **cybercrime ecosystem** is currently in a state of rapid flux. Following significant disruptions to major ransomware operators, we're seeing a competitive scramble as groups vie to recruit top-tier affiliates.

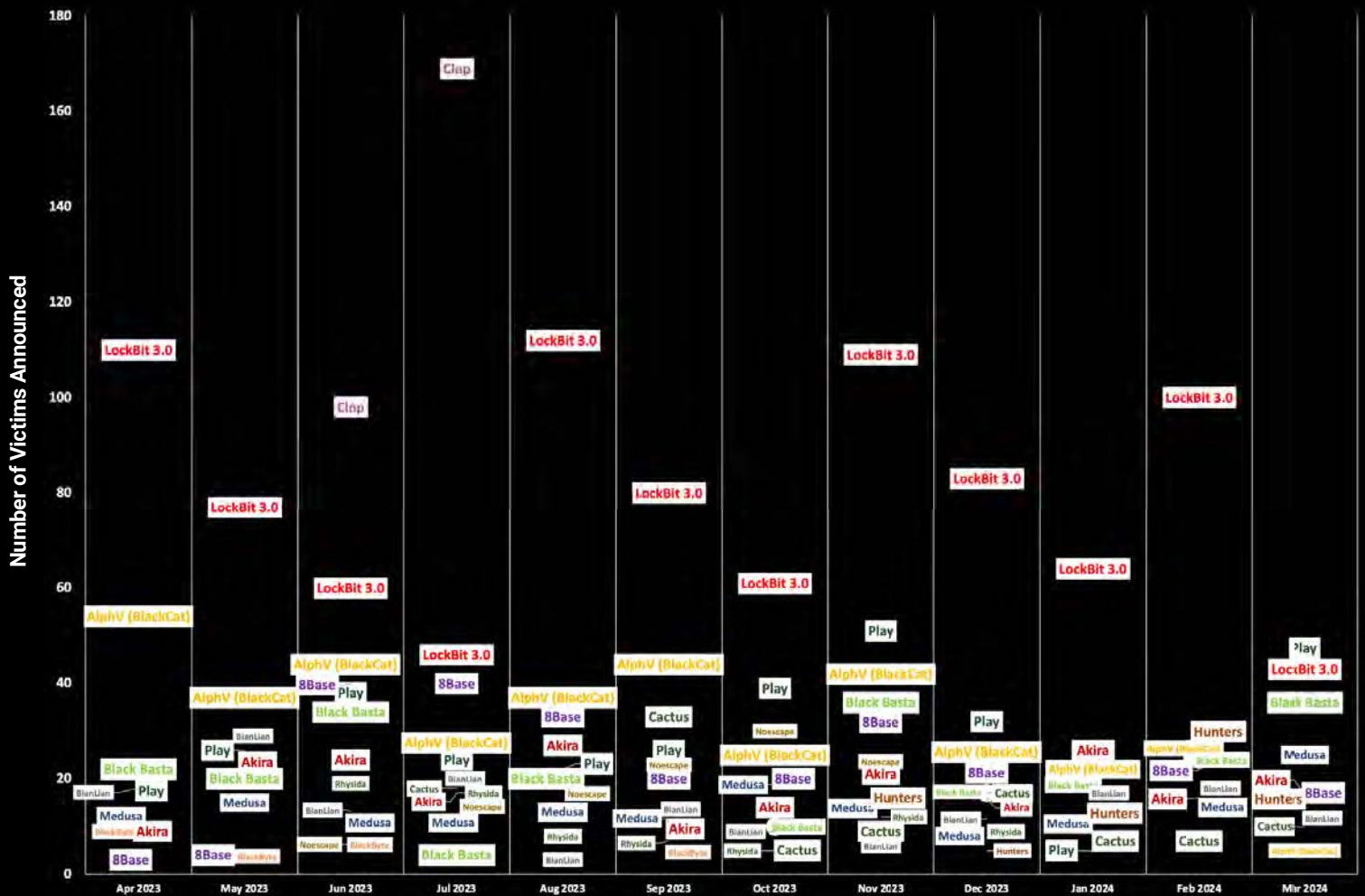


## RANSOMWARE GROUP DYNAMICS:

# The Shifting Power

The past year has witnessed a dramatic shift within the ransomware ecosystem. As key players have been disrupted by law enforcement actions, a power vacuum has emerged, prompting rapid movement within the rankings. The chart below offers a visual narrative of these changes.

### Changes of Leadership Table in Time





# Here are the pivotal shifts:

## The Rise and Reformation of AlphV and LockBit

AlphV, known for high-profile attacks, suffered an FBI-led shutdown in December 2023. They rebounded temporarily with LockBit's aid but later executed an exit scam.

LockBit faced its disruption in February 2024, causing a significant number of their affiliates to defect. The group attempted a comeback but could not reclaim its former dominance.

## Shuffling of the Leaderboard

The leaderboard saw newcomers rise as established players fell. Groups like Play made rapid ascents, now ranked #3 overall, topping March 2024's list.

Other groups such as Cl0p have maintained consistent yet less aggressive activity, indicating a strategic shift in operations.

## The Decline and Silence of Former Players

Notably, Royal and Vice Society, active in early 2023, have since retreated into inactivity.

Karakurt and AvosLocker, once prominent names, have ceased victim announcements post-mid-2023, indicating potential operational ceases or strategic reclusions.

## Emerging and Ascending Groups

New entrants like Akira, which debuted in March 2023, have quickly climbed to rank #6.

8Base, initially outside the top ten, has now surged to rank #5, suggesting successful recruitment and operations.

## Watchlist for New Entrants

Fresh faces such as Cactus, Rhysida, Hunter, and INC Ransom are carving their niches, indicating a diversifying threat landscape.

A plethora of small groups, including Trigona, Knight, and RansomHub, have entered the arena, with RansomHub gaining notoriety after announcing Change Healthcare as a victim.

This rapid realignment within the ransomware hierarchy signals not a cooling period but a bustling bidding war for affiliates. The data suggests that the ecosystem is more dynamic than ever, with power balances shifting quickly as groups jockey for position in the post-AlphV and LockBit era.



## Declining Ransomware Groups: Table 1

Ransomware Group	Previous Rank	Current Rank	Key Notes
<b>LockBit</b>	#1	Losing leadership rapidly	Once the clear leader, now dethroned following law enforcement actions and loss of affiliates.
<b>AlphV</b>	#2	N/A	Operations disrupted by the FBI, exit scam executed, no longer active.
<b>CloP</b>	#4	Maintained	Known for hit-and-run tactics, less active but still consistent.
<b>Malas</b>	N/A	Disappeared	Short-lived, targeted Russian entities, no longer active.
<b>Royal</b>	#5	#19	Backed by Conti, ceased activities after the first half of 2023.
<b>Vice Society</b>	#7	#48	Focused on European organizations, especially in education, now inactive.
<b>Karakurt</b>	#9	#34	Previously linked to Conti and Diavol, stopped announcing victims since Q3 2023.
<b>AvosLocker</b>	#11	#54	Warned by FBI for targeting U.S. infrastructure, no victims announced post-Q2 2023.
<b>WereWolves</b>	Entered Top 3 in the month of December	N/A	Emerged late 2023, silent after announcing a single 2024 victim.
<b>Nokoyawa</b>	N/A	Silent	Small group, became inactive since Q3 2023.

## Rising and Newcomer Ransomware Groups: Table 2

Ransomware Group	Previous Rank	Current Rank	Key Notes
<b>Play</b>	#10	#3	Rapid ascension, potential to lead the ransomware space, most victims in March 2024.
<b>8Base</b>	Not in Top 10	#5	Significant activity increase, noteworthy rise in the ranks.
<b>Akira</b>	New Entrant	#6	Debuted in March 2023, quickly attracting affiliates and climbing ranks.
<b>Medusa</b>	N/A	#10	Transitioned from MedusaLocker variant to a full-fledged RaaS in 2023.
<b>Cactus</b>	New Entrant	#12	Part of the 2023 wave of new ransomware groups, making a mark. Attacked Schneider Electric in mid-January.
<b>Rhysida</b>	New Entrant	#13	Another 2023 debutant showing active operations. Predominantly deployed against the education, healthcare, manufacturing, information technology, and government sectors according to CISA.
<b>Hunters</b>	New Entrant	#14	Entered the scene in 2023, rapidly rising through the ranks.
<b>INC Ransom</b>	New Entrant	#15	Newcomer in 2023, part of the diversifying ransomware ecosystem.
<b>RansomHub</b>	New Entrant	Not Ranked	Gained attention with the announcement of Change Healthcare as a victim.

## CASE STUDIES:

# Operational Disruptions in the Ransomware Echelon

## The Strategic Dismantling of AlphV

AlphV, once a notorious entity within the cybercrime landscape for targeting heavyweights like MGM Resorts, found its empire compromised by a decisive FBI operation in December 2023. The takedown not only shattered their operational front but also spotlighted the group's vulnerabilities. In a bid for revival, AlphV aligned with LockBit but soon staged an exit scam, leaving their affiliates in disarray and abruptly severing their revenue stream.

The aftermath saw AlphV's scattered affiliates seeking refuge with other rising ransomware groups, catalyzing a realignment in the power dynamics of the cybercrime ecosystem. This migration underscored the volatility within these illicit networks and highlighted the impact of law enforcement interventions in disrupting established ransomware operations.

The broad impact of AlphV's operation and subsequent fallout provides an intricate case study of the vulnerabilities within cybercriminal syndicates. It also highlights the effective outcomes of concerted law enforcement initiatives to disrupt cybercrime operations. The detailed account of AlphV's exit scam has been meticulously chronicled by Black Kite's cybersecurity experts, offering an in-depth perspective into the operation's unraveling and the subsequent realignment within the cybercrime underworld. This comprehensive case study serves as a significant entry in the annals of cybercrime and is detailed further in [Black Kite's report](#).

AlphV's story is a testament to the transient nature of cybercrime dominion, where today's leaders can swiftly become tomorrow's fallen, reshaping the threat landscape and compelling a dynamic cyber defense posture.

# LockBit's Operational Setback and Market Shift

LockBit's reign as a formidable force in ransomware was upended in February 2024 when law enforcement agencies successfully infiltrated and disrupted their operations. Known for their aggressive and widespread attacks, LockBit's infrastructure faced a significant blow that extended beyond the digital realm, leading to the doxxing of affiliate nicknames and a loss of anonymity crucial for their operations.

The exposure not only dismantled the trust within the group but also precipitated the disbanding of its affiliate network. The confidence shake-up caused by the exposé led many affiliates to defect to other groups, leaving LockBit in a state of disarray and struggling to maintain its status quo. In a landscape where reputation is currency, LockBit's was deeply devalued.

Attempting to reclaim their influence, LockBit initiated a rebranding effort with the launch of a new dark web presence, posting a list of alleged victims. This move, however, was met with skepticism as claims of victimization included potentially fabricated entries or ex-victims, reflecting a desperate bid to portray dominance where influence had waned.

The detailed story of LockBit's decline from a cyber titan to a compromised entity is thoroughly documented by Black Kite, providing valuable insights into the group's fall and the consequent shifts in the cybercrime market. The full account, shedding light on the strategic implications for cybersecurity defenses, can be found in [Black Kite's detailed analysis](#).

LockBit's case underscores the dynamic nature of cyber threats and the effectiveness of collaborative law enforcement efforts. As the ransomware scene continues to evolve, the LockBit narrative serves as a reminder of the continuous need for adaptive security strategies in the digital age.



## THE AFFILIATE CHESS GAME:

# Ransomware's Recruitment Rush

The ransomware ecosystem is undergoing a significant transformation, propelled by the strategic recruitment of affiliates. This shift focuses on how ransomware operators innovate to attract and retain the best cybercriminal talent, especially in the wake of disruptions to groups like AlphV and LockBit.

## The Battle for Talent in the Underworld

In the shadowy realm of ransomware, the battle lines are drawn not just around technology and targets but in a high-stakes game of affiliate recruitment.

### Ransomware's Recruitment Models

#### The Standard Cut:

Historically, ransomware operators have adhered to a revenue-sharing model, offering affiliates a significant percentage of the ransom payments. This model has been the backbone of ransomware operations, incentivizing affiliates to launch successful attacks. Typically, operators retain a share (often around 20-30%) of the ransom, while the executing affiliate takes the lion's share.

#### Innovative Incentives:

However, the landscape is evolving. Operators now offer more than just a share of the ransom—they're crafting unique propositions to lure top-tier talent. RansomHub, for example, disrupts the traditional model by offering a staggering 90% cut to affiliates, with the added twist of requiring payment upfront. This approach not only attracts affiliates but also ensures their loyalty and commitment to the success of each attack.

## The Shift in Affiliate Allegiances

In the aftermath of AlphV and LockBit's operational disruptions, a noticeable migration of affiliates has occurred. Many of AlphV's former affiliates, left adrift by the group's exit scam, have found new homes among rising stars like Play, Akira, and Hunters. Play, in particular, has seen a meteoric rise, bolstered by an influx of experienced affiliates seeking refuge and opportunity. Their ascent highlights a broader trend: The ability to attract and retain skilled affiliates is now a critical determinant of a ransomware operator's success. RansomHub also succeeded to attract AlphV's affiliates.

The migration of affiliates underscores a dynamic shift within the ransomware ecosystem, where the ability to attract and retain skilled operators can dictate the rise and fall of these digital syndicates. As the landscape continues to evolve, the strategies employed to woo affiliates will undoubtedly become more sophisticated, further intensifying the competition among ransomware operators.



## SPOTLIGHT:

# Change Healthcare Incident

The ransomware attack on Change Healthcare has emerged as a defining moment in the realm of healthcare cybersecurity, drawing comparisons to the “Colonial Pipeline attack” due to its extensive repercussions. Orchestrated by an affiliate of AlphV, a notorious ransomware group known for its sophisticated cyberattacks, this incident has cast a spotlight on the technical concentration risk in the vendor ecosystems.

Change Healthcare, a cornerstone in the healthcare infrastructure, provides a wide array of administrative, financial, and clinical information exchange services. This makes it a repository of vast amounts of sensitive patient data, financial information, and critical operational data for numerous healthcare providers. This meticulously planned ransomware attack paralyzed Change Healthcare’s critical services, echoing through the healthcare system by disrupting data exchange, billing, and clinical operations.

## ALPHV’S EXIT SCAM: The Underlying Connection

The Change Healthcare ransomware incident unveils a deeper narrative tied to AlphV’s notorious exit scam. Following the breach orchestrated by an AlphV affiliate, the group’s unexpected disappearance and theft of ransom payments marked a pivotal moment in ransomware criminal operations. This act not only disrupted the traditional affiliate-core group dynamics but also left affiliates, including those involved in the Change Healthcare attack, in search of new harbors, such as emerging entities like RansomHub.

AlphV’s actions have rippled through the cybersecurity landscape, underscoring the complex and shifting threats posed by ransomware groups and their cascading impacts on industries and cybersecurity defenses.

### **Black Kite’s Proactive Response: Change Healthcare Client FocusTags™**

In the aftermath of the Change Healthcare ransomware incident, Black Kite swiftly mobilized to assist its clients through the innovative use of Change Healthcare Client FocusTags™. This strategic initiative exemplifies Black Kite’s commitment to providing timely, actionable intelligence in response to emergent cybersecurity threats.



## RansomHub's Emergence and the Change Healthcare Incident

In the evolving landscape of ransomware threats, RansomHub has quickly gained attention following its announcement that Change Healthcare fell victim to its operations. This declaration came in the wake of significant disruptions within the ransomware community, notably AlphV's exit scam.

RansomHub, distinguishing itself with a unique affiliate payment system, allows affiliates to first receive the ransom payment from the victim and then forward the operator's cut, offering an enticing 90% share to its affiliates. This model has attracted former AlphV affiliates among others in the cybercriminal sphere. Notably, the incident with Change Healthcare is solely an extortion attempt based on previously stolen data, with no second deployment of ransomware involved.

It is important to note that RansomHub did not provide any evidence (as of April 10, 2024) about their claim of having the data and the statement is a copy-and-paste from the original announcement made by AlphV.



## Potential impact due to Change Healthcare ransomware incident

Change Healthcare Client

██████████ has a vendor relationship with Change Healthcare

The BlackCat/ALPHV ransomware gang claimed responsibility for an attack on Change Healthcare, alleging they stole 6TB of data including sensitive information from healthcare providers, insurance providers, and pharmacies. The data reportedly includes medical records, insurance records, dental records, payment information, claims information, and personal identifying information (PII) of millions, including U.S. military personnel. UnitedHealth Group, owning Change Healthcare, has been working to restore services, with most pharmacies adopting new electronic claim procedures. Due to Change Healthcare position in the industry, companies and organizations getting service from Change Healthcare are at risk of data breach.

Given ██████████ vendor relationship with Change Healthcare, it's crucial to monitor the recent breach attributed to the BlackCat/ALPHV ransomware gang. The theft of 6TB of data, potentially including personal and medical information, raises serious concerns about privacy, regulatory compliance, and potential financial fallout. This incident could affect ██████████ operations and its obligations to protect client data, highlighting the need for rigorous cybersecurity measures and a reassessment of vendor risk management strategies.

### Recommended Actions:

- Urgently access if your data was compromised, focusing on sensitive personal, medical and financial records.
- Engage with Change Healthcare for breach updates and recovery efforts.
- Promptly inform affected clients and partners if your data was compromised, adhering to legal and regulatory guidelines.
- Review and bolster your cybersecurity defenses to guard against future threats.
- Advise impacted individuals to watch their accounts for any unusual activities.
- Ensure you're compliant with data protection regulations, preparing for any potential audits and investigations.
- Reevaluate the security measures of all your vendors to minimize future risks.

### References:

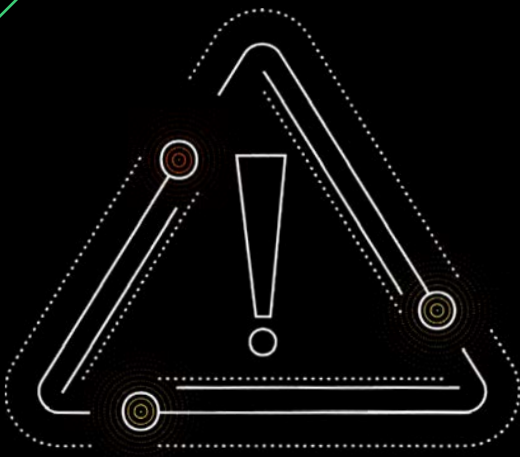
- [Ransomware gang claims they stole 6TB of Change Healthcare data](#)
- [Change Healthcare Blames "Blackcat" Group For Cyber Attack That Disrupted Pharmacies And Health Systems](#)

Date: March 1, 2024

Source for vendor relation: <https://support.changehealthcare.com/> ██████████

Black Kite's deployment of **Change Healthcare Client FocusTags™** not only underscores the importance of rapid response capabilities in the face of cyber threats but also highlights the value of tailored, data-driven insights in enhancing organizational resilience against ransomware attacks.

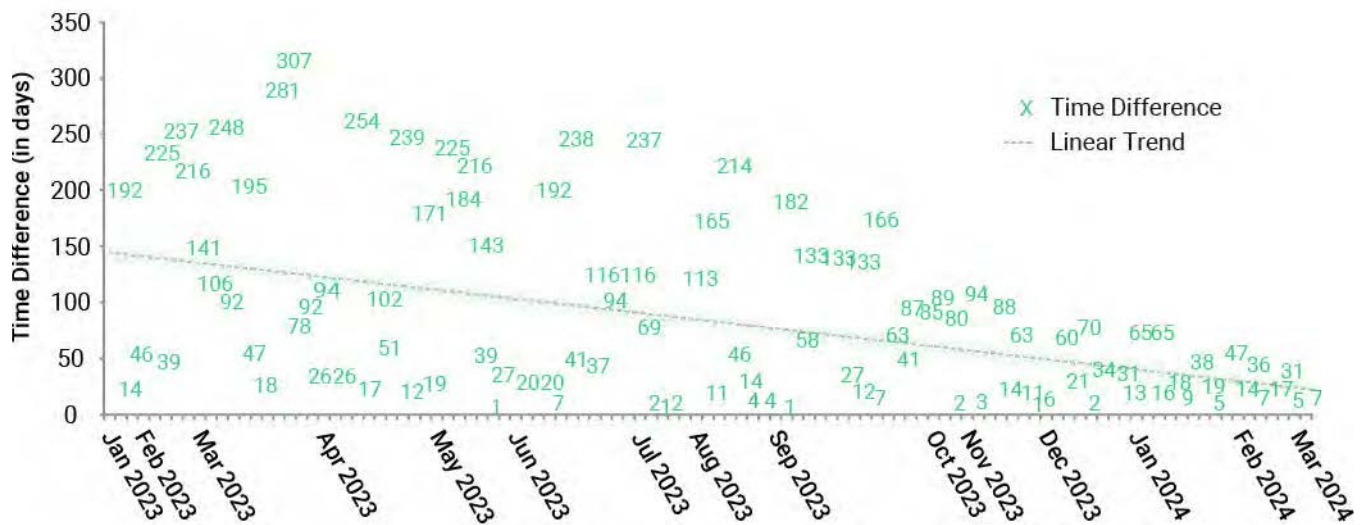
**LEARN MORE →**



# The Alarming Trend of Quick Succession Ransomware Attacks

The landscape of ransomware threats is evolving, as evidenced by a concerning trend: Companies are experiencing attacks in quicker succession by different operators. Our data indicates that 104 companies have fallen prey to two different ransomware operators, while a smaller number, three to be exact, have been unfortunate enough to be targeted by three groups. Our analysis reveals that while it's not uncommon for a company to face more than one ransomware attack, the shrinking time gap between such attacks is a relatively new and alarming development.

## The Difference Between Announcements of the Same Victim by Two Different Groups

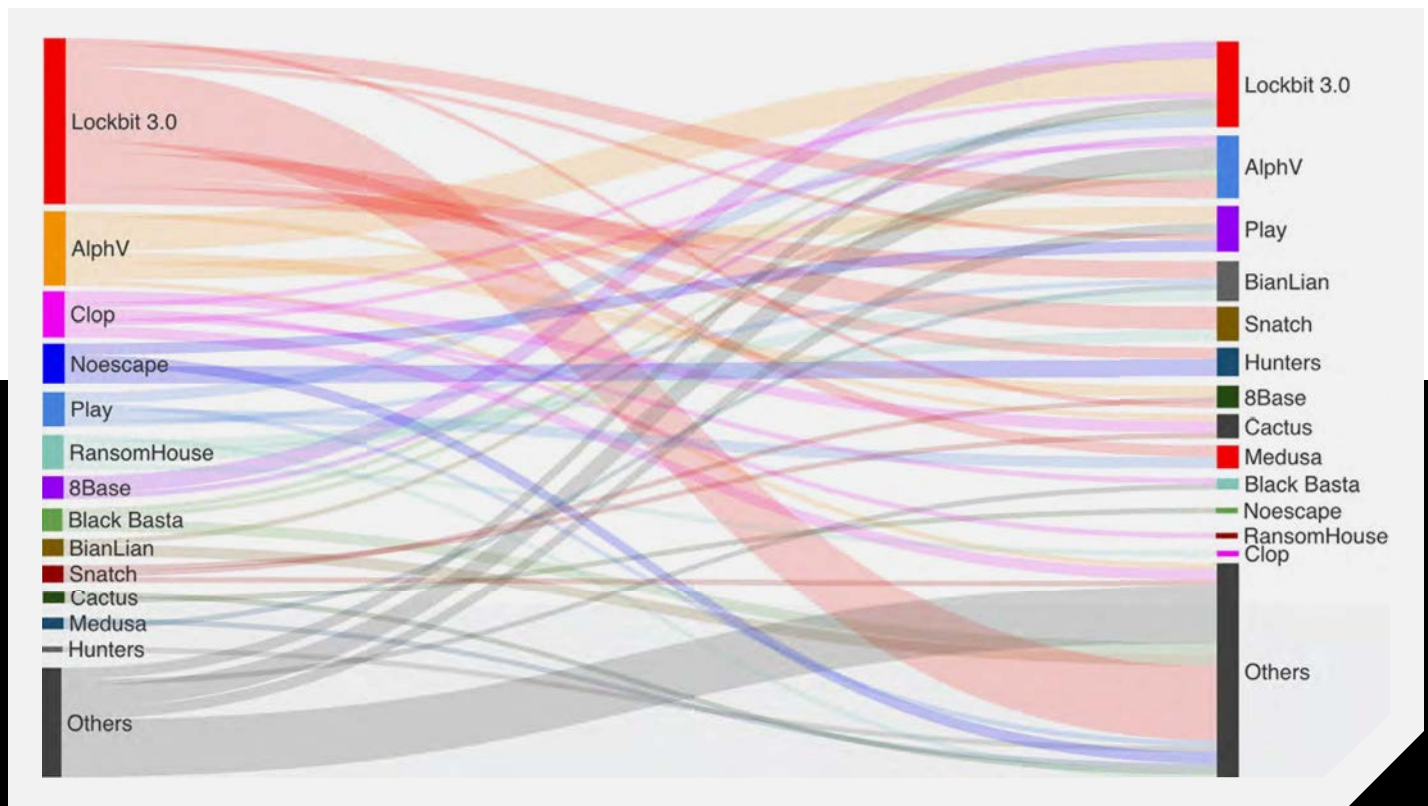


## AFFILIATE DYNAMICS:

# The Ransomware Crossover

The ransomware ecosystem is often depicted as a rigid hierarchy of operators and their foot soldiers. However, the data tells a different story, one of a fluid network where affiliates freely transition between groups, taking their skills where they find the best fit or opportunity.

## Victims Transitions between Ransomware Groups



### The graph illustrates affiliates working for multiple groups.

For instance, affiliates working with AlphV spread out to various ransomware operations, like tendrils seeking new soil, notably enriching the ranks of up-and-coming groups such as Play and 8Base. We can also witness that LockBit's affiliates also work with BianLian, Snatch, Hunters, Medusa, and so on. The affiliates do not believe in non-compete agreements.

# The Affiliate Marketplace

This movement paints the ransomware scene not as a collection of isolated groups but as a thriving marketplace. Here, affiliates are the currency, and their movement among groups like Cactus and others demonstrates a vibrant path that rewards versatility and adaptability.

## Why do we see the same company victimized by multiple ransomware groups?

There may be multiple reasons for the victimization by multiple ransomware groups:

- Ransomware affiliates may work with multiple RaaS providers, leading to multiple payloads from different groups in a single environment.
- Certain ransomware actors employ false claims to boost their influence, as seen in tactics by Snatch and RansomedVC.
- Collaboration among ransomware actors is common, partly due to the collectivist culture within Russian cybercrime circles, especially after the Ukraine invasion in 2022.
- Access to major ransomware programs like BlackCat is highly exclusive to guard against infiltration by adversaries of Russian state policies.
- LockBit has been known to support other groups like BlackMatter by sharing infrastructure, indicating a tradition of mutual aid among ransomware groups.
- Ransomware groups strategically target businesses with strong cyber insurance, exploiting knowledge of their policies to ensure payout.
- Technological convergence is occurring among ransomware groups, with shared platforms and tools leading to simultaneous exploitation of the same vulnerabilities.
- International sanctions and legal actions against cybercrime influence ransomware tactics, causing groups to rebrand, regroup, and then often launch high-profile attacks to establish their new identity quickly.

## OPINION:

# Dr. Ferhat Dikbiyik

Chief Research and Intelligence Officer

## The Rise of Multi-Operator Collaboration

As we observe the ransomware landscape adapt to recent disruptions, particularly the exit scam of AlphV, a curious pattern of multi-affiliate attacks on the same targets within a short timeframe has emerged. In my view, this isn't merely a coincidence or a result of disorganization within the cybercriminal ranks; rather, it appears to be a strategic evolution of ransomware affiliates.

## Diversified Risk and Increased Payouts

Post-AlphV, there's a rationale for affiliates to diversify their operations across multiple ransomware groups. I suspect that this move is a hedge against the risk of any single operator's downfall, ensuring they aren't left uncompensated. By spreading their efforts, they're not just guaranteeing a commission but potentially increasing their overall take.

This shift towards multi-operator collaboration is underscored by the trend of ransomware groups, both old and new, claiming the same victim. Such patterns are not merely haphazard; they are indicative of a more significant, possibly coordinated, strategic maneuver. These duplicated attacks could serve to maximize gains from entities that are insured and more likely to pay out.

## A New Phase of Cybercrime Collaboration

The affiliates' move to work with various groups could mark a new phase of cybercrime, one characterized by greater coordination and shared strategies amongst these threat actors. It's a sophisticated approach that pushes the boundaries of how ransomware groups operate, reflecting a quasi-industrial level of collaboration and competition within this digital underworld.

From my standpoint, this growing trend of ransomware groups targeting the same entities is a sophisticated mix of maximizing returns and mitigating risks. Affiliates are possibly taking a page from the business world, diversifying their "investment portfolio" of attacks to assure their payouts in a tumultuous ecosystem where alliances and power centers are rapidly changing.

The strategy of affiliates working with multiple ransomware groups is a significant development that could redefine the modus operandi within the ransomware community. As we watch this trend evolve, it's crucial for businesses to adapt their cybersecurity defenses, understanding that ransomware threats are becoming more complex and collaborative.

## THE GLOBAL RANSOMWARE MARKETPLACE:

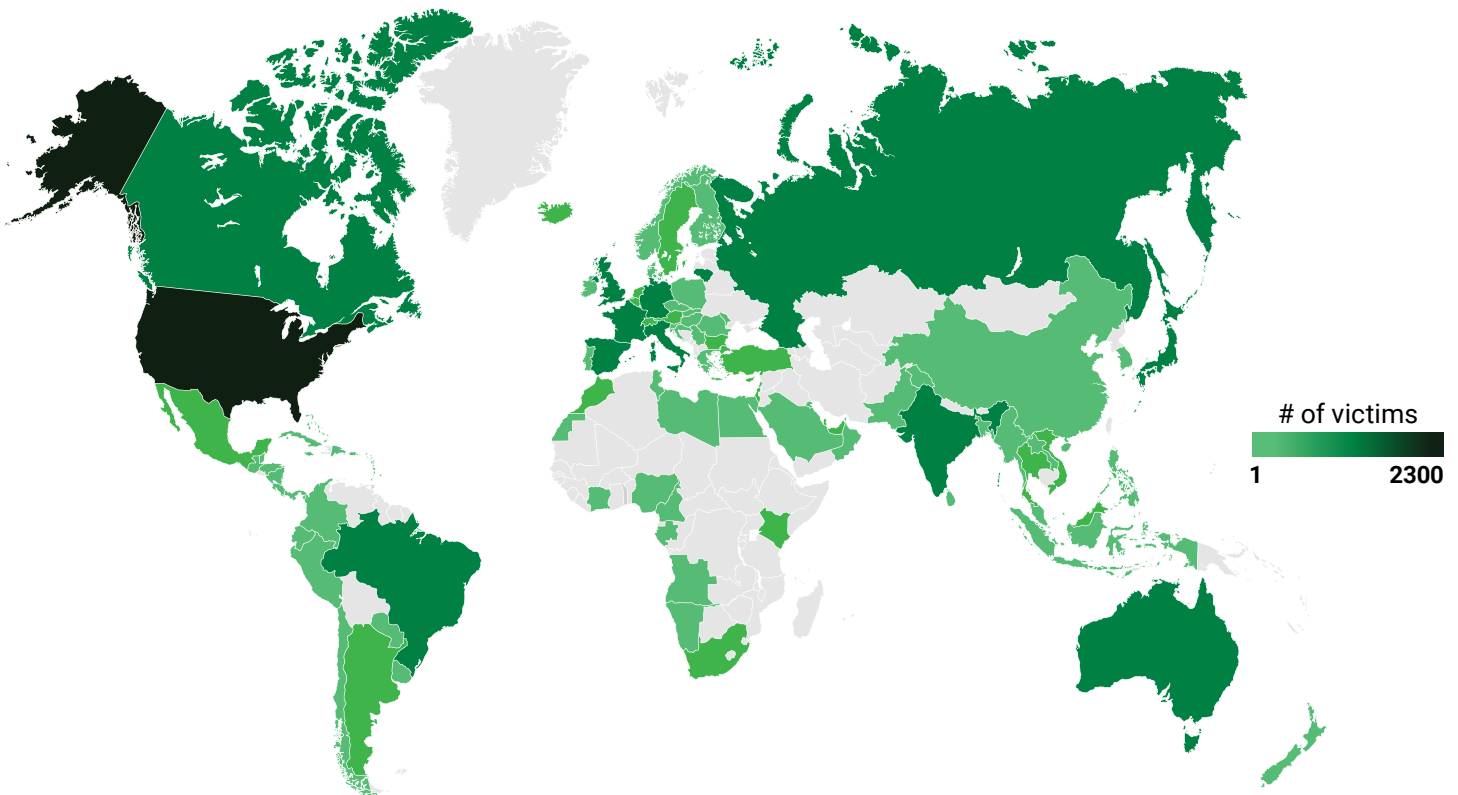
# Victim Profiling and Strategic Targeting

In aligning with our overall theme of ‘the business of ransomware,’ we delve into the data-driven world of cybercriminal targeting. This analysis unpacks the strategic selection of victims by geography, industry, and revenue and illuminates the business-minded tactics at play behind the digital threats.

## Geographic Landscape of Ransomware Victims

The geographical spread of ransomware victims tells a story of global impact, with certain regions bearing a heavier brunt. The United States sits at the epicenter, accounting for 47% of reported ransomware victims, indicative of the cybercriminals’ focus on lucrative targets within a nation deeply intertwined with global business networks.

### Number of Ransomware Victims: April 1, 2023 to March 31, 2024



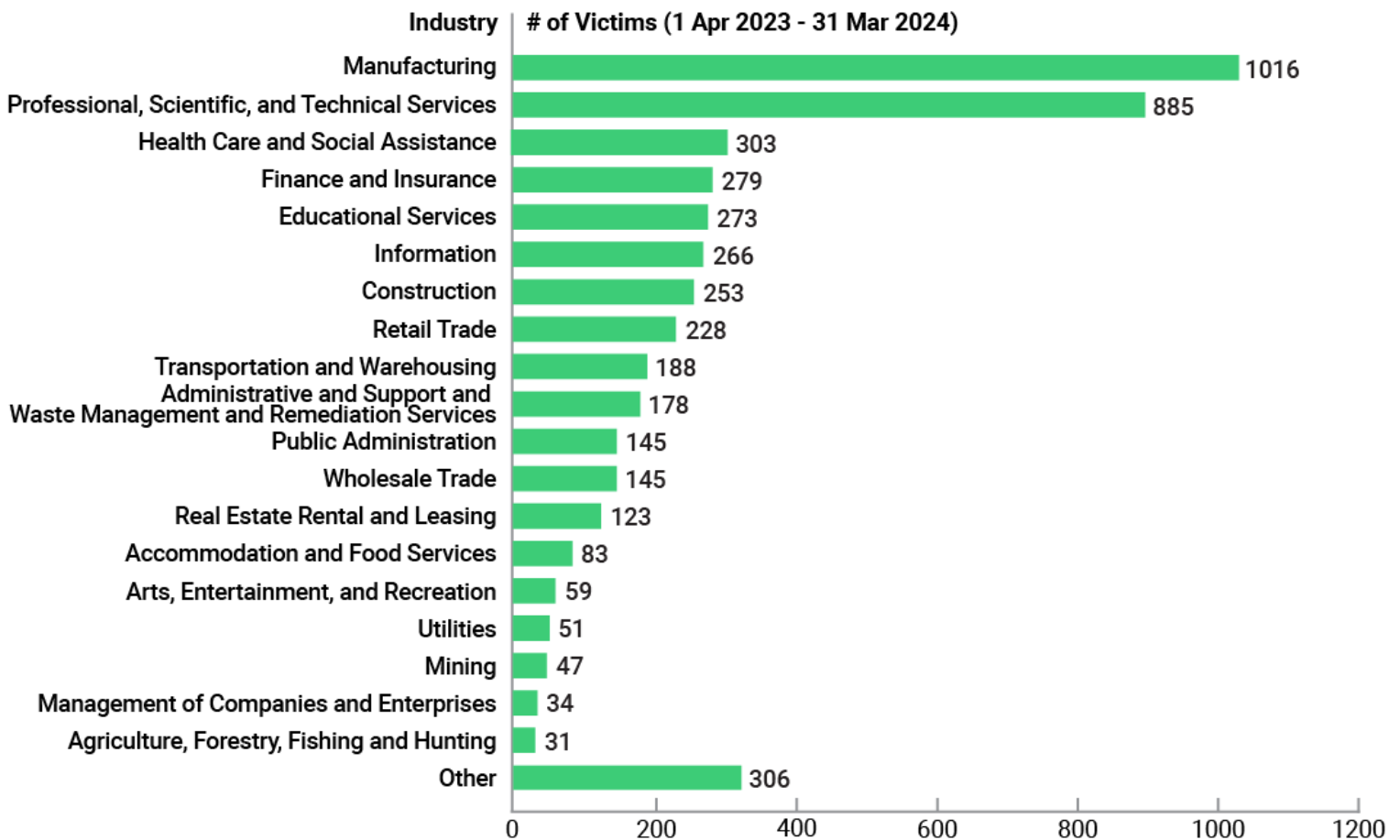
## Concentration in Economic Powerhouses

An analysis of the victim distribution reveals a pattern aligning with economic prominence. Following the United States, the United Kingdom, Canada, Germany, and Italy round out the top five nations affected. This concentration in economically developed nations mirrors the cybercriminals’ strategic targeting of entities within prosperous economies, where the potential returns from ransom demands are higher.

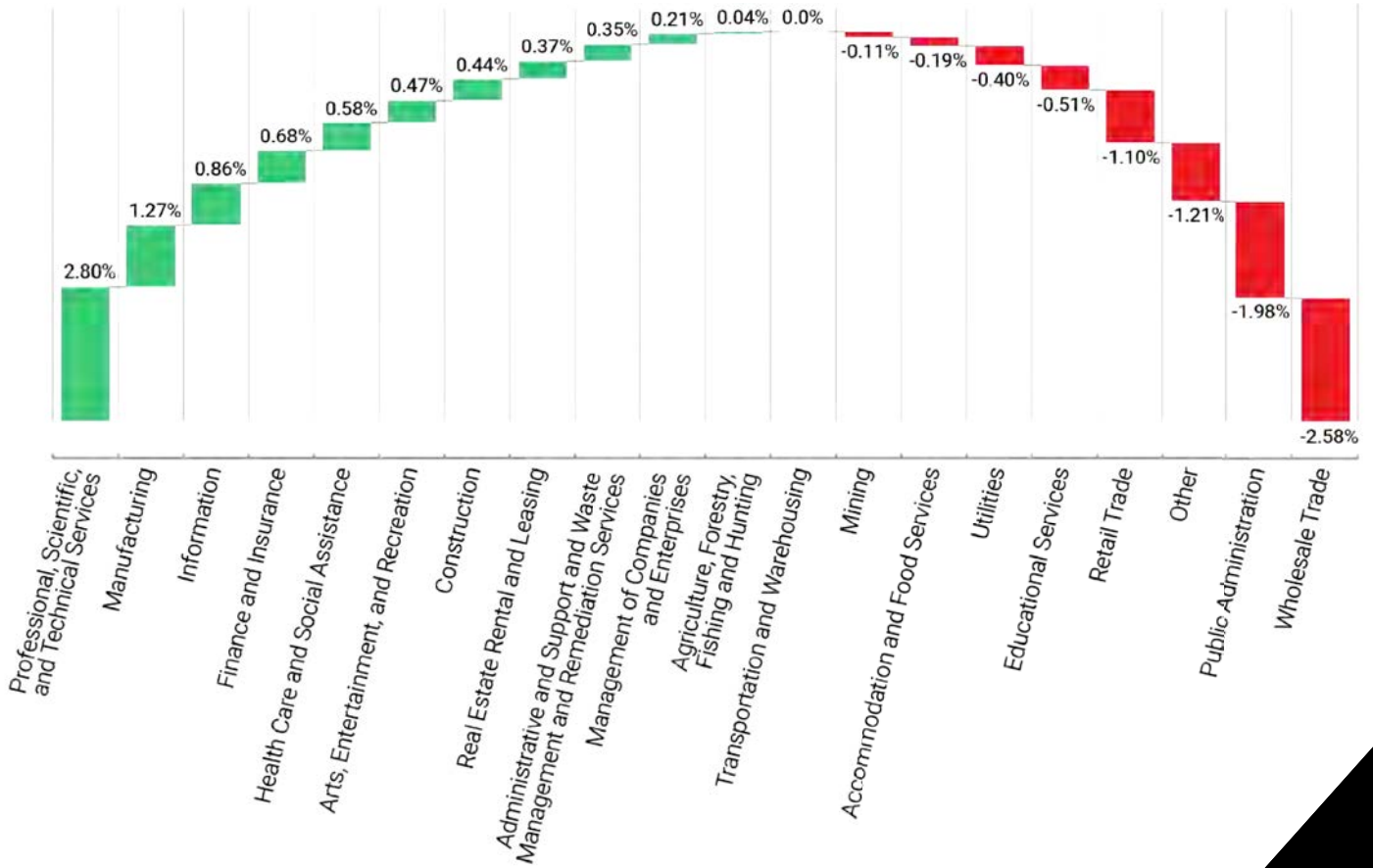
The geographical analysis paints a clear picture: Ransomware is a significant threat unconfined by borders, with its sights set squarely on countries that are keystones of the global economy.

# Calculated Industry Strikes

Ransomware trends indicate an ominous shift: Top sectors under siege are facing more pronounced attacks. Manufacturing, leading with 1,016 victims, notched up its share in total onslaughts, indicating the targeting of industries foundational to national economies. The Professional, Technical, and Scientific Services sector, with 885 victims, echoes this trend, revealing that ransomware groups are zeroing in on knowledge-driven domains.



## Percent Change of Compared to Previous Year





Industry	Rank (change)
Manufacturing	1 ↔
Professional, Scientific, and Technical Services	2 ↔
Health Care and Social Assistance	3 ↑ +2
Finance and Insurance	4 ↑ +3
Educational Services	5 ↓ -2
Information	6 ↑ +4
Construction	7 ↑ +2
Retail Trade	8 ↓ -4
Transportation and Warehousing	9 ↑ +2
Administrative and Support and Waste Management and Remediation Services	10 ↑ +2
Wholesale Trade	11 ↓ -5
Public Administration	12 ↓ -3
Real Estate Rental and Leasing	13 ↔
Accommodation and Food Services	14 ↔
Arts, Entertainment, and Recreation	15 ↑ +2
Utilities	16 ↓ -1
Mining	17 ↓ -1
Management of Companies and Enterprises	18 ↑ +1
Agriculture, Forestry, Fishing and Hunting	19 ↓ -1

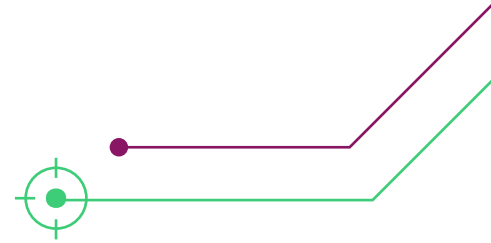
Healthcare and Finance, highly regulated and data-intensive industries, have climbed up the ranks to third and fourth with 273 and 266 victims respectively. This move is telling; major ransomware groups are strategizing, likely using intelligence tools to assess the lucrative nature of potential targets. The stakes are higher, the play more sophisticated, and the payoffs potentially larger in these data-rich pools.

The flip side? Not all attackers play this sophisticated game. Some, possibly less informed affiliates, hit softer targets like schools and nonprofits, entities less likely to yield financial rewards. Yet, the overall trend suggests a deliberate pivot by the top players: They're refining their aim, investing time to understand the value of their victims, signaling a deepening of cybercrime business acumen.

As we interpret these numbers, the narrative is clear: The gravity of attacks is intensifying where the data is dense and the regulations are tight. It's a telling sign that ransomware is not a random act of digital violence but a calculated business maneuver, with its crosshairs steadily trained on the most vital cogs of the industry wheel.

**Note that we use North American Industry Classification System (NAICS) codes for industries. The industries shown here are high-level (2-digit NAICS code) classification. In the next section, we provide a lower-level (4-digit NAICS code) industry classification breakdown.**

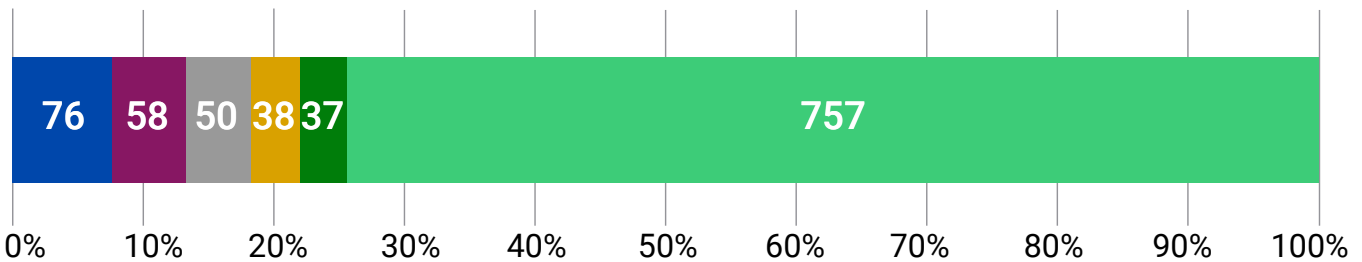
## MANUFACTURING SECTOR:



# A Ransomware Hotspot

The manufacturing sector's rapid digital transformation post-COVID-19 has inadvertently turned it into a prime target for ransomware attacks. Cybersecurity defenses, often robust against operational technology (OT) threats, have not kept pace with the sector's expanded digital footprint, leaving a chink in the armor for cybercriminals to exploit. The industry, which leads with over a thousand ransomware victims, faces unique challenges due to the operational disruption that halts production lines, causing significant financial and reputational damage.

## Manufacturing



The pressure exerted by halting a manufacturing line is not lost on ransomware groups. They recognize the cascading effect of disrupting supply chains, as elucidated in our 2024 Third-Party Breach Report, which ranks ransomware as the second leading cause of third-party data breaches. Delving into the manufacturing sub-sectors, the spread of ransomware is indiscriminate. Industrial Machinery Manufacturing tops the list with 76 victims, followed by Motor Vehicle Parts Manufacturing at 58, and Pharmaceutical and Medicine Manufacturing at 50. Electrical Equipment and Aerospace Product and Parts Manufacturing are not far behind, with 38 and 37 victims respectively, highlighting the cybercriminals' calculated approach to inflict maximum disruption across various facets of the industry.

- Industrial Machinery Manufacturing
- Motor Vehicle Parts Manufacturing
- Pharmaceutical and Medicine Manufacturing
- Electrical Equipment Manufacturing
- Aerospace Product and Parts Manufacturing
- Others

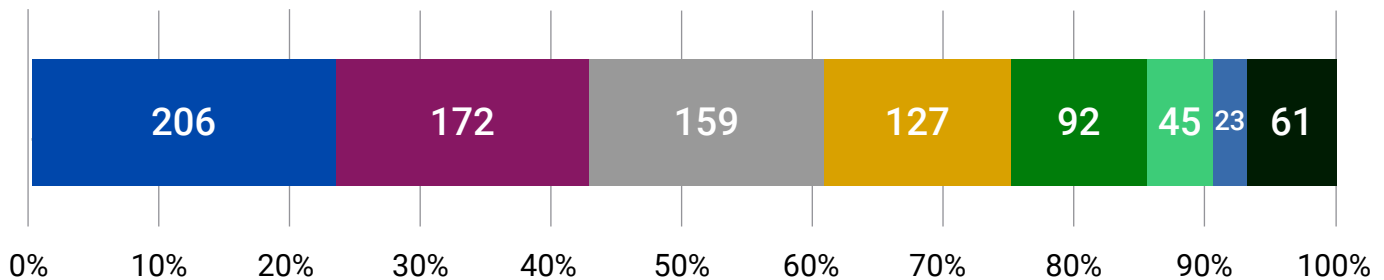
**This assault on manufacturing is a clarion call for the sector to fortify its cyber defenses, aligning its security posture with the evolving threat landscape to mitigate the risk of becoming the next ransomware statistic.**

NAICS Code: 31 - 33

# Targeting Knowledge: The Vulnerability of Professional Services

The Professional, Scientific, and Technical Services sector stands as the second-most targeted industry, maintaining this dubious honor over the past three years with nearly 900 victimized entities. This sector spans a diverse range of expertise, yet certain subindustries have been hit harder than others. 23% of the incidents have been recorded against legal services alone, which isn't surprising given the sensitive nature of the data they handle. Law firms are attractive targets for ransomware due to the high-value information they possess, which, if compromised, can have far-reaching consequences.

## Professional, Scientific, and Technical Services



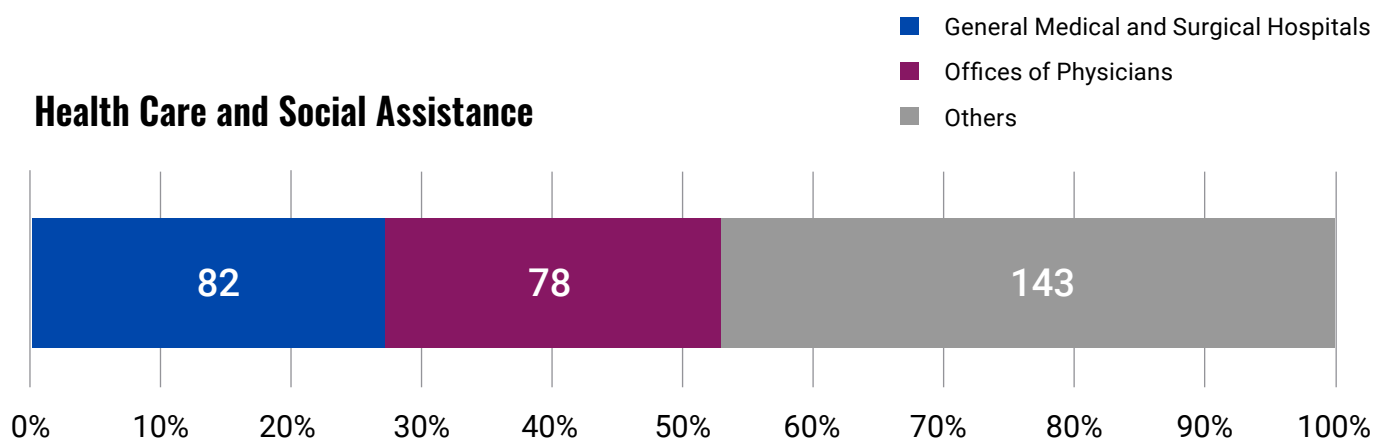
Following close behind, the Computer Systems Design and Related Services subindustry has seen about 20% of the victims. These are the very entities that weave the digital fabric of our businesses and infrastructures, making them critical nodes in the supply chain. Cybercriminals are astutely aware of the domino effect that can be triggered by compromising these firms, indicating a strategic, calculated approach to their attacks. As ransomware groups continue to refine their methods, it becomes increasingly clear that no sector is immune, and the custodians of our digital infrastructure must remain ever-vigilant.

**NAICS Code: 54**

- Legal Services
- Computer Systems Design and Related Services
- Architectural, Engineering, and Related Services
- Management, Scientific, and Technical Consulting Services
- Accounting, Tax Preparation, Bookkeeping, and Payroll Services
- Advertising, Public Relations, and Related Services
- Scientific Research and Development Services
- Other Professional, Scientific, and Technical Services

# Healthcare Under Siege: The Escalating Ransomware Threat

The health sector's battle with ransomware is intensifying. While hospitals are frequently spotlighted as prime targets, the scope of vulnerability extends far beyond their walls. In fact, 0.6% more healthcare entities were affected this year than last, with doctor's offices and small clinics comprising a significant portion of the victims. These smaller practices, often lacking the robust cybersecurity defenses of larger hospitals, present a soft target for ransomware groups.



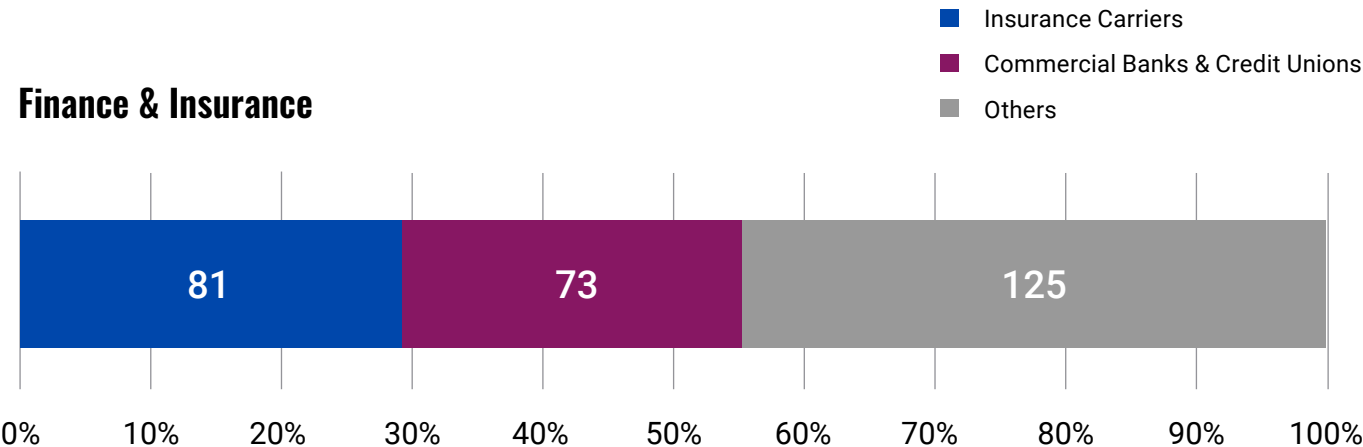
The impact of such attacks is profound: Healthcare services are disrupted, and the theft of sensitive patient health information (PHI) provides cybercriminals with considerable leverage. The ability to apply pressure on healthcare providers to meet ransom demands is compounded by the critical nature of the services they render. This vulnerability is not just a breach of data; it's a direct threat to patient welfare and a stress test for the resilience of healthcare infrastructures against the rising tide of cybercrime.

**NAICS Code: 62**

# Finance and Insurance on the Ransomware Frontline

Within the financial battlegrounds, insurance carriers and commercial banks endure the brunt of ransomware attacks, comprising 20% and 18% respectively of the sector’s breaches. Such institutions represent a tantalizing jackpot for cybercriminals due to the significant capital and sensitive data they harbor. The consequential 0.7% increase in attacks within the finance and insurance sector compared to the previous year echoes a persistent cyber risk narrative: Monetary gain and data-rich targets yield a high return for threat actors.

## Finance & Insurance



In the shadows of cyber threats, every percentage point reflects a multitude of disruptions, potentially spiraling into economic repercussions. Insurance carriers, with their expansive data pools and pivotal role in risk mitigation, present a problem when they fall victim to ransomware. Similarly, banks and credit unions serve as the lifeblood of cash flow; a cyber-attack impeding their operations sends ripples across the financial ecosystem. Ransomware groups, with their finger on the pulse of economic vulnerabilities, have recalibrated their crosshairs, aiming with precision to exert maximum pressure where resilience seems the most robust yet vital.

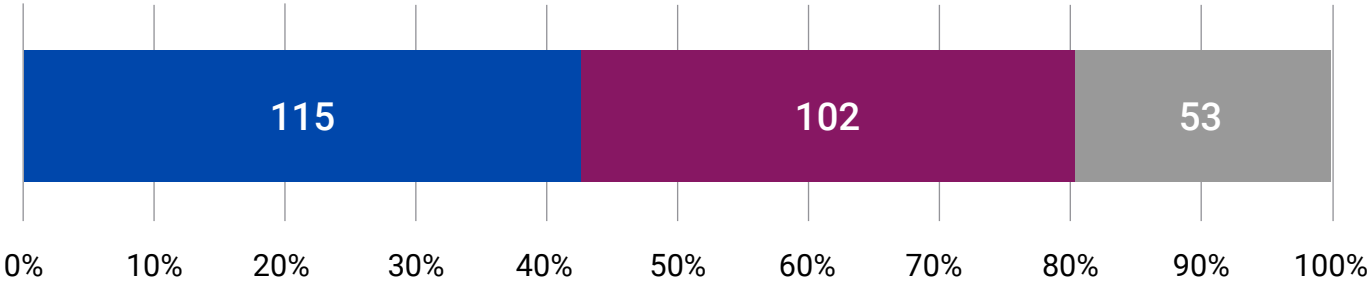
**NAICS Code: 52**

# Ransomware’s Educational Imprint: Disruptions in Academia

In the educational arena, higher education institutions form the nucleus of ransomware attacks, reflecting close to a third of all incidents within the sector. This trend not only spotlights the value of intellectual property and research data prevalent in universities but also underscores the vulnerability of their expansive networks. Cybercriminals, cognizant of the disruption potential, exploit these targets, fully aware of the institutions’ propensity to settle swiftly to safeguard their reputations and maintain operational continuity.

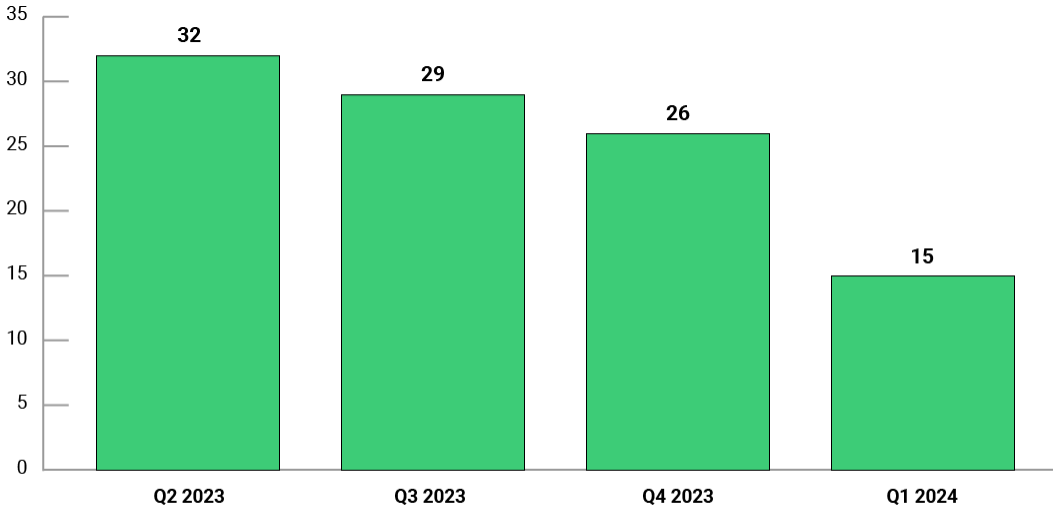
## Educational Services

- Higher Education
- K-12
- Other Educational Services



The narrative diverges when scrutinizing K-12 schools. While they account for a substantial 26% of educational breaches, their limited financial resources often translate to negligible ransom payouts. This economic reality shapes the tactical approach of seasoned ransomware operators, prompting a strategic pivot towards more lucrative educational echelons. Recent quarters illustrate this shift, with K-12 victim announcements halving from an average of 32 to a mere 15, a strategic retreat possibly indicating a newfound ransomware targeting ethos focused on return on investment.

### NAICS Code: 61



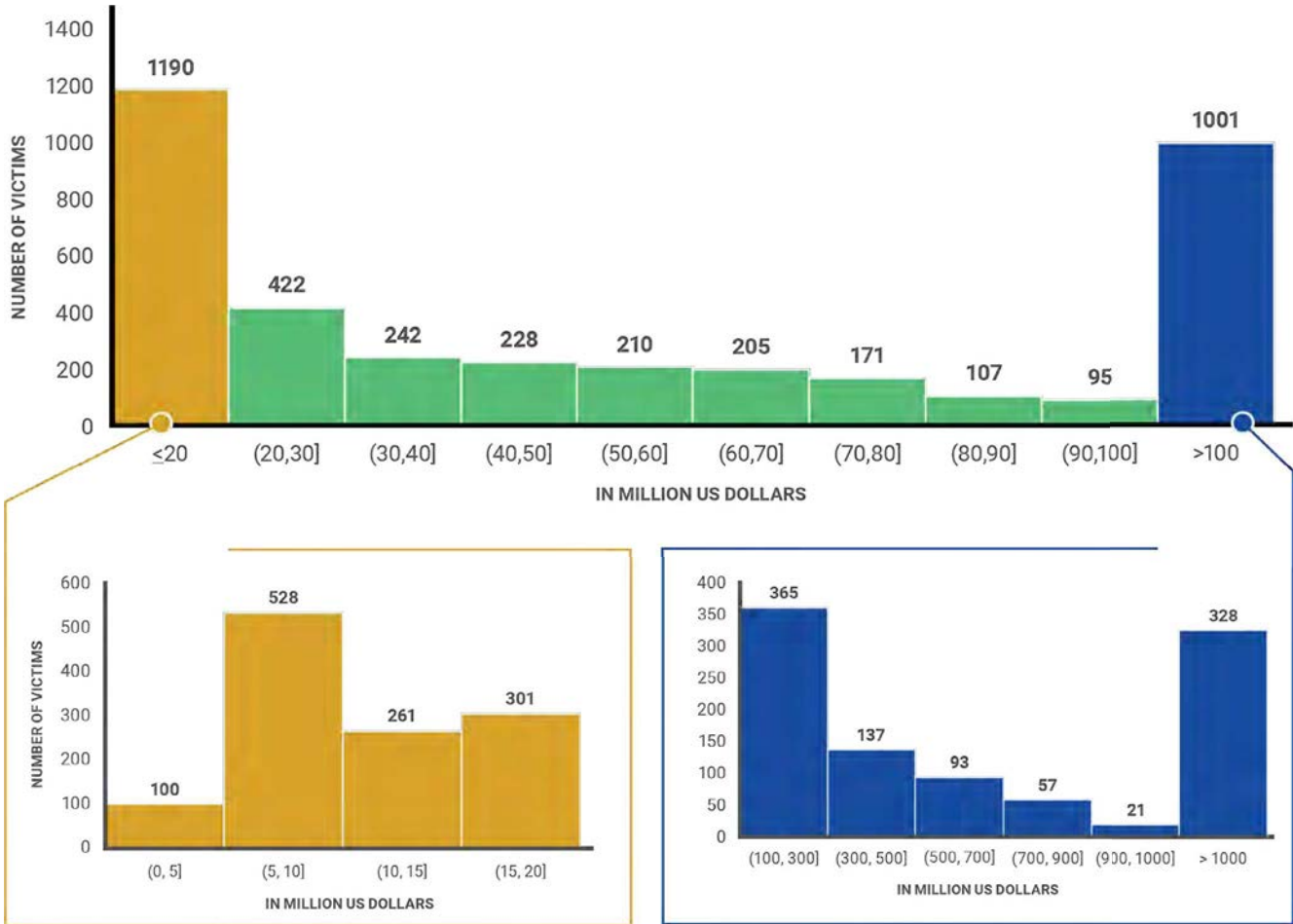
## EVALUATING THE BOUNTY:

# Ransomware Targets by Financial Footprint

Ransomware attackers are not just easy-target opportunists; they are methodical, sizing up their victims by their annual earnings. This section deciphers how attackers tailor their strategies based on the financial profiles of their targets. It's a high-stakes game where company revenues are weighed against the potential ransom payoff. Here, we dissect the correlation between a company's revenue and its attractiveness to cyber criminals, shining a light on the financial tiers most frequented by ransomware campaigns.



## Annual Revenue Distribution of Ransomware Victims



## Assessing Ransomware Targets: A Revenue Perspective

In the ransomware economy, victim companies' annual revenues paint a target on their back, but not always the ones you might expect. We delve into the surprising sweet spots for ransomware attackers, based on our analysis of 3,870 victims identified via open-source intelligence.

Ransomware attackers are casting their nets far and wide, yet their choice of targets often defies expectations. A significant 31% of ransomware victims, within our scope of revenue-identified entities, are organizations with less than \$20 million in annual revenue. This statistic challenges the narrative that only the richest are at risk, illuminating the vulnerability

of small to medium-sized enterprises (SMEs) in the face of cyber extortion.

Conversely, at the upper echelon, only 8.5% of victims boast annual revenues exceeding the \$1 billion threshold. This data point underscores a tactical preference within the ransomware community: targeting the more modestly sized companies that have enough liquidity to meet ransom demands but aren't prominent enough to consistently trigger aggressive law enforcement pursuit. This nuanced approach to victim selection reveals a calculated balancing act by ransomware operators, aiming to maximize payouts while minimizing risk and exposure.

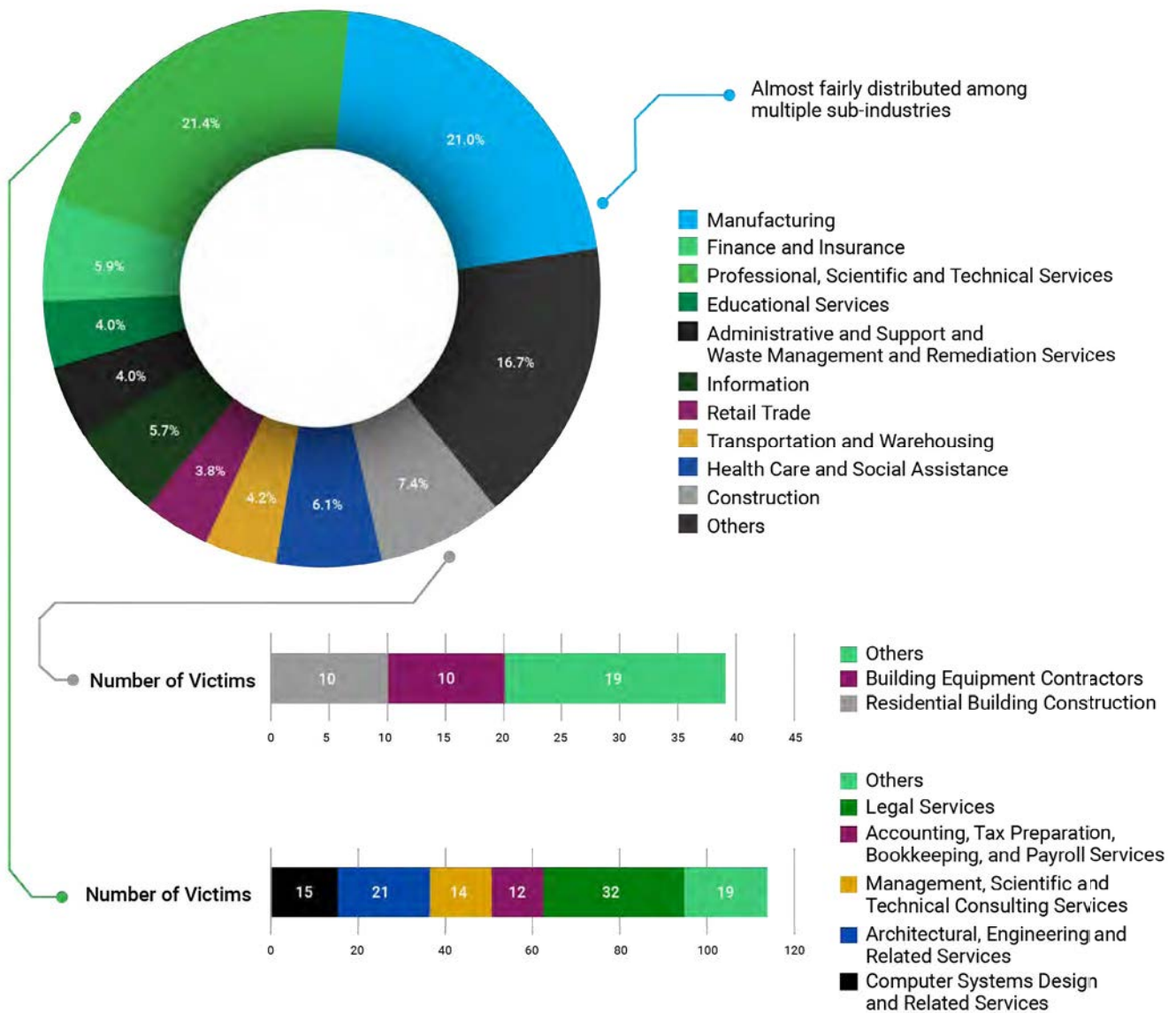


# Revenue Brackets and Industry Vulnerabilities

At the heart of ransomware target selection, annual revenue brackets offer a glimpse into the operational mindset of these digital marauders. We picked three brackets: (\$5M - \$10M) to represent the small-to-medium size companies, [\$100M - \$300M] for medium-sized companies, and over one billion dollars for large companies. These brackets have enough victims to analyze the industry selection.

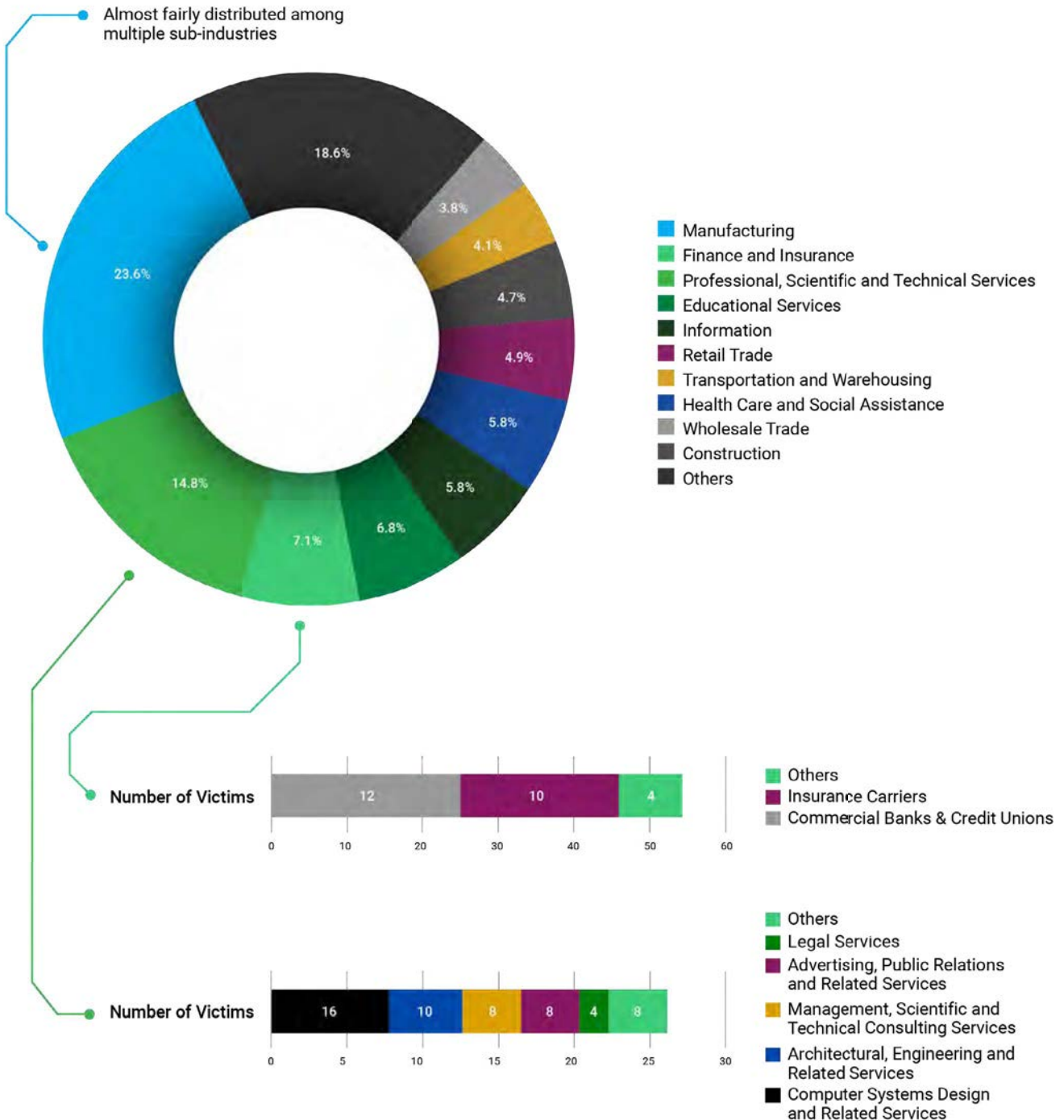
## Small-to-Medium Size [\$5M - \$10M]

For entities with revenues between \$5M and \$10M, the Professional, Scientific, and Technical Services sector endures the brunt of the onslaught, with legal services encountering heightened targeting due to the sensitive data they harbor. Manufacturing mirrors this sector's victim count, showcasing an expansive subindustry risk profile, while the construction sector holds a notable 7.4% victim share.



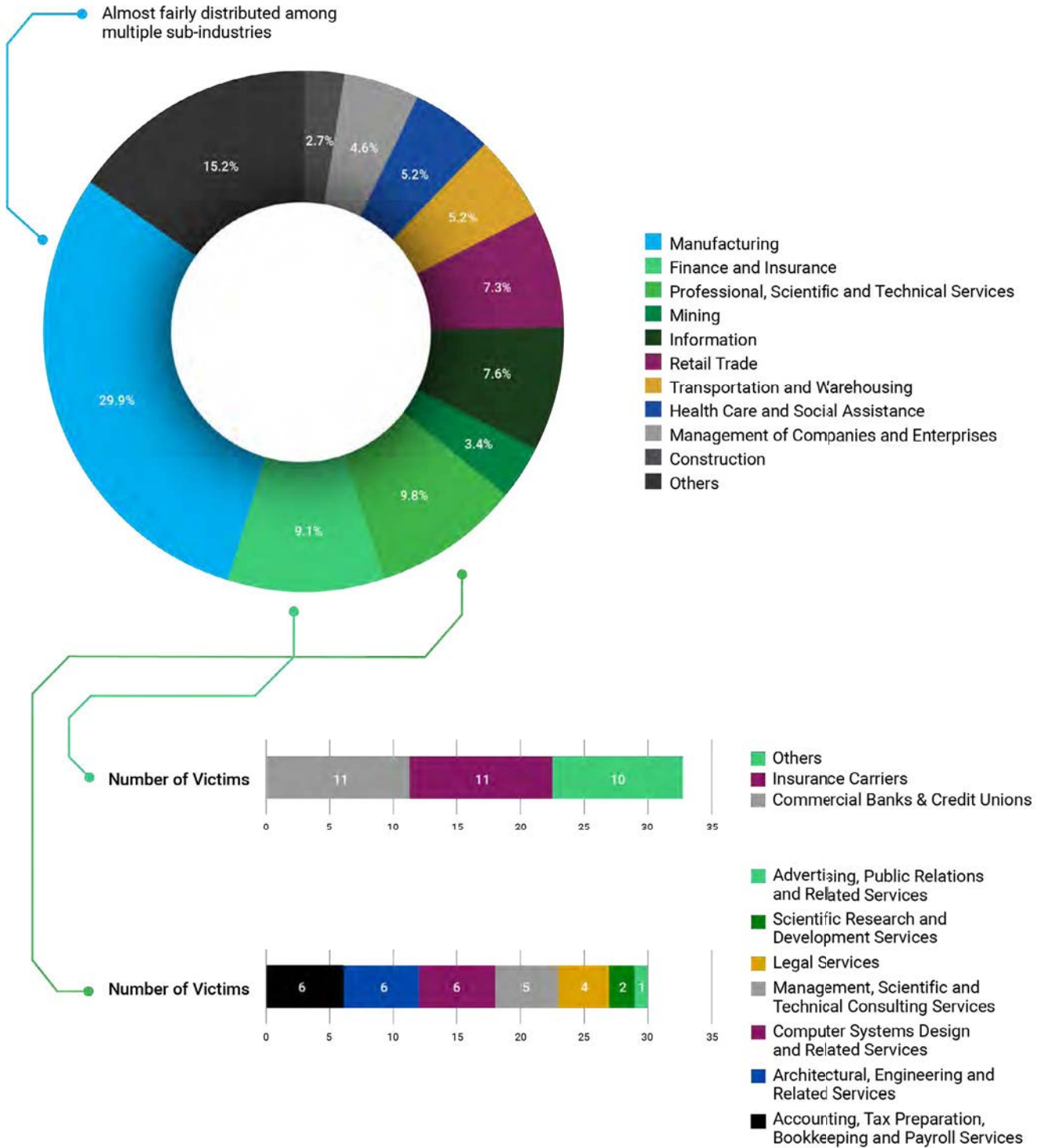
## Medium Size [\$100M - \$300M]

Climbing the revenue ladder to the \$100M to \$300M bracket, Manufacturing secures the top spot with 23.6% of attacks, spanning a broad industrial gamut. IT services emerge as prime prey within the Professional, Scientific, and Technical Services arena, accounting for a significant victim percentage. Not far behind, the Finance and Insurance sector represents 7% of the targets, with ransomware groups exploiting the substantial financial assets and regulatory pressures at play.



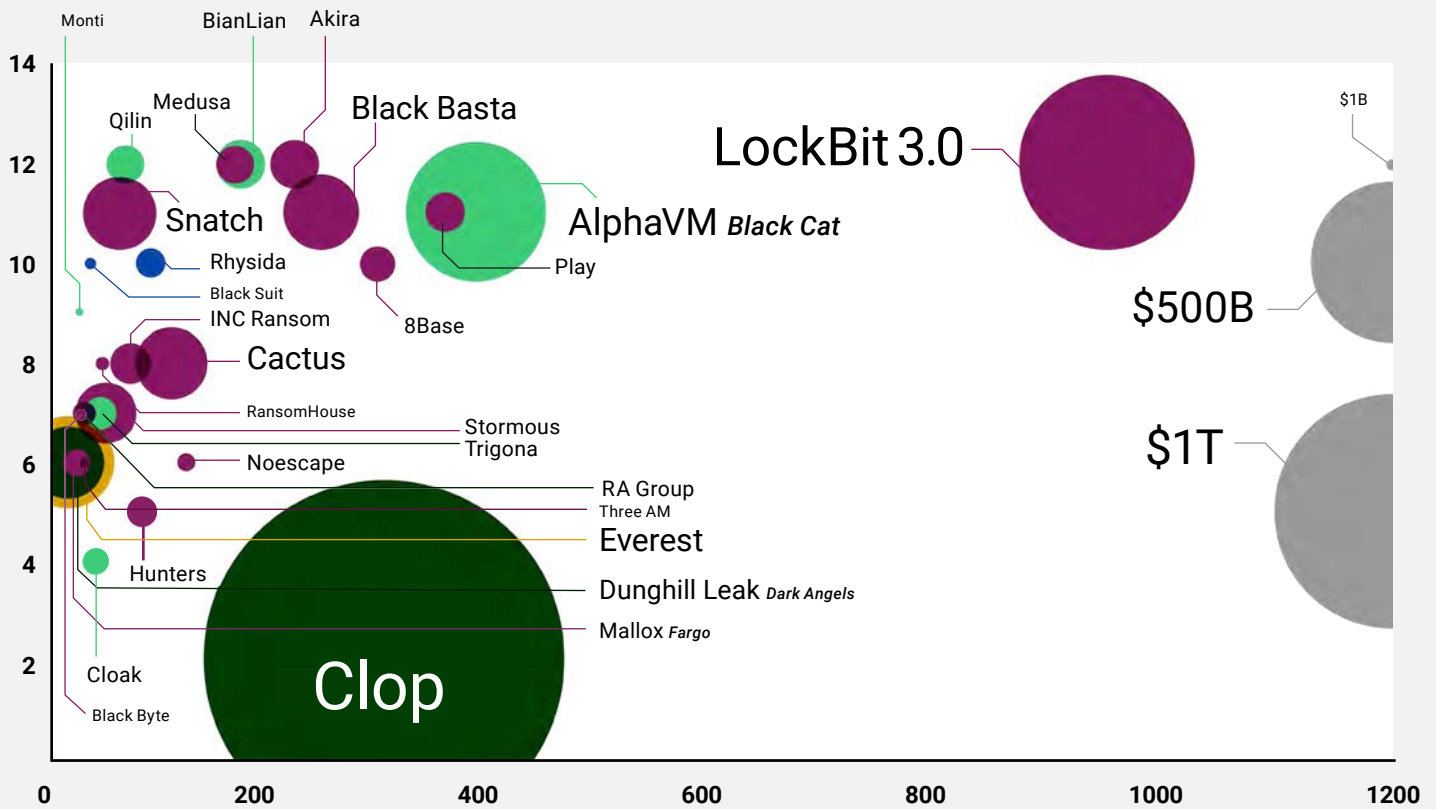
## Large/Enterprise Companies [>\$1B]

In the grander scale of companies exceeding \$1 billion in annual revenue, the Manufacturing sector continues to reign as the primary quarry, drawing nearly 30% of ransomware incidents. Finance and Insurance trail this sector's prominence in the ransomware economy at 9.8%, and Professional, Scientific, and Technical Services at 9.1%. Remarkably, three-quarters of the victims in this elite revenue range fall between the \$1 billion and \$10 billion mark.



# Financial Focal Points of Ransomware Syndicates

In the cyber threat landscape, ransomware groups vary widely in their operational vigor and the financial echelons they target. A granular look at the ransomware groups and the combined annual revenue of their victims reveals the depth and range of their reach into the corporate world's coffers.



- Information
- Manufacturing
- Professional, Scientific, and Technical Services
- Finance and Insurance
- Construction
- Educational Services

## OPINION:

# Dr. Ferhat Dikbiyik

Chief Research and Intelligence Officer

## Crafting a Corporate Veil:

### The Dichotomy of Ransomware PR

In the dark web's underbelly, ransomware groups like LockBit are not mere hackers; they're becoming corporate-like entities, paradoxically striving for ethical optics in an unethical landscape. Their public relations maneuvers (issuing formal apologies, crafting rules against hospital attacks, and even providing decryptors for breaches against their 'policies') paint a picture of cybercriminals with a conscience. But what lies beneath is a calculated move to preserve a facade of professionalism and mitigate backlash, all while enabling their affiliates' predatory activities.

Ransomware groups, notably LockBit, are acutely aware of their image. They market their incursions as 'post-paid pen testing services' and demonstrate a level of organization and rules reminiscent of corporate entities. When LockBit affiliates violate these rules, as in the cases of healthcare institutions in Germany and Canada, the group swiftly swings into damage control mode, offering decryption keys and apologies. This isn't altruism; it's image management. It's LockBit curating their brand in the digital underworld, walking a tightrope between appeasing law enforcement's gaze and maintaining affiliate loyalty.

The reality, however, is less polished than the PR spin. For each unauthorized hospital hack, for every statement distancing themselves from their affiliates' actions, the stark truth remains: LockBit's operations cause real harm. These moves are mere band-aids on the systemic issue of cyberattacks that disrupt critical services and endanger sensitive data. We see a group caught between maintaining control over unruly affiliates and a constructed identity of reformed cyber outlaws. It's a precarious balance, a performance where each misstep could spell a PR disaster, revealing the true chaos behind their carefully curated veneer.

As we analyze these cybercriminals' public statements and internal communications, it's clear they have adopted a twisted corporate speak, a dark mirror to the legitimate businesses they prey upon. These actions highlight a sophisticated understanding of perception management in the digital age, and they're setting a concerning precedent. With ransomware groups acting as pseudo-corporate entities, complete with customer service and PR spin, the cybercrime ecosystem is evolving into a more complex and nuanced domain. It is crucial for us to discern the genuine from the facade and the remorse from the strategic posturing as we navigate this new terrain of cyber threats.

## CASE STUDY:

# A Look at Ransomware's Impact on US Essential Industries

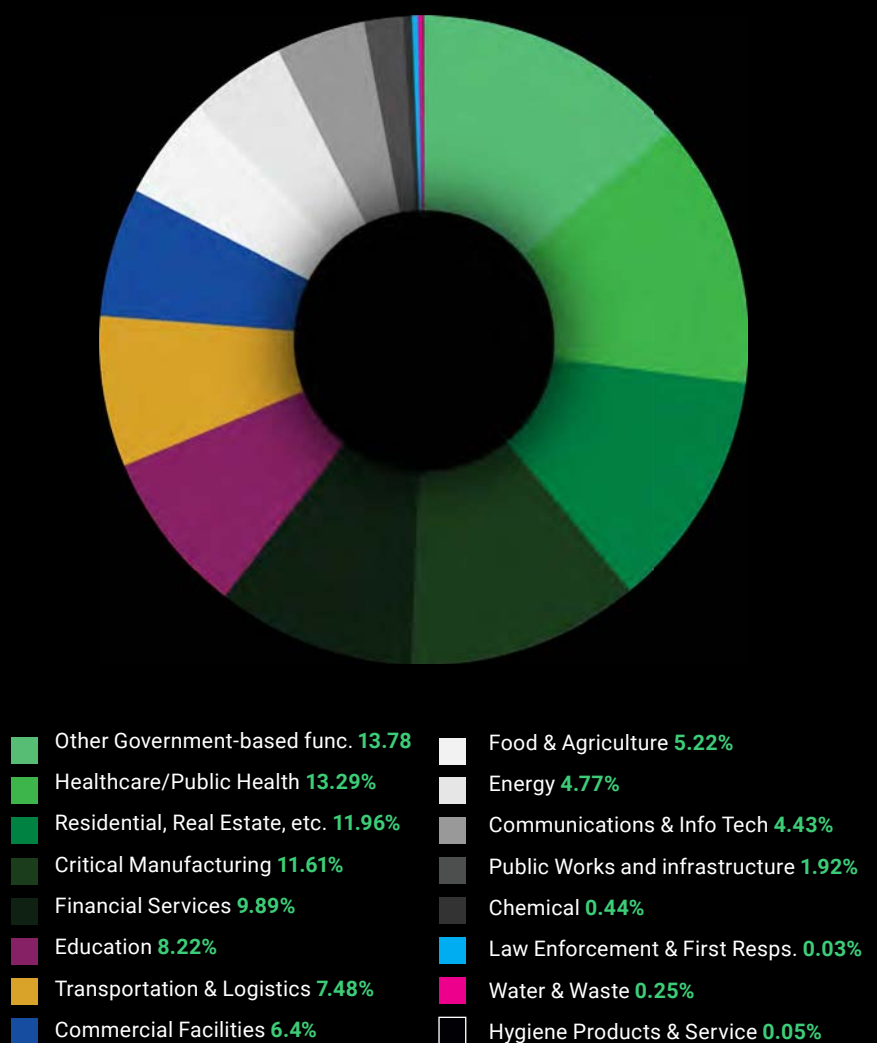
In the realm of cyber threats, essential industries are the lifelines that keep society functioning. This section provides an analysis of how ransomware has permeated the vital sectors that underpin our day-to-day lives. By aligning victim profiles with the Critical Infrastructure Sectors as defined by CISA, we gain insight into the cyber vulnerabilities of our most crucial services.

## Methodology:

To map the ransomware threat across U.S. industries, we've aligned victim company data with the Essential Critical Infrastructure Workforce Guidance from CISA, using NAICS codes to categorize companies into essential industry sectors. Essential Industries designated by CISA in the guidance encapsulates the critical infrastructure sectors. This methodology allows us to pinpoint and understand the ransomware risk landscape within these vital areas of our national fabric.

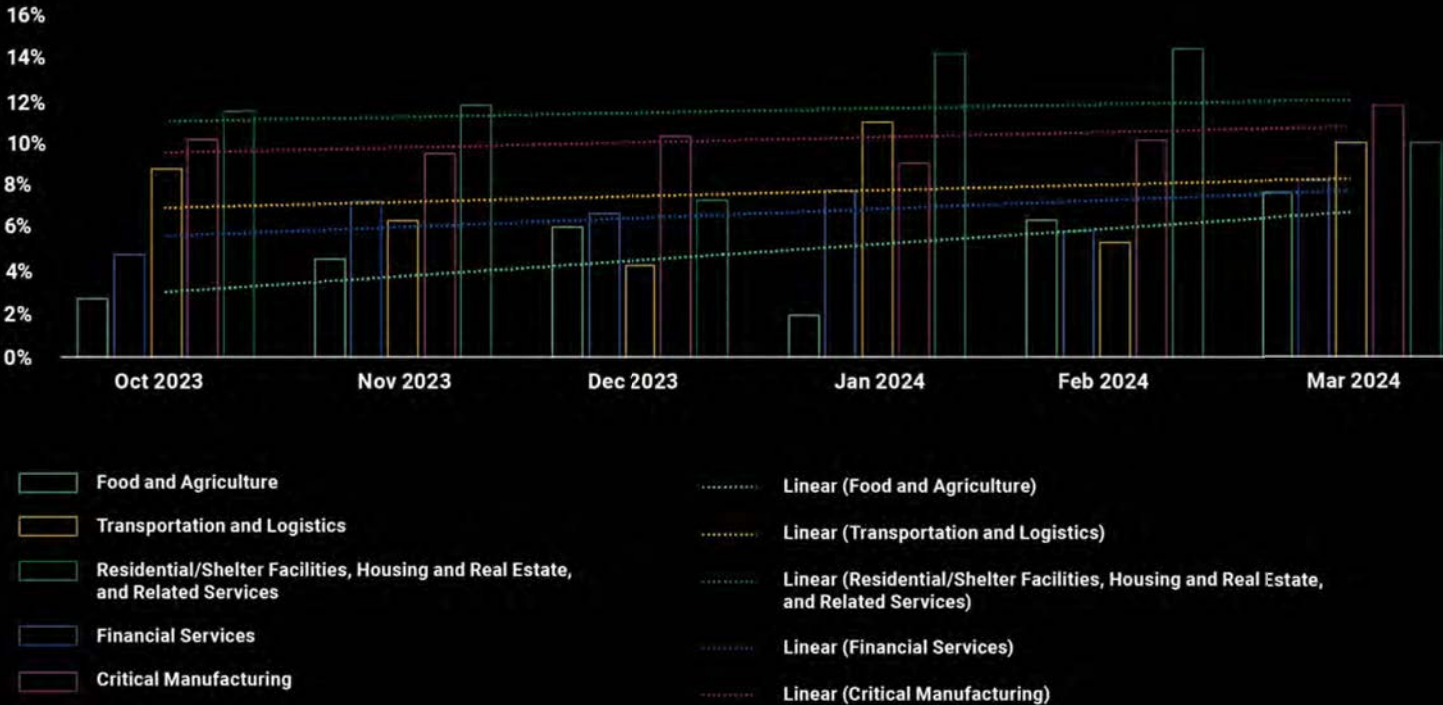
The infiltration of ransomware into America's essential industries is a pressing concern, with recent trends highlighting a shift towards sectors that form the backbone of daily life and national stability. This analysis examines the prevalence of ransomware across these critical sectors, revealing which are most at risk and underscoring the need for fortified defenses.

A Look at Ransomware's Impact on US Essential Industries



Drawing from a pool of 2,293 victims in the US, a staggering 88% are entities within essential critical infrastructure industries. Among the identified sectors, Healthcare/Public Health stands out, accounting for 13.29% of the affected entities. The sector’s pivotal role in community well-being makes it a significant target, with attackers likely aiming to exploit the urgent need for functional health services. Critical Manufacturing, making up 11.61%, is also a prime target, reflecting the potential for massive operational disruptions that can extend far beyond the initial breach. Residential/Shelter Facilities, Housing and Real Estate, and Related Services collectively bear 11.96% of ransomware incidents, a testament to the attractive disruption potential perceived by cyber adversaries within the places we live and work.

### Ratio Over Total Critical Infrastructure Victims



The data reveals an unsettling trend over the past half year, pointing to a rise in ransomware incidents within specific sectors. The Food and Agriculture sector, embodying the sustenance of the nation, has seen a marked increase in attacks, reflecting cybercriminals’ awareness of the disruptive power they wield. Financial Services, the bloodstream of the economy, continues to face persistent threats, indicating an ongoing risk to economic stability. Meanwhile, Transportation and Logistics, Critical Manufacturing, and Residential/Shelter Facilities, including Housing and Real Estate, emerge as rising areas of concern. These sectors, essential for the nation’s continuity and recovery in a crisis, are attracting more ransomware activity, a trend that merits close observation and swift protective action.





Notably, groups like CIOp have been exploiting the vulnerabilities in GoAnywhere and MOVEit en masse, while others, such as LockBit, take advantage of weaknesses like the CitrixBleed. Other frequent targets include vulnerabilities in Ivanti ICS, ScreenConnect, and Microsoft Exchange.

Credential stuffing is also a hot strategy. Hackers buy or find lists of usernames and passwords, trying them on different systems to get in. They might buy

these from Initial Access Brokers, the middlemen of the cybercrime world, who dig up and sell these digital break-in tools from Stealer Logs.

Phishing and social engineering tactics, although not as dominant as before, remain a threat. The [MGM Resort incident](#) serves as a stark reminder that a well-executed impersonation can still lead to significant breaches.

Open RDP/SMB ports are also highly utilized by the ransomware actors.

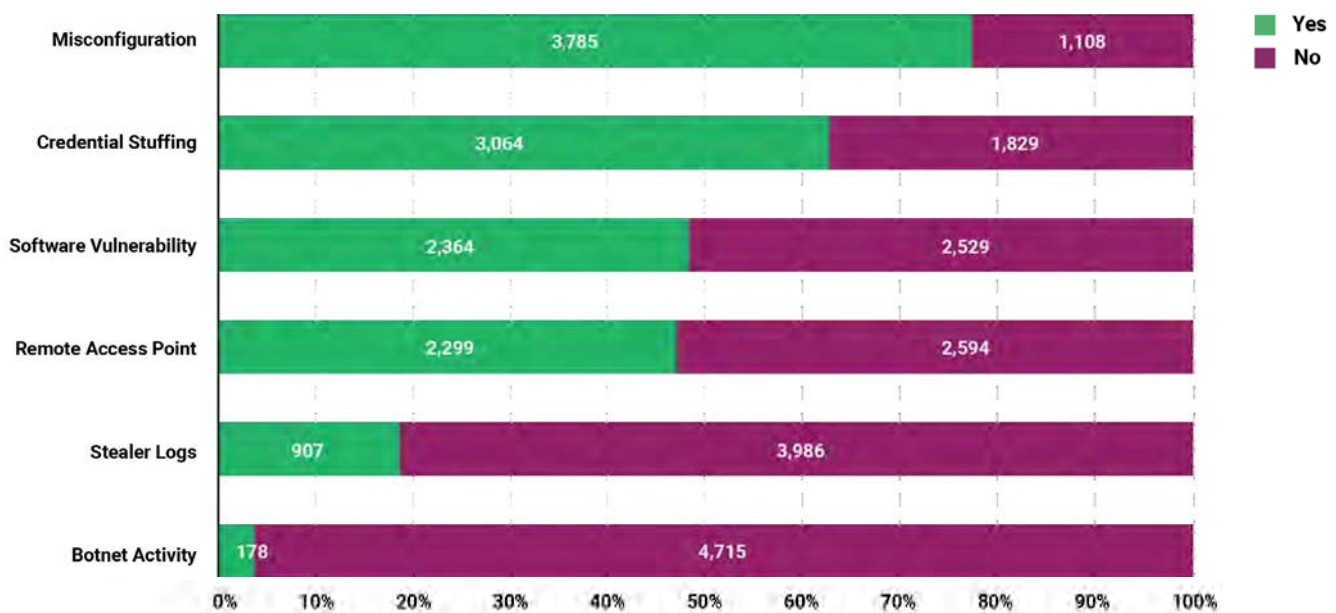
## Recognizing Ransomware Risk Factors

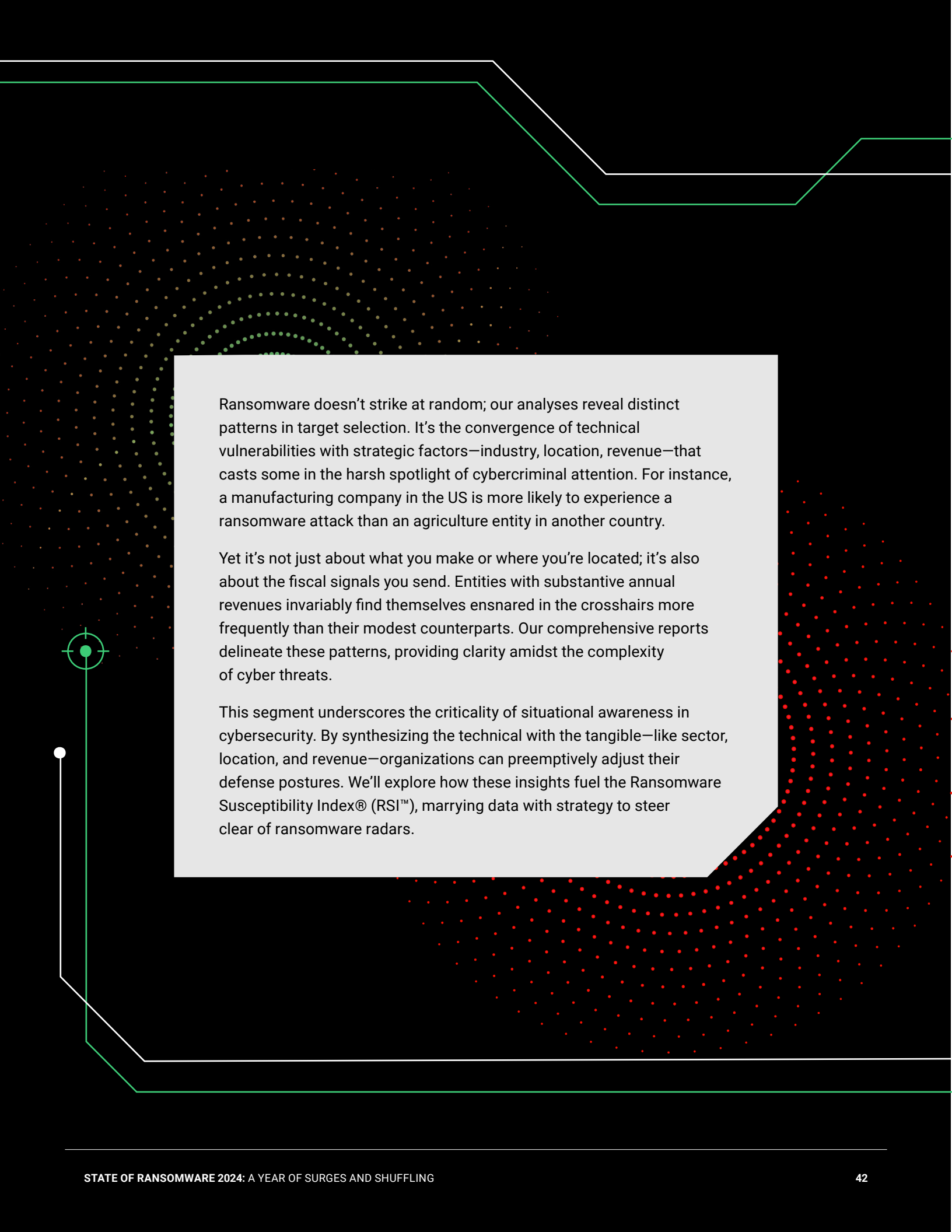
Within the digital landscape, certain indicators elevate the risk of attracting ransomware hunters. **Our analysis pinpoints these red flags that could potentially place an organization in the crosshairs.**

- **Exploitable Vulnerabilities:** Almost half of the victims had a critical vulnerability that was discoverable using OSINT techniques.
- **Leaked Credentials:** 3,064 victims had at least one credential leaked in the last 90 days prior to the attack. We also observed critical information exposed in Stealer Logs for 907 victims.
- **Misconfiguration on MX Servers:** More than 75% of the victims had a misconfiguration such as missing SPF or DMARC records before the ransomware attack was executed.
- **Open Access Points:** RDP/SMB ports were left unprotected in 2,299 cases.

The data showcases the prevalence of each indicator among past victims. It's crucial to note that while misconfiguration is the most observed issue, it doesn't necessarily serve as the primary entry point for attacks.

### Ransomware Indicators of Ransome Victims prior to Attacks





Ransomware doesn't strike at random; our analyses reveal distinct patterns in target selection. It's the convergence of technical vulnerabilities with strategic factors—industry, location, revenue—that casts some in the harsh spotlight of cybercriminal attention. For instance, a manufacturing company in the US is more likely to experience a ransomware attack than an agriculture entity in another country.

Yet it's not just about what you make or where you're located; it's also about the fiscal signals you send. Entities with substantive annual revenues invariably find themselves ensnared in the crosshairs more frequently than their modest counterparts. Our comprehensive reports delineate these patterns, providing clarity amidst the complexity of cyber threats.

This segment underscores the criticality of situational awareness in cybersecurity. By synthesizing the technical with the tangible—like sector, location, and revenue—organizations can preemptively adjust their defense postures. We'll explore how these insights fuel the Ransomware Susceptibility Index® (RSI™), marrying data with strategy to steer clear of ransomware radars.

# Understanding Ransomware Susceptibility

In the landscape of cyber threats, being on the radar of ransomware groups is akin to swimming in shark-infested waters; the longer you're there, the higher the chances of an attack. The Ransomware Susceptibility Index® (RSI™) serves as a beacon, guiding organizations away from these dangerous waters.

The RSI™, a measure refined through comprehensive data analysis, quantifies the likelihood of becoming a target. In this index, a metric between 0.0 and 1.0, considers both technical indicators, such as software vulnerabilities and leaked credentials, and contextual details, such as industry type, company size, and geographical location.

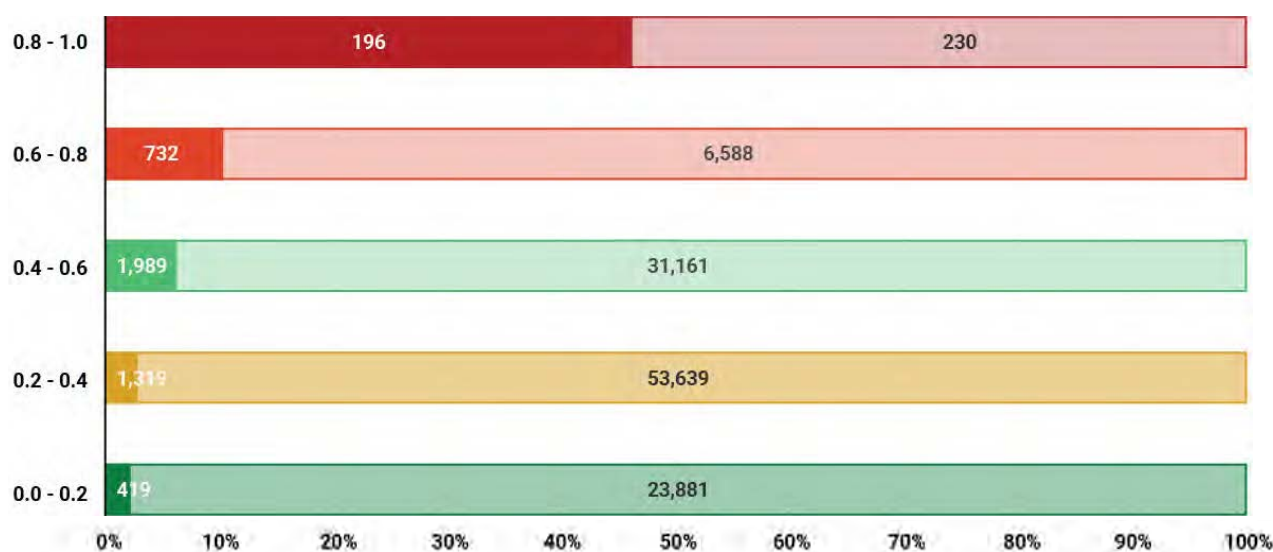
Black Kite's Ransomware Susceptibility Index® (RSI™) stands as a cutting-edge tool, finely tuned to gauge the probability of organizations facing ransomware attacks. This tool is meticulously updated to mirror the latest state of cyber threats by integrating a vast array of ransomware incident data from a comprehensive

database. The updated RSI™ leverages data analysis, pooled cybersecurity knowledge, and key factors such as the company's location, industry, and annual revenue, aligning them with the common attack vectors of ransomware to predict the risk more accurately.

When we analyze the RSI™ values of the victims right before the ransomware attack, we observe that most of them have an RSI™ value between 0.4 and 0.6 while the range of 0.8-1.0 has the least number of victims. To truly see the power of RSI™, we need to compare the companies in the same ranges that were not victimized by ransomware groups. For that purpose, we have added more than 120,000 non-victim companies to the analysis.

Among the companies whose RSI™ value is between 0.8 and 1.0, 46% experienced a ransomware attack. The ratio drops to 10% for the RSI™ values between 0.6 and 0.8, and 6% for the values between 0.4 and 0.6. These figures show that the higher the RSI™ value is, the more likely to experience a ransomware attack.

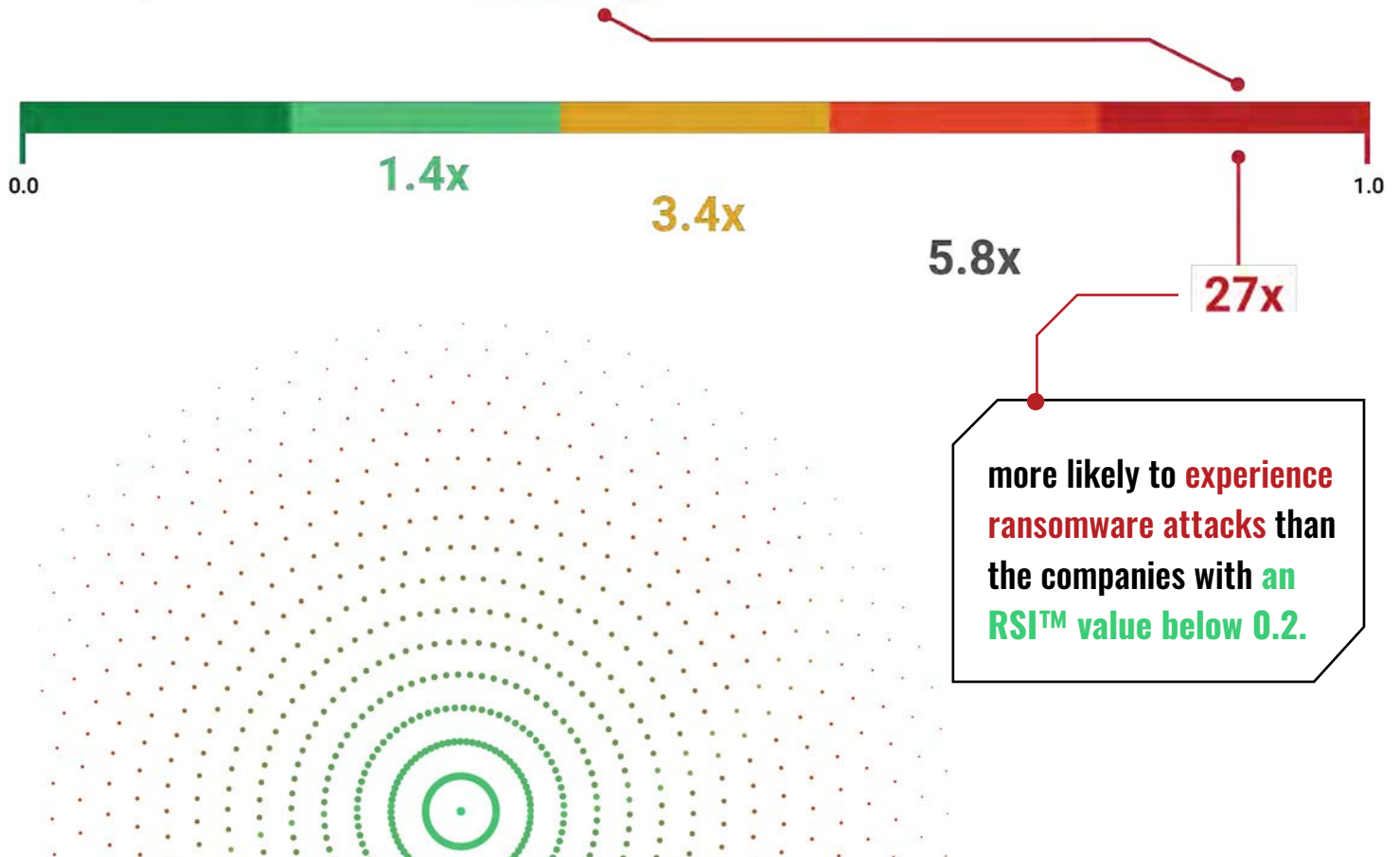
## RSI™ Distribution for Ransome Victims and Non-Victums



Victims are shown in solid colors, while the non-victims are shown in transparent colors.

When we did an analysis of the number from a comparative perspective, we can see that the companies with an RSI™ value above 0.8 are 27 times more likely to experience a ransomware attack than the companies with an RSI™ value below 0.2. The ratio becomes 5.8 times for the companies with an RSI™ value between 0.6 and 0.8, and it is 3.4 times for the RSI™ values between 0.4 and 0.6.

The companies with an RSI value **in this range** are



# How RSI™ Helps to Mitigate Ransomware Risk

Understanding how to use a company's RSI™ value can mean the difference between business disruption and smooth business operations.

The Black Kite [Ransomware Susceptibility Index®](#) indicates the likelihood of a ransomware attack on your organization or on an organization in your supply chain. RSI™ follows a process of inspecting, transforming, and modeling collected from a variety of OSINT sources (internet wide scanners, hacker forums, the deep/dark web and more). Using the data and machine learning, the correlation between control items is identified to provide approximations. With this tool you can understand which vendors are most prone to ransomware and create a mitigation strategy based on which vendors are most susceptible and would have the greatest impact on your business operations.

We recommend thinking about ransomware detection and response in three categories: prevention to minimize risk, mitigating risk in your third-parties and responding to an attack. We also offer some guidance on how to recover from an attack.

below 0.2.

# Prevention and Minimizing Ransomware Risk

## Internal Security Measures for Ransomware Prevention

Taking a proactive approach to internal security measures can greatly reduce the likelihood of a ransomware attack. Implement the following best practices to minimize the chances of an attack and ensure your organization is not an attractive target for ransomware groups:

- 1. Monitor Your Ransomware Indicators:** Keep track of your ransomware indicators to avoid being on the radar of ransomware groups. Regularly check for open critical ports, leaked credentials, email security configurations, and phishing/fraudulent domains.
- 2. Patch Management:** Ensure all systems, applications, and software are up to date with the latest patches, focusing on those with known remote code execution vulnerabilities.
- 3. Endpoint Security:** Implement strong endpoint security measures, including antivirus and anti-malware software, and consider deploying advanced solutions like micro VMs to prevent malware from spreading.
- 4. Email Security:** Strengthen your email security by implementing SPF, DKIM, and DMARC records, and conduct regular security awareness training to educate employees on how to identify and report phishing attempts.
- 5. Network Security:** Restrict remote access to your network by closing unnecessary ports, using VPNs, and employing strong authentication methods like multi-factor authentication (MFA).
- 6. Data and System Backup:** Regularly back up critical data and systems to allow for quick recovery in the event of an attack. Store backups both on-site and off-site, and consider using air-gapped storage for added protection. Test your backup and recovery processes periodically to ensure their effectiveness.
- 7. Incident Response Plan:** Develop and maintain a comprehensive incident response plan to address potential ransomware attacks, including clear roles and responsibilities, communication protocols, and recovery strategies.

**By implementing these internal security measures, you can reduce the likelihood of falling victim to a ransomware attack and minimize the potential damage if an attack does occur.**

# Mitigating Third-Party Ransomware Risk

To mitigate the risk of ransomware attacks due to third-party vendors, organizations should:

1. Evaluate the cybersecurity posture of third-party vendors using tools like Black Kite's Ransomware Susceptibility Index® (RSI™).
2. Require vendors to adhere to industry best practices and implement robust cybersecurity measures.
3. Perform regular audits of vendors' security practices and provide guidance for improvement if necessary.
4. Foster a culture of collaboration and information sharing among vendors to enhance overall cybersecurity.

## RESPONDING TO A RANSOMWARE ATTACK

In the event of a ransomware attack, taking immediate action is critical to mitigate the damage.

### Steps to take when hit by a ransomware attack include:

1. Isolate affected systems to prevent the spread of the ransomware.
2. Notify relevant authorities and stakeholders.
3. Engage with cybersecurity experts to assess the situation and explore potential remediation options.
4. Preserve evidence and document the incident for future reference and potential legal actions.

## POST-ATTACK RECOVERY

After a ransomware attack, it is crucial to learn from the experience and strengthen your organization's cybersecurity defenses.

### Post-attack steps include:

1. Conduct a thorough analysis of the incident to identify root causes and vulnerabilities.
2. Implement recommended security measures to prevent similar attacks in the future.
3. Review and update your incident response plan based on the lessons learned.
4. Share information about the attack with relevant parties and collaborate with industry peers to improve overall cybersecurity.

By understanding the complex nature of ransomware attacks and taking a proactive approach to prevention, response, and recovery, your organization can significantly reduce the likelihood of falling victim to ransomware and better protect its critical data and operations.



# Conclusion

This report shed light on the pervasive threat of ransomware, highlighting its evolving tactics and the ripple effects these attacks can have on an organization or industry. The massive growth in the number of attacks and victims these past twelve months suggests we will only see attacks continue to increase as ransomware groups become more embolden by past successes. As these shadow enterprises continue to refine their methods, it is imperative for organizations to prioritize robust proactive threat intelligence to better understand their own susceptibility to ransomware as well as the susceptibility of their supply chain to avoid business disruption.





# Methodology

The methodology employed by the Black Kite Research & Intelligence Team (BRITE) for this research report encompassed comprehensive monitoring and analysis of ransomware activities from April 1, 2023, to March 31, 2024. BRITE actively monitored a vast array of ransomware groups, totaling more than 130, to gain insights into their operations, tactics, and targets.

## Ransomware Group Monitoring:

BRITE's monitoring process involves real-time tracking of over 130 ransomware groups, allowing for timely identification of their activities and targets.

## Victim Analysis:

Among the monitored ransomware groups, 67 were identified to have published at least one victim within the last 12 months preceding the study period. For each victim, BRITE conducted a detailed analysis of their cybersecurity posture both before and after the ransomware attack, leveraging the capabilities of the Black Kite platform.

## Dark Web Monitoring:

In addition to monitoring ransomware groups' activities, BRITE actively tracks dark web blogs, hacker forums, and Telegram channels to gather intelligence on the evolving tactics and narratives employed by these groups. This ensures a holistic understanding of the ransomware landscape and facilitates the identification of emerging threats.

## Victim Enumeration:

Over the course of the study period, BRITE observed a total of 4,893 victims affected by ransomware attacks. For each victim, meticulous attention was given to fine-tune the identification of the victim's country and industry, providing valuable context for further analysis.

By employing this multifaceted approach, BRITE offers a comprehensive analysis of ransomware activities during the specified timeframe, shedding light on trends, vulnerabilities, and mitigation strategies within the cybersecurity landscape.

# Black Kite Research & Intelligence Team (BRITE)

## Ferhat Dikbiyik

Chief Research & Intelligence Officer

## Gokcen Tapkan

Director of Data Research

## Ozcan Akdora

Director of Data Engineering

## Basri Ciftci

Senior Data Engineer

## Serkan Ekrem Cengiz

Senior Data Engineer

## Yunus Dogan

Senior Technical Lead

## Ferdi Gul

Senior Cybersecurity Researcher

## Yavuz Han

Senior Cybersecurity Researcher

## Gulsum Budakoglu

Data Analyst

## Ekrem Selcuk Celik

Junior Cybersecurity Researcher

## Gizem Toprak

Junior Data Analyst