2025 Ransomware Report

How Ransomware Wars Threaten Third-Party Cyber Ecosystems

By the Black Kite Research & Intelligence Team (BRITE)

For the best experience, view the interactive report: content.blackkite.com/ebook/2025-ransomware-report/

Ransomware Report Executive Summary

Ransomware Wars escalated between April 2024 and March 2025—not with more powerful enemies, but with more of them.

As dominant syndicates like **LockBit** and **AlphV** collapsed under global law enforcement pressure, the battlefield fractured. In their place, dozens of **new, less coordinated ransomware groups** emerged, waging unpredictable campaigns across a wider target base.

The number of **publicly disclosed victims rose to 6,046**, a 25% increase from the previous year. **Small and mid-sized businesses (SMBs)** became the new frontline. Attackers increasingly favored targets with **$4M-$8M in revenue**, where defenses are thinner and the risks of retaliation lower.

This year also saw a rise in **supply chain warfare**, where attacks on vendors like Cleo and CDK Global caused disruption far beyond the initial breach. While **ransom payment amounts declined**, the volume and collateral impact of attacks continued to grow.

To help organizations predict and prioritize risk, Black Kite's **Ransomware Susceptibility Index® (RSI™)** remained a critical signal. Among companies with RSI above 0.8, **46% were ultimately attacked**. Most showed rising RSI trends well before the breach.

Even as ransomware grows more chaotic, **intelligence-driven defense, proactive vendor monitoring, and early warning signals like RSI** give organizations a fighting chance.

Key Findings

6046
publicly disclosed ransomware victims, up 24% year over year

96
active ransomware groups, including **52 new entrants**

$4M-$8M
SMBs ($4M-$8M) were the most frequently targeted

67%
Ransomware responsible for 67% of known third-party breaches

46%
46% of companies with RSI > 0.8 experienced ransomware attacks

Ransom payment values declined
but overall impact widened

Major law enforcement operations
but overall impact widened

Regulatory enforcement lags
behind incident disclosures

Key Takeaway

The ransomware threat hasn't disappeared—it has fractured and multiplied. With more actors, less predictability, and deeper entanglement in supply chains, organizations must shift from reactive defenses to proactive intelligence and third-party monitoring. As the battlefield changes, so must the strategy.

TABLE OF CONTENTS

01 | INTRODUCTION
How the past year changed the ransomware landscape.

02 | ATTACK DATA
Trends in victim numbers, geographic distribution, and industry impact.

03 | SUPPLY CHAIN IMPACT
Ransomware's increasing focus on third-party vendors with case studies.

04 | CLOP'S CLEO CAMPAIGN
Spotlight on an attack large in scope, but quiet in impact.

05 | AVOIDING RANSOMWARE
How to pinpoint ransomware risk with third-party risk intelligence.

06 | LOCKBIT & ALPHV
The collapse of major groups and the resulting power struggle.

07 | TOP GROUPS
Profiles of the most active and emerging ransomware groups.

08 | LEGAL RESPONSE
Legal and operational efforts against ransomware.

09 | AI IN RANSOMWARE
How artificial intelligence is impacting attack methods.

10 | NEXT STEPS
Future trends in ransomware and recommendations for defenders.

11 | APPENDIX
Report Methodology

Discover the events that redefined the ransomware battlefield this past year.

NEXT PAGE

Introduction

The Year the Ransomware War Changed

Between April 2024 and March 2025, ransomware evolved—not in sophistication, but in strategy.

It was a year defined by collapse, chaos, and recalibration. The fall of two of the most dominant ransomware syndicates, LockBit and AlphV, triggered a power vacuum across the cybercriminal landscape.

These weren't just threat groups—they were institutions. Their downfall did not end the war. It reshaped the battlefield.

In their place, dozens of new actors emerged, many of them lacking the infrastructure, discipline, or credibility of their predecessors. The result: a rise in volume, a drop in coordination, and a growing unpredictability in how, where, and why attacks unfold.

The Numbers Behind the Noise

In the twelve months observed:

6046

Publicly disclosed ransomware victims climbed to **6,046**, up from **4,893** the year prior—a **24% increase** year over year.

2708

That figure has more than **doubled since 2023**, when it stood at **2,708**.

96

The number of ransomware groups making public disclosures rose from **61 in 2023** to **96 in 2025**.

52

52 entirely new groups emerged in the last year, compounding the 51 new entrants that appeared in the preceding year.

The ransomware ecosystem didn't shrink. It splintered.

While some interpret recent declines in ransom payments as a sign that ransomware is losing relevance, the sheer volume of victims and the instability of new actors suggest otherwise. The threat didn't retreat—it scattered.

LockBit: From Reign to Ruin

LockBit's story was once a blueprint for ransomware success: polished infrastructure, professional negotiations, and dominant market share. But 2024 marked a turning point.

Operation Cronos, a multi-agency law enforcement effort, dealt a crushing blow to the group's reputation and operations. Affiliates fled. Market share collapsed. And for the first time, **LockBit administrators were publicly identified and targeted with international bounties**. What was once the most feared brand in ransomware now became a cautionary tale for aspiring operators.

LockBit didn't just fall. It fractured the economy that revolved around it.

The Rise of the Rest

With LockBit and AlphV gone, **no single group emerged to take the crown**. Instead, smaller actors flooded the space, many with hastily assembled infrastructures, erratic victim targeting, and limited capacity for negotiation or follow-through. This era marked the start of a new ransomware phase—less strategic, more opportunistic.

Groups like **RansomHub**, **Play**, and **Akira** filled parts of the void. But the broader trend was clear: **affiliates dispersed**, **brand loyalty dissolved**, and **Ransomware-as-a-Service became Ransomware-as-a-Chaos**.

About Our Ransomware Report

This report is the product of a year-long investigation conducted by the Black Kite Research & Intelligence Team (BRITE). It draws from real-time monitoring of over **150 ransomware groups**, deep intelligence gathered from **dark web channels**, and the **technical telemetry** of more than **6,000 victims**.

Among these groups, **96 were observed to have published at least one victim** during the past 12 months.

For each confirmed victim, BRITE performed:

- Industry and country attribution using the NAICS standard
- Pre- and post-incident analysis using the Black Kite platform Monitoring of ransomware blog disclosures, affiliate communications, and extortion tactics across forums, Telegram channels, and leak sites

A **dedicated Methodology section** at the end of this report provides more detail.

Explore the stark realities revealed by the latest ransomware attack data.

PREVIOUS NEXT

The Business of Ransomware

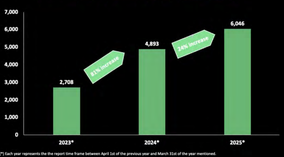
Booming, Fragmenting, Evolving

Beyond the Headlines

The Real Growth Story of Ransomware

Ransomware is no longer a series of isolated attacks—it is a sustained, system-wide threat. In the twelve months covered by this report, the number of publicly disclosed ransomware victims climbed to 6,046, marking a 24% year-over-year increase. This follows an even steeper rise in the previous period, when the number surged by 81%, from 2,708 to 4,893. Together, this amounts to a 123% increase over two years.

Ransomware Victim Growth (2023–2025)



(*) Each year represents the the report time frame between April 1st of the previous year and March 31st of the year mentioned.

This chart shows the number of victims announced by ransomware groups and the alarming year-over-year increase.

While some industry reports point to declining ransom payments and use that to suggest diminishing risk, the data tells a different story. The number of victims continues to rise. More groups are operating. And the damage is no longer measured in payments alone. The operational disruption caused by these attacks—especially in the context of supply chains—is growing more severe.

Incidents involving Clearwater HealthCare, Blue Yonder, and CDK Global made clear that ransomware's impact is no longer contained within the four walls of the initially affected organization. When threat actors compromise a widely used vendor, the effects ripple outward, paralyzing downstream businesses in multiple sectors. In this way, ransomware is increasingly a supply chain problem, not just a cybersecurity one.

This year's growth in victim count signals more than just a surge in activity—it reflects a deeper shift in how ransomware groups operate and who they target. With newer, less experienced groups flooding the ecosystem, small and mid-sized vendors have become popular entry points. These are companies that may not make headlines when attacked, but they often sit at critical intersections of industry workflows. Disrupting them means disrupting everything they connect to.

In the sections that follow, we explore how these numbers evolved over time, which sectors were hit hardest, and how the ransomware ecosystem is shifting in both structure and intent.

We'll look at:

1. Monthly Activity
2. Geographic Distribution
3. Industries Impacted
4. SMB Targets
5. Revenue Targets
6. Payment Demands
7. Repeat Victims

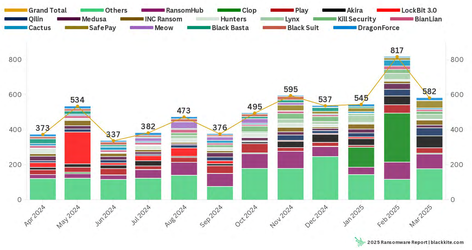
1. Peaks and Patterns: Ransomware Activity by Month

Ransomware activity in this reporting period was not only elevated—it was persistent. Monthly victim disclosures fluctuated throughout the year but remained consistently high, with only two months seeing a drop below 400 incidents. The most active period was February 2025, which saw a staggering 817 victims, largely driven by Clop's mass exploitation of Cleo vulnerabilities.

Despite occasional dips, each quarter surpassed the previous year's equivalent, contributing to the overall 24% rise in victim count. The trend line reflects a maturing but fragmented ecosystem—one where smaller groups launch opportunistic campaigns, and larger ones drive major surges through mass exploitation events or strategic timing.

Monthly Ransomware Victim Disclosures by Group

(April 2024-March 2025)



What stands out even more than the raw victim numbers is the expansion in the number of active groups. Over the past two years, the ransomware landscape has nearly doubled in operator count. In April 2023, just 61 groups had published at least one victim in the past year. By April 2024, that number reached 84. And by the end of this reporting period, it hit 96.

Active group:

A ransomware group published at least one victim in their darkweb blog in the previous 12 months.

This growth points to a key shift: the barriers to entry have lowered, allowing less sophisticated but still effective actors to enter the field. Many of these groups reuse leaked tools, copy existing ransomware playbooks, or even brand-hop between campaigns.

Number of Active Ransomware Groups

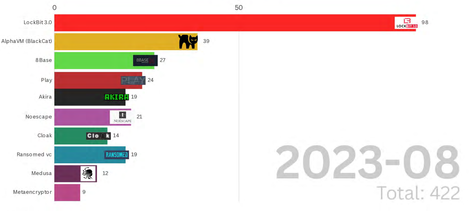
(12-Month Rolling Window)

Yet, their collective activity keeps the pressure on defenders and expands the surface area of risk.

The spikes we observe are not just statistical noise—they map directly to specific threat actor behavior. The February surge aligns with Clop's delayed and ultimately chaotic Cleo campaign. Meanwhile, groups like RansomHub, Play, and Akira maintained steady output, creating a rising floor of monthly disclosures.

Ransomware Cybercrime Ecosystem:

Number of Victims Published



Pause

View the animated chart: content.blackfile.com/ebook/2025-ransomware-report/attack-data

2025 Ransomware Report | blackfile.com

This sustained activity reinforces a key trend: ransomware is no longer a seasonal or opportunistic threat. It is an always-on business model, shaped by automation, vulnerability exploitation, and low entry costs. The rise in group count is not just a signal of scale—but of strategic diversification across the ransomware economy.

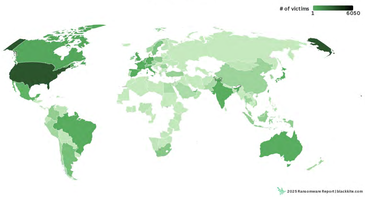
Back to Top ^

2. Global Pressure Points: Geographic Distribution of Ransomware Victims

The United States continues to be ransomware's most targeted geography—by a wide margin. This year, 3,141 U.S.-based organizations were publicly named as victims, up from 2,293 the year before. That's a 37% increase year over year, and it accounts for 54% of all known global ransomware disclosures.

Ransomware Victim Distribution by Country

(April 2024-March 2025)



While the U.S. remains ransomware's ground zero, several other regions experienced meaningful shifts. Countries with the sharpest increases include:

India
growing from 51 to 133 victims

Brazil
growing from 72 to 139

Canada
growing from 216 to 318

These changes reflect both expanded threat actor reach and the global exposure of these countries' vendors and subsidiaries.

The top five most targeted countries this year:

3141 United States

318 Canada

250 United Kingdom

191 Germany

149 Italy

Interestingly, some countries saw steep drops in victim count. **Russia**, for example, dropped from 70 victims last year to just 2 this year. This sharp decline is largely attributable to **Malas**, a politically motivated ransomware group that briefly emerged and disappeared after targeting around 70 Russian companies in a single month in 2023. With Malas gone, the data for Russia returned to baseline.

What's clear is that ransomware's footprint is **expanding, not shifting**. The number of countries with at least one publicly named victim rose from **112 last year to 134 this year**. While this might suggest growing strategic reach, part of the spread reflects the **amateurship of newer groups**. Unlike more seasoned actors—who often rely on insider data or carefully curated victim lists—many of the newer entrants appear to operate blindly, casting wide nets and testing the waters. This explains why we see **one or two victims in countries that typically fall outside the ransomware crosshairs**.

At the same time, deeper targeting of small vendors and supply chain intermediaries continues. And while the country of headquarters may appear in breach disclosures, the real vulnerability lies in the **digital interdependence across borders**. Campaigns like **Clop's Cleo exploitation** showed that ransomware damage radiates far beyond a single geography—and often far beyond the first name that gets published.

Back to Top ^

3. Hit Where It Hurts: Sectoral Breakdown and Industry Impact

Ransomware actors didn't just go after large targets—they went after strategic ones. For the second consecutive year, the top three most targeted industries were:

1314 Manufacturing

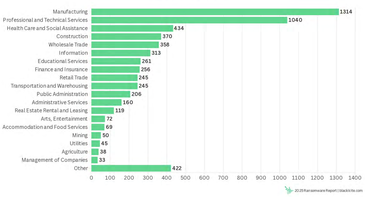
1040 Professional, Scientific, and Technical Services

434 Healthcare and Social Assistance

These classifications are based on NAICS codes, ensuring consistency with prior reporting periods. While the rankings remained unchanged from last year, the absolute number of victims increased in all three categories, and their internal dynamics shifted in telling ways.

Ransomware Victims by Industry

(April 2024-March 2025)



Rank Change of Ransomware Victims by Industry

Industry	Rank(change)
Manufacturing	1 (→)
Professional, Scientific, and Technical Services	2 (→)
Health Care and Social Assistance	3 (→)
Construction	4 (↑3)
Wholesale Trade	5 (↑7)
Information	6 (→)
Educational Services	7 (↓2)
Finance and Insurance	8 (↓4)
Transportation and Warehousing	9 (→)
Retail Trade	10 (↓2)
Public Administration	11 (→)
Administrative and Support and Waste Management and Remediation Services	12 (↓2)
Other Services (except Public Administration)	13 (↑1)
Real Estate Rental and Leasing	14 (↓3)
Arts, Entertainment, and Recreation	15 (↑1)
Accommodation and Food Services	16 (↓3)
Mining	17 (↑1)
Utilities	18 (↓1)
Agriculture, Forestry, Fishing, and Hunting	19 (↑1)
Management of Companies and Enterprises	20 (↓1)

Rising Heat: Percentage Growth in Select Sectors

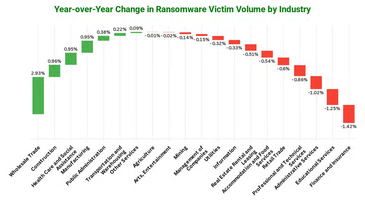
Looking beyond raw totals, certain industries experienced disproportionate growth in victim counts compared to the previous year. According to the data, the biggest year-over-year increases were seen in:

+2.93% Wholesale Trade

+0.96% Construction

+0.95% Healthcare and Social Assistance

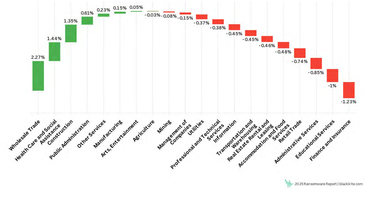
Year-over-Year Change in Ransomware Victim Volume by Industry



However, some of these figures are skewed by Clop's mass exploitation of Cleo vulnerabilities. To account for this, we generated an adjusted chart excluding Cleo victims—revealing that Healthcare still ranks second in growth even without Clop's outlier event.

Adjusted YoY Change by Industry

(Excluding Clop's Cleo Campaign)



Healthcare's Upward Trend: A Warning Signal

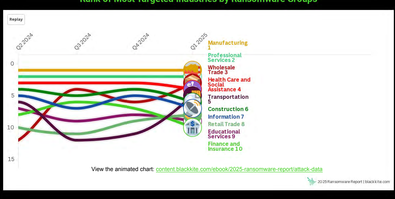
One of the most notable shifts this year was the steady quarterly rise in healthcare targeting, which began in Q4 2023 and held firm through Q1 2025. In previous years, healthcare often hovered around fifth or sixth place. This year, it locked into third and stayed there.

This sustained rise aligns with insights from our standalone 2025 report, "Healthcare Under Ransomware Attack: Why Healthcare Is Now the 3rd Most Targeted Industry in the Ransomware Cybercrime Ecosystem."

As noted in that analysis, the healthcare ecosystem's complexity, legacy infrastructure, and urgency of services make it an increasingly attractive—and vulnerable—target.

- Notably, offices of physicians and health practitioners overtook hospitals in ransomware victim counts this year.
- Smaller practices often lack dedicated security teams, but still handle sensitive patient data—making them low-hanging fruit with high extortion potential.

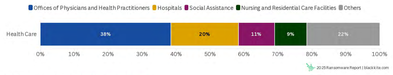
Rank of Most Targeted Industries by Ransomware Groups



View the animated chart: content.blackfile.com/ebook/2025-ransomware-report/attack-data

2025 Ransomware Report | blackfile.com

Healthcare: Ransomware Attacks by Subindustry



2025 Ransomware Report | blackfile.com

More insights are available in the full healthcare report.

🔍 Subsector Spotlight

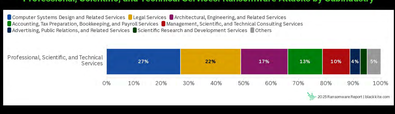
Professional, Scientific, and Technical Services

Within this diverse category, two subindustries continued to dominate:

- Computer Systems Design and Related Services
- Legal Services

Last year, legal services held the top spot. This year, the two swapped positions, though the margin remains narrow. Both subindustries house high-value data and complex confidentiality chains, making them high-leverage ransomware targets.

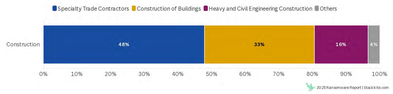
Professional, Scientific, and Technical Services: Ransomware Attacks by Subindustry



2025 Ransomware Report | blackfile.com

Construction

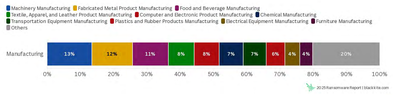
Ransomware in the construction sector overwhelmingly affected **specialty trade contractors** and **building construction firms**. These businesses often rely on decentralized IT, subcontractor-heavy ecosystems, and urgent project timelines—conditions that favor threat actors seeking quick payouts. Additionally, contractors have a wealth of client relationships, which amplifies their vulnerability when compromised and places them in a significantly challenging position.



2025 Ransomware Report | blackfile.com

Manufacturing

Unlike other industries, the **distribution of ransomware victims across manufacturing subindustries was fairly even.** From electronics and furniture to transportation and chemicals, no single category dominated—underscoring the sector's broad exposure to ransomware risk.



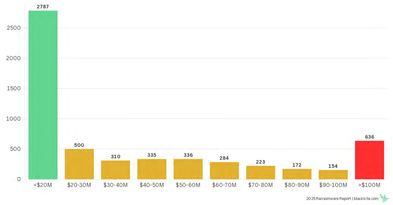
2025 Ransomware Report | blackfile.com

Back to Top ^

4. The SMB Squeeze: Ransomware Shifts Downmarket

Ransomware groups are no longer just targeting "big game." While headlines continue to spotlight attacks on large enterprises, the data tells a different story: **small and mid-sized businesses (SMBs) have become the core targets.**

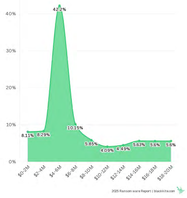
Ransomware Victims by Revenue Tier (Full Spectrum)



2025 Ransomware Report | blackfile.com

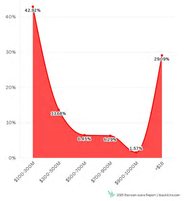
This year, only **11%** of the known ransomware victims had an annual revenue over $100 million—a notable drop from **26%** the previous year. For companies with revenue over **$1 billion**, the decline is just as sharp: from **8%** in **2024** to **3.2%** in **2025**.

Breakdown of Ransomware Victims with Revenue Under $20M



2025 Ransomware Report | blackfile.com

Breakdown of Ransomware Victims with Revenue Over $100M



2025 Ransomware Report | blackfile.com

At the other end of the spectrum, **businesses earning under $20 million per year accounted for the largest share of victims**, with a clear concentration in the **$4M to $6M** range. This lower middle tier appears to be the new ransomware "sweet spot."

The reasons behind this shift are multifaceted:

SMBs are easier targets.
They're often under-resourced, understaffed, and underprepared.

New groups lack infrastructure.
Many emerging ransomware operators simply don't have the technical or logistical capacity to compromise well-defended enterprises.

Big targets bring big heat.
Law enforcement actions against prominent groups like REvil, DarkSide, AlphV (aka Black Cat), and LockBit served as cautionary tales. The cost of attacking a Fortune 500 company may now outweigh the benefit.

Security investments are working.
Large enterprises have steadily increased cybersecurity budgets and hardened their environments—making them not only tougher, but also riskier.

Quiet payouts, less drama.
SMBs are more likely to pay something quickly and quietly, without triggering public or regulatory alarms.

From an economic lens, ransomware actors are becoming more pragmatic. Many are **choosing quantity over notoriety**, volume over visibility. The result: a **scalable extortion model** focused on hundreds of mid-sized businesses instead of a few big logos.

This strategy also aligns with a broader pattern: **avoiding targets that escalate consequences**. Unless they're making a PR move or signaling dominance, most groups now steer clear of the giants. It's a survival tactic—and a business model.

Back to Top ^

5. Who Gets Hit Depends on What They Earn

Not all industries are targeted equally across the revenue spectrum. As ransomware operators shift their focus downmarket, we observe a corresponding change in which sectors are most frequently victimized at each company size tier.

Among companies earning below $20M annually, the most targeted industry is Professional, Scientific, and Technical Services—accounting for almost a quarter (23.3%) of all victims in this range. This group includes legal services and computer systems design firms, both of which frequently handle sensitive data, intellectual property, or third-party integrations that can be used for further pivoting.

Top Targeted Industries for Companies with <$20M Annual Revenue

As company revenue increases, **manufacturing steadily climbs the ranks.** For organizations earning between **$100M and $300M, manufacturing becomes the top industry**, representing **30%** of ransomware victims in that tier.

2025 Ransom ware Report | Stackl ris.com

Top Targeted Industries for Companies with $100M–$300M Annual Revenue

And for enterprises with more than **$1 billion** in revenue, **manufacturing dominates—comprising a staggering 38.9%** of ransomware victims. These companies tend to have complex operational technology (OT), global exposure, and intricate digital footprints—making them attractive, high-stakes targets when groups are willing to take the risk.

2025 Ransom ware Report | Stackl ris.com

Top Targeted Industries for Companies with >$1B Annual Revenue

The data underscores an important trend: **industry targeting is increasingly shaped by company size**. Smaller organizations in service-heavy verticals are picked off quietly and efficiently. Meanwhile, **manufacturing remains ransomware's favorite high-value target**, but only when the attackers have the resources, infrastructure, and confidence to go after large, hardened enterprises.

2025 Ransom ware Report | Stackl ris.com

That targeting is not accidental. **Manufacturing underwent rapid digital transformation post-COVID**, but its **cybersecurity maturity lagged behind**. As companies embraced automation, IoT, and interconnected supply chains, their attack surfaces expanded significantly. Yet for many, **cyber risk still doesn't rank among their top business risks**—creating a vulnerability gap that ransomware actors continue to exploit.

This duality shows how **ransomware is not one-size-fits-all**. It's adaptive, resource-aware, and tailored to attacker capability and risk tolerance

Back to Top ^

6. Less Money, More Mayhem: The Shifting Economics of Ransomware

In 2024, ransomware payments declined—but that doesn't mean the threat did.

According to multiple industry sources, **average ransom payments fell by as much as 35%**, and **fewer victims are paying**. Coveware reports that just **25% of organizations paid a ransom**, and among those hit with **data exfiltration-only attacks**, 41% paid—still far from a majority. Chainalysis, Sophos, and others have echoed the trend: **fewer dollars are changing hands**, and when they do, it's often under more constrained negotiations.

Data points:

Average ransom demand in 2024	Median ransom payment	Highest known demand
$4.32 Million	$2 Million (up from $400K in 2023)	$70 Million (up from $400K in 2023)

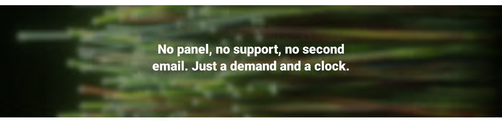
Average ransom payment	Median payment (Q3)	Total ransomware payments
$553959 according to Coveware Q3	$110890 (down 45% from prior quarter)	$813 Million according to Chainalysis (down from $1.25B in 2023)

So what's behind the numbers?

The answer is simple: **the groups have changed.**

After the takedowns of **LockBit** and **AlphV**, no single group has emerged to claim the same dominance. In their place, we see **smaller, less sophisticated operators** that often lack the infrastructure to run complex extortion operations. Without the polished negotiation portals and "customer service" tactics of legacy players, these groups tend to **skip the negotiation phase entirely**—demanding what they can and hoping to get anything at all.

With one shot at extortion, most settle on **lower demands upfront**.



At the same time, organizations have become more resilient. Stronger **backups**, more **mature incident response**, and **greater legal and reputational risk awareness** have made it easier for victims to say no. In regulated industries, payment refusal is increasingly the default—not the exception.

This change in the economics of ransomware doesn't signal a dying threat. It signals a **more chaotic one**—one where actors are **less predictable**, campaigns are **less coordinated**, and **impact is measured in disruption, not just dollars**.

Back to Top ^

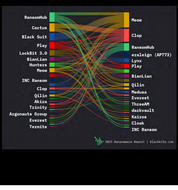
7. Double Trouble: When Ransomware Strikes the Same Victim Twice

The ransomware battlefield is becoming increasingly congested — and sometimes, it's the same victim getting caught in multiple crossfires. While the average organization dreads a single ransomware attack, some faced **two separate attacks** by different ransomware groups within a relatively short time frame.

This troubling trend has two major explanations:

1. Affiliate Overlap Across Ransomware-as-a-Service (RaaS) Operations:

Many RaaS groups rely on affiliates to carry out attacks. These affiliates frequently move from one group to another, bringing their victim lists, tools, and tactics with them. If an affiliate switches allegiances or decides to monetize a target again, they might hit the same organization using a different ransomware strain. In some cases, both groups end up publicly listing the same victim — as captured in the Sankey diagram below.



2. "Recycled" Victims on Public Leak Sites:

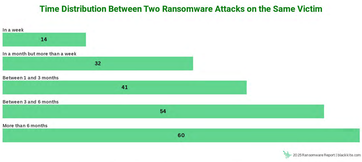
Public disclosures are double-edged swords. When one ransomware group publishes a victim's name, it can inadvertently put a target on their back. Other groups scanning leak sites may see that the victim paid once or otherwise appears vulnerable and launch a follow-up attack. Sometimes, the second attack follows just days after the first. Other times, it happens months later, giving the false impression that the danger has passed.

The data reveals a chilling reality:

In **14 cases**, the second attack occurred **within a week**.

In **32 cases**, it came **within a month**.

And in **more than 60 cases**, the follow-up happened **after six months**, underscoring that once targeted, organizations remain on threat actor radars for extended periods.



This phenomenon is not just a fluke — it reflects how **interconnected, opportunistic**, and **reputation-driven** the ransomware ecosystem has become. Whether it's due to affiliate churn or data visibility from leak sites, victims are no longer "one and done." They're being treated as **repeatable revenue streams**.

Organizations need to treat a ransomware incident not as an endpoint, but as the beginning of long-term vulnerability unless meaningful remediations are made immediately. A single compromise is now a **beacon** — a warning that more attacks may be on the horizon.

Back to Top ^

The initial breach is only the beginning. Discover the cascading impact of ransomware in the supply chain.

PREVIOUS NEXT

Supply Chain Attacks

A Growing Threat Vector

Ransomware is no longer just an endpoint problem—it's a supply chain crisis.

In 2024, attackers increasingly focused on third-party vendors, knowing that one compromised provider can disrupt dozens—or hundreds—of downstream organizations. These incidents, often called silent breaches, went unnoticed until their ripple effects halted operations across industries.

Why Supply Chain Attacks? Why Now?

The appeal is simple. Supply chain attacks offer scalability, deniability, and leverage. Instead of breaching a well-defended enterprise, attackers now exploit the weakest link in its vendor network—often a mid-sized provider handling critical functions like file transfers, software updates, or cloud data access.

Several factors drove this shift in 2024:

- **Systemic vulnerability:** Widely used tools like Cleo and Snowflake became entry points.
- **Vendor opacity:** Many organizations lack visibility into their third and fourth-party connections.
- **Disruption over dollars:** Even if ransom isn't paid, the disruption itself creates value for threat actors.

What Supply Chain Attacks Look Like

According to Black Kite's 2025 Third-Party Breach Report, The Silent Breach: How Third Parties Became the Biggest Cyber Threat in 2024, ransomware was the **most common known attack vector** in third-party breaches, accounting for **66.7%** of all analyzed incidents with clear attribution. These attacks are rarely isolated. One breach spreads through Nth-party connections, causing **cascading delays, inventory disruptions, and patient care issues** across the ecosystem.

> **"Silent breaches don't announce themselves. You see them in missed shipments, delayed diagnoses, and angry customers. By then, the damage is already done."**
>
> — Black Kite Third-Party Breach Report, 2025

Case Studies: The High Cost of Third-Party Disruption

CDK Global

In July 2024, CDK Global—a core software provider for the automotive industry—was hit with a $25M ransomware demand. The attack **crippled 3,000+ car dealerships** in the U.S., stalling inventory systems, delaying customer deliveries, and freezing CRM platforms. The attackers exploited weak segmentation and lack of threat detection to move laterally within CDK's systems.

Lesson

Industry-specific providers are systemic risk points. Segment, monitor, and pressure-test your vendors.

Change Healthcare

A ransomware attack on Change Healthcare in February 2024 halted the flow of claims, lab results, and insurance authorizations across U.S. hospitals and providers. Attackers infiltrated via **stolen credentials and missing MFA** to remotely access a Change Healthcare Citrix portal, exposing data from over **100 million individuals**.

Lesson

The deeper the vendor in your operational bloodstream, the more urgent the need for hardening and continuous monitoring.

Cleo

Clop's exploitation of Cleo's MFT tools paralyzed retail and logistics companies relying on its unpatched software. The two vulnerabilities—**CVE-2024-50623** and **CVE-2024-55956**—enabled remote code execution and data exfiltration. (Read a deep dive of Clop's Cleo campaign in the next section.)

Lesson

Patch management isn't just your job—it's your vendors' job too. And your resilience depends on how seriously they take it.

One group's campaign perfectly illustrates this danger: A deep dive into Clop's Cleo exploitation.

PREVIOUS NEXT

Spotlight

Clop's Cleo Campaign, A Case Study in Exploitation

Just like in previous years, Clop returned with a campaign built around a newly discovered vulnerability. After the noise surrounding MOVEit, the group had gone relatively quiet, releasing victim posts sporadically. But in December 2024, they reemerged by exploiting critical flaws in Cleo—unleashing what could have been another major supply chain crisis.

The attack itself was large and sophisticated. But limited media coverage, organizations' increased resistance to paying ransoms, and the fact that Clop's once-effective tactics have begun to lose their sting all contributed to something unusual: a campaign that was successful in execution, but surprisingly subdued in impact.

CVEs Found in Cleo

So, what exactly happened with Cleo?

Cleo is a widely used Managed File Transfer (MFT) platform relied upon by thousands of companies worldwide for secure data transfer and system integration. However, in late 2024, two critical vulnerabilities were identified in Cleo's core products, posing serious threats to overall system security.

- CVE-2024-50623 contains a flaw that permits unrestricted file uploads and downloads. This flaw allows attackers to upload malicious files that result in remote code execution. In this scenario, attackers can bypass standard authentication checks to execute arbitrary commands on the targeted system, thereby increasing the risk of complete system compromise.
- CVE-2024-55956 targets the default configuration of the Autorun directory. Attackers who exploit this vulnerability are able to execute Bash or PowerShell commands on the host system by leveraging the system's behavior of automatically processing files placed in a predetermined directory.

Both vulnerabilities present significant risks, which makes it critically important for affected organizations to promptly implement the necessary security updates.

Clop's Cleo Attack Chronology: From Holiday Excuses to Chaos

2024

Oct 27 — **Cleo Vulnerability Disclosed**
Cleo disclosed CVE-2024-50623 and urged customers to patch immediately.

Nov 25 — **Cleo Breach Confirmed**
The Blue Yonder breach took place. While the attack was initially claimed by the Termite group, Cleo systems were directly involved in the compromise.

Dec 13 — **Operation Begins**
Clop officially announced in a blog post that it had exploited vulnerabilities in Cleo.

Dec 15 — **Second Vulnerability Emerges**
A second flaw, CVE-2024-55956, was publicly disclosed.

Dec 23 — **First Threat to Publish Victims**
Clop published blurred names of 66 companies and issued a warning:

> *YOU HAVE 48 HOURS, AFTER WE WILL REVEAL THE NAMES!!!*

Dec 25 — **Deadline Passes, No Action**
The 48-hour deadline passed, but the victims were not exposed. Instead, a new message followed:

> *THE ENTIRE LIST OF COMPANIES WILL BE OPEN ON MONDAY THE 30TH*

Dec 30 — **Disclosure Postponed Again**
Once again, the promised disclosures were delayed:

> *SINCE IT'S HOLIDAYS NOW, WE WILL OPEN THE LIST OF COMPANIES FOR ALL IN THE NEW YEAR... !!!*

2025

Jan 14 — **Stage One: 66 Victims Revealed**
The original 66 blurred victims were revealed.

Jan 21 — **Stage Two: 50 New Victims Blurred**
50 new blurred victims were added.

Jan 27 — **Stage Two Fulfilled: 50 Victims Revealed**
The 50 victims from January 21 were fully revealed.

Feb 10 — **Stage Three: Another 50 Victims Disclosed**
Another 50 victims were disclosed.

Feb 24 — **All Cards on the Table**
A new list of 50 victims was posted, followed later the same day by an additional 183 disclosures.

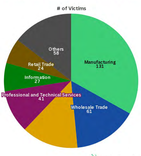
2025 Ransomware Report | blacklistc.com

By the end of February, the total number of victims had climbed to nearly 400.

Industries Impacted by Clop's Cleo Campaign

Cleo's MFT solution is heavily utilized across several key industries for secure data integration and transfer. Unsurprisingly, the sectors most reliant on such infrastructure were also the ones most impacted by Clop's exploitation of Cleo's vulnerabilities.

Clop's Cleo Campaign Victims by Industry



2025 Ransomware Report | blacklistc.com

Top 3 Industries Impacted by Clop's Cleo Campaign

1. Manufacturing

131 Victims

Manufacturing stands out as the most affected sector, accounting for more than a quarter of the victims. This aligns with Cleo's widespread usage in production workflows.

2. Supply Chain-Related Sectors

61 Wholesale Trade (victims)

54 Transportation & Warehousing (victims)

Two sectors are deeply integrated with manufacturing operations and rely heavily on Cleo for logistics, scheduling, and real-time data exchange, making them highly vulnerable and impactful targets.

3. Professional Services & Information Technology

68 Victims

These industries often serve as integrators, consultants, or technical service providers for Cleo deployments. Targeting them likely provided Clop with access to secondary targets or amplified the reach of the breach.

In summary, Clop targeted not only the technical vulnerability in its Cleo campaign, but also industries at the core of the supply chain. The goal was not just data theft, but to create operational chaos. Maybe they though this would make everything more impactful. But they failed.

Why?

Clop's Strategy and Tactics: Stir Curiosity, Buy Time

A campaign large in scope—but quiet in impact.

Clop disclosed nearly 400 victims. **That's a substantial number, yet the public response was barely a whisper.**

400
Victims

The group kept postponing its publication dates. First, it was "within 48 hours," then "on December 30," and finally, a vague "after the holidays" excuse. These repeated delays made Clop resemble a child throwing a tantrum for attention—but this time, no one looked their way. The industry didn't flinch, the media didn't bite, and the reaction Clop seemed to expect… never came.

Their tone grew sharper. Their strategy lost direction. And eventually, they dumped the entire victim list in one go, bringing the campaign to a blunt, anticlimactic end.

Perhaps the most telling aspect: This campaign failed to match the impact of Clop's highly successful 2023 attacks via mass exploitation of MOVEit vulnerabilities. Same group, similar tactics, another MFT product, hundreds of victims… but this time, the media was indifferent, the industry stayed quiet, and the public barely noticed.

Clop was a star during the MOVEit mass exploitation. During the Cleo campaign, their voice got lost in the noise.

So, how can organizations avoid becoming the next victim? The answer lies in proactive intelligence.

PREVIOUS NEXT

From Indicators to Intelligence

How to pinpoint Ransomware Risk with RSI™

Knowing who has been hit is useful. But knowing **who's next** is transformative.

If you want to understand how ransomware works, look at the victims.
If you want to stop it, look at who's next.

That's the idea behind the Ransomware Susceptibility Index® (RSI™), a score that reflects the likelihood of an organization being on a ransomware group's radar. Built by Black Kite's Research & Intelligence Team (BRITE), RSI was introduced four years ago to help defenders think like attackers.

Ransomware groups don't pick victims randomly. They weigh profitability, ease of access, geopolitical considerations, and even media visibility. RSI doesn't just track misconfigurations or exposed ports. It reflects the ransomware mindset—how threat actors think, prioritize, and act. Since its launch four years ago, RSI has helped hundreds of risk and cybersecurity teams proactively identify vendors and business units that are most likely to appear on a ransomware group's radar.

What RSI Measures:

RSI is a numerical score between 0.0 and 1.0, where a higher score represents greater susceptibility to a ransomware attack. But unlike traditional cyber risk metrics that focus solely on technical missteps, RSI is a composite score. It incorporates both:

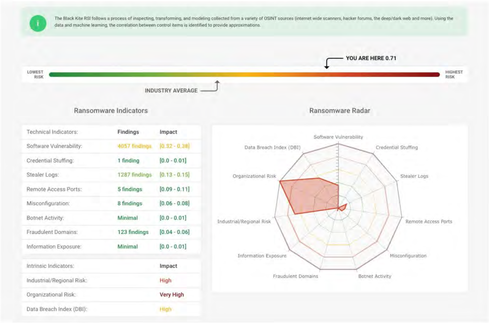
Technical Indicators: Misconfigurations, exposed remote ports, exploitable vulnerabilities, stealer logs, leaked credentials, botnet activity, and more.

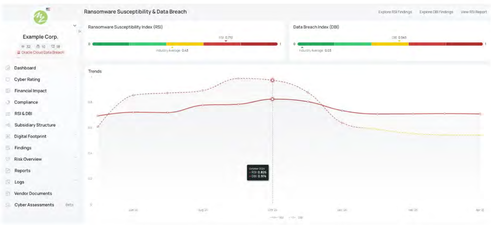
Intrinsic Risk Factors: Industry classification, geographic location, company size (revenue), and exposure history.

Black Kite's Ransomware Susceptibility Index findings for a company show their likelihood of a ransomware attack and why.

Ransomware groups don't need to know you to find you. They use automation, data leaks, and open-source scanning to identify low-friction, high-leverage targets. RSI is built on that logic.

Everything in this report—from industry targeting to supply chain attacks—is reflected in how RSI is constructed.





As an example, the Oracle Cloud breach in March 2025 showed alarming scores on Black Kite's Ransomware Susceptibility Index and Data Breach Index peaked in October 2024, which gives Black Kite customers advanced warning of an attack.

The Power of RSI: Correlation That Shows Compromise

Ransomware is considered a rare event by cyber insurers—and statistically, that holds. With an estimated 7,000–10,000 successful ransomware attacks per year across millions of companies worldwide, the odds seem low.

But those odds change drastically when a company becomes visible to ransomware groups.

That's what RSI captures. It's not a broad guess—it's a focused spotlight. When companies exhibit the combination of technical vulnerabilities and intrinsic traits that ransomware groups prey on, the likelihood of attack rises sharply:

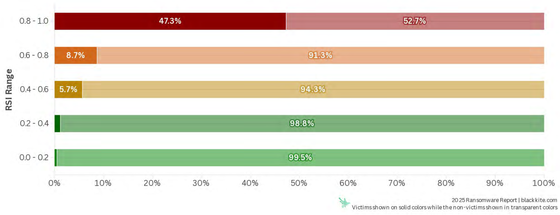
- **47.3%** of companies with an **RSI above 0.8** suffered a ransomware attack between April 2024 and March 2025.
- 8.7% of those with RSI between **0.6–0.8** were hit.
- Even in the **0.4–0.6** range, **5.7%** experienced a breach.
- Meanwhile, companies with low RSI values (<0.2) had **0.5%** victimization.

This isn't theoretical—it's **real-world probability**, grounded in data from more than 5,700 confirmed ransomware victims and hundreds of thousands of non-victims.

It's also important to note that **only 0.82% of all monitored companies** in the Black Kite platform had scores greater than 0.8. RSI is not inflated to increase predictive hits—it is **highly selective** by design. This is what makes RSI such a powerful signal: **the group it flags is small, but the correlation is strong.**

RSI doesn't just measure risk—it filters signal from noise.

RSI Distribution for Victims and Non-Victims



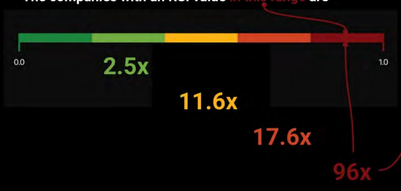
This is why RSI has become an essential input for cyber insurers, vendor risk teams, and breach prevention workflows. It isolates the high-risk population—before the incident—and helps security teams take action while there's still time.

When a score crosses a certain threshold, security teams take action. Some set automated alerts. Others build workflows around RSI spikes. For many, RSI is the early warning system they didn't have before.

It's not just who is weak—it's who is likely to get noticed.

POWER OF RSI

The companies with an RSI value in this range are



more likely to experience a ransomware attack than the companies with an RSI value below 0.2.

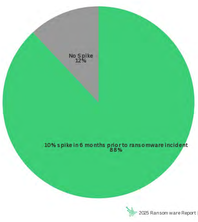
RSI in Motion: Why Tracking Changes Matters

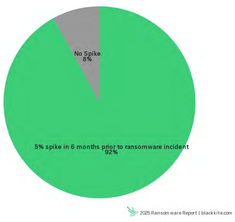
The average ransomware victim doesn't just have a high RSI—they often show a pattern of increasing risk in the lead-up to an attack:

61% had a rising RSI trend in the 6 months before compromise

88% had a 10% spike within that same window

92% experienced at least a 5% RSI spike between consecutive months





This is why many Black Kite customers monitor RSI spikes—not just thresholds. Even small movements in RSI can indicate a shift in visibility or exposure that puts an organization on the radar.

Recent victim cases further reinforce the predictive strength of RSI. The two companies below were both hit by ransomware in March 2025. In the month prior to the attacks, both showed RSI values well above 0.6, with a clear upward trend—signals that they were already on the radar of ransomware groups.

RSI & DBI for Victim A – RSI: 0.708 in February 2025

RSI & DBI for Victim B – RSI: 0.655 in February 2025

These are not isolated cases. Our historical analysis shows similar RSI patterns before the vast majority of ransomware attacks. This real-time, trend-based insight is exactly why RSI has become an indispensable signal for proactive cyber risk management.

Calibrating RSI: Keeping Up With a Shifting Landscape

RSI is not a static score—it's recalibrated each year to reflect how ransomware groups evolve. On March 15, 2025, we completed our most recent recalibration using:

Industry-Level Adjustments

Healthcare saw a notable rise; manufacturing and professional services remained top targets. RSI now better reflects subindustry nuances.

Country-Based Adjustments

U.S., Canada, UK, and Israel's risk coefficients were increased to reflect their growing share in victim counts.

Revenue Sensitivity

With large RaaS groups dismantled, ransomware targeting shifted toward smaller companies—particularly in the $4M–$10M range. RSI now places more weight on SMB vulnerability.

Despite these changes, **over 50% of companies** experienced less than **0.1 RSI shift**, ensuring continuity for most risk programs.

Go behind the scenes and explore how the Ransomware Wars started with the demise of LockBit and AlphV.

PREVIOUS NEXT

The LockBit and AlphV Aftermath

The Power Struggle

The back-to-back collapse of LockBit and AlphV at the end of 2024 left a void in the ransomware ecosystem. These weren't just high-volume operators. They shaped the market through their affiliate structures, negotiation strategies, and technical infrastructure. That order has now crumbled, creating a window of opportunity for others.

Last year, the number of active ransomware groups stood at 79. This year, it jumped to 95, with 52 new groups emerging in just twelve months. But the rise in quantity didn't come with a rise in quality. Instead of offering affiliates robust support, many newcomers promise quick wins and fast deployment. Several are copying LockBit's infrastructure and playbook. **The group may be gone, but its shadow still looms large.**

Affiliate Distribution and Migration

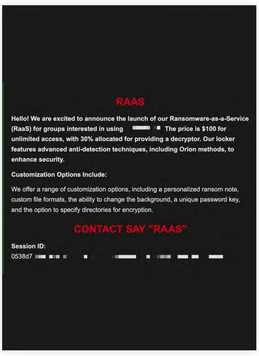
The collapse of major groups like LockBit and AlphV didn't just leave a numerical gap—it disrupted the very structure of the ransomware ecosystem. The most significant shift has taken place in how affiliates relate to operator groups.

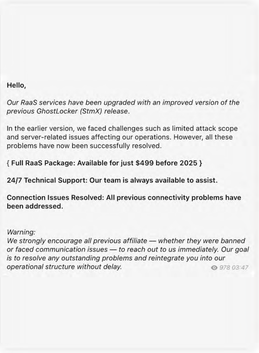
Previously, an affiliate had to prove technical skill to gain access to a top-tier group. In return, the group would provide tools, infrastructure, and hands-on support. The operator managed ransom negotiations and handled payments, giving the affiliate a predefined cut.

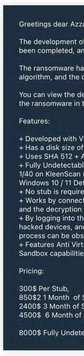
There was a sense of loyalty in this model—almost a corporate structure. LockBit, in particular, **ran its operation like a company.**

Evolution of the RaaS Model: From Organized Services to Open Chaos

What once resembled a corporate structure is now a chaotic market. The Ransomware-as-a-Service (RaaS) model—once centralized and selective—has unraveled into an open bazaar. Pre-packaged kits are now available for purchase, allowing even low-skill actors to launch attacks with minimal effort.







View all screenshots: content.blackkite.com/ebook/2025-ransomware-report/lockbit-alphv

The result?

- More attacks
- Less impact
- A loss of seriousness

RaaS is no longer just a threat—it's a business.

Some groups have begun offering additional services alongside ransomware kits, including:

- **Penetration testing reports**
- **Credential and stealer data**
- **Open port and DNS vulnerability scans**

No More Affiliate Loyalty: Everyone Works with Everyone

Affiliates are no longer tied to one operator. Today, they work with multiple groups simultaneously, leading to new dynamics:

- **The same victim company is disclosed by different groups at different times.**
- **The data is identical, the threat language unchanged—only the group name varies.**

Negotiation Breakdown: Loss of Leverage

Ransomware's strength has always come from more than just encryption—it came from psychological pressure at the negotiation table. But with LockBit and AlphV gone, that leverage has eroded.

New groups are loud in their threats, but weak in strategy. From the first message, there's panic. Data is leaked within days, and negotiations often don't even start. This approach reduces impact—and with it, the victim's motivation to pay.

Legal ambiguity, shifting insurance policies, a disengaged media, and the growing "don't pay, disclose instead" mindset are all weakening ransomware's strongest weapon: the threat of public exposure.

The old era was professional, structured, and methodical. The new one is fast, cheap, and chaotic. The volume of threats is rising—but their credibility is fading. In the future, the real shift in ransomware may not be in how strong the threat is—but in how seriously victims take it.

Which ransomware groups have risen to fill the void? Meet the current top players.

PREVIOUS NEXT

Profiling the Top Ransomware Groups

Top 5 Ransomware Groups

RansomHub – The New Boss at the Top

- RansomHub closed out 2024 at the top, disclosing 736 victims—the highest among all groups. With strong operational discipline and stable leadership, it quickly filled the void left by LockBit and AlphV.
- Its encryptors are effective, and its leak site language is threatening, but measured. The group appears to have attracted many former affiliates from LockBit, helping to explain the variety and geographic spread of its attacks.
- As we continue to 2025, RansomHub stands out as the most organized ransomware group in operation.

Play – Quiet Consistency

- Play emerged quietly in 2022, found its footing in 2023, and made a notable leap in 2024 with 369 disclosed victims.
- What sets the group apart is its focus on operational execution rather than media theatrics. Victim disclosures often come in waves, designed less to attract attention and more to apply direct pressure on targets.
- Despite its low profile, Play operates with a solid infrastructure and a well-established affiliate network.

Akira – The Old Fox

- Launched in 2023, Akira experienced a sharp rise in 2024, disclosing 349 victims.
  The group, once known for infrequent activity, has since ramped up its operations and maintained a steady pace.
- As one of the more veteran players in the field, Akira holds a position of strength rooted in experience.

Qilin – The Silent Hunter

- Qilin first appeared in 2022, but 2024 marked its breakout year, with around 200 victims—156 of them based in the U.S.
- By targeting healthcare and public service providers like Synnovis, Qilin showed just how impactful its attacks can be.
- The group disclosed victims consistently throughout the year.
- Not as loud as Clop or as widespread as RansomHub, but Qilin's target choices send a clear message: these attacks are deliberate, not random.

Medusa – The Snake's Head

- A long-time presence in the scene, Medusa stepped up in late 2024 and began pushing past its own ceiling.
- They drew attention with a string of high-profile victims and remain focused on financial gain, offering extensions for ransom deadlines.
- Loud, but behind the noise lies a group advancing with methodical precision.

Rising Ransomware Stars

Lynx

First spotted in mid-July, Lynx has quickly disclosed nearly 180 victims. The consistency of their postings is notable. Their rapid rise suggests a low-profile, yet highly capable actor is emerging.

SafePay

SafePay entered the scene in late November and broke its silence with 122 victims. The group keeps a low profile, operating with focus. Its primary targets lie within the financial sector, following a calm but direct strategy.

Kill Security

Active for about a year, Kill Security has recently stood out with a steady flow of victim disclosures and the promotion of its RaaS model and additional services. Notably, the group has launched over 40 attacks targeting organizations in India—highlighting a clear regional focus.

Fighting back is crucial. Learn about the legal and operational responses to ransomware.

PREVIOUS NEXT

The Legal and Operational Response to Ransomware

Fighting ransomware takes a lot of effort from many sides, but one big challenge is that many attacks go unreported. Even though ransomware cases are rising, a lot of them stay hidden, making it harder to respond quickly and understand the full picture. The FBI's IC3 2023 report (released in March 2024) showed 2,825 ransomware complaints, an 18% increase from 2022. To fight this growing threat, international teamwork is key. Some experts are even discussing banning ransom payments to discourage attackers.

"Banning ransomware payments could reduce transparency and discourage reporting, which is an issue the industry is already struggling with. As the organizations fear more legal trouble, they might go in the direction of handling the attacks quietly. In this case, it will be harder for law enforcement to track trends and for the cybersecurity community to share lessons. Such bans could also lower cybersecurity investment unintentionally by driving incidents underground."

– Müzeyyen Gökçen Tapkan, Director of Data Research at Black Kite

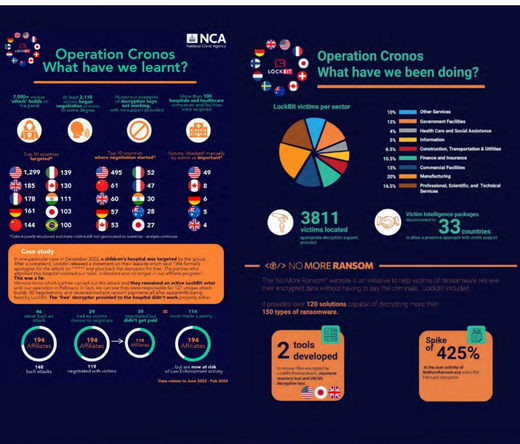
Strong cybersecurity regulations are critical. They are already pushing organizations to adopt more robust security and incident response protocols. Reward initiatives by agencies like the U.S. DOJ and OFAC also play a key role, offering incentives for information that leads to the arrest of cybercriminals—most notably, the $10 million bounty placed on LockBit members.

Police and Government Operations Make an Impact on Ransomware

Police and government operations are finally starting to show real results. For example, ransomware groups like 8Base have been taken down, and several cybercrime group members have been caught and sent to the U.S. These wins show that authorities are getting better at holding cybercriminals accountable and breaking up their networks.

In February 2024, Interpol's Operation Synergia helped find over 1,300 suspicious IP addresses and shut down many servers used in ransomware attacks. Around the same time, major groups like LockBit and Hive were still active—until Operation Cronos led to arrests and major data seizures. A big turning point came earlier with the takedown of the Sodinokibi/REvil group in 2022, thanks to international cooperation. That case showed that even the most dangerous ransomware groups can be stopped.

Later in 2024, Operation Serengeti focused on stopping cybercriminals across Africa, while Operation Endgame—led by Europol—took down key malware tools used to spread ransomware. These efforts show a smarter approach: not just going after the attackers, but also targeting the tools and systems that help them operate.



How Cybersecurity Companies Are Combating Ransomware

Cybersecurity companies are helping too. They create decryption tools that let victims get their files back without paying a ransom. These tools, along with strong security practices, make a big difference in limiting the damage ransomware can do.

Ultimately, defeating ransomware demands a coordinated response across governments, law enforcement, cybersecurity firms, regulators, and individuals. Promoting transparency and improving data sharing are essential to overcoming underreporting. The IC3 report reinforces the urgency of the threat—and with the combined strength of legal frameworks, enforcement actions, and technological solutions, a more resilient defense is within reach.

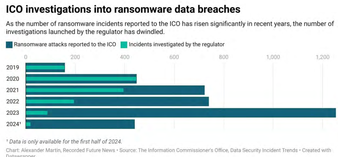
How Regulations Fight Ransomware

In response to the escalating threat of ransomware, regulatory bodies worldwide are intensifying their focus on cybersecurity, particularly concerning third-party and supply chain risks. The interconnected nature of modern supply chains means that vulnerabilities in a single vendor can have cascading effects on multiple organizations. Recognizing this, frameworks like the National Institute of Standards and Technology's (NIST) Ransomware Risk Management guidelines emphasize the importance of comprehensive risk assessments that encompass not only internal systems but also external partners.

Moreover, financial sector authorities, such as the Financial Industry Regulatory Authority (FINRA), have issued advisories highlighting the necessity for firms to conduct thorough due diligence and continuous monitoring of third-party providers. These guidelines stress that effective third-party risk management is not merely a best practice but a regulatory expectation, aiming to mitigate potential entry points for ransomware attacks through the supply chain.

Despite the growing number of ransomware attacks reported to the UK's Information Commissioner's Office (ICO), the number of regulatory investigations has sharply declined. As shown in the chart, while 2023 saw a record-breaking number of ransomware breaches reported, the proportion of incidents actually investigated by the regulator fell to its lowest point in years.

This disparity highlights a critical challenge: regulatory agencies are overwhelmed by the volume of disclosures, leading to inconsistent enforcement and follow-up. The widening gap underscores the need for organizations to proactively monitor and manage ransomware risk—including third-party exposures—rather than relying solely on regulatory response.



[1] *Data is only available for the first half of 2024.*

Chart: Alexander Martin, Recorded Future News • Source: The Information Commissioner's Office, Data Security Incident Trends • Created with Datawrapper

AI is everywhere. How is it showing up in ransomware campaigns?

PREVIOUS NEXT

AI's Impact on the Ransomware Landscape

How are Ransomware Actors Using AI?

Artificial intelligence (AI) is no longer a futuristic concept; it's a present-day reality transforming industries and, unfortunately, empowering cybercriminals. The ransomware landscape is particularly vulnerable to AI's influence, enabling attackers to design more convincing schemes and execute more efficient operations.

Website and Communication Design

We are now seeing design similarities across different ransomware groups' websites and communication. While this could be attributed to shared knowledge and copying, AI could also be used to optimize the design and user experience of these sites.

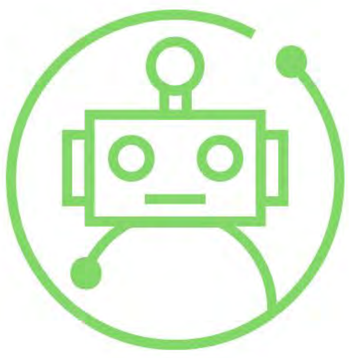
For example, the LockBit ransomware group is well-known for its professional website and sophisticated operation. Other groups have been known to copy their style of operation and website. Multiple reports have noted resemblances between the Royal Ransomware group and Conti, including similarities between the ransom notes each group uses

Victim Selection and Social Engineering Schemes

AI can also power target selection, analyzing vast amounts of data to pinpoint the most vulnerable and profitable victims. Furthermore, the development of more sophisticated and evasive malware, capable of bypassing traditional security measures is another facilitation of AI.

A particularly alarming trend is the rise of AI-driven social engineering attacks. For instance, as Funksec notes in their recent interview, threat actors are using AI to "craft phishing emails that **mimic the language patterns and communication styles** of specific individuals within a targeted organization." This allows for highly personalized and convincing attacks. They further elaborate that "AI helps in automating tasks like identifying security vulnerabilities and generating code to exploit them," speeding up the attack process significantly.

The Future of AI in Ransomware



The AI-driven future of ransomware is alarming. Expect highly targeted attacks tailored to specific vulnerabilities, as AI enables attackers to bypass existing security systems more easily. Funksec's insights suggest "**adaptive ransomware**" could evolve its behavior to **evade detection**, like analyzing EDR logs or monitoring incident response communications to **adjust ransom demands**. Combating this requires investment in AI-powered security, comprehensive training, and stronger public-private collaboration. Preparing for this AI-driven landscape is now essential for digital security.

The Ransomware Wars are far from over. Learn crucial next steps for defending your cyber ecosystem.

PREVIOUS NEXT

Conclusion: The Next Chapter in the Ransomware Wars

Looking ahead, we expect this fragmentation to deepen. In 2025-2026, organizations should anticipate:

- **Higher turnover among ransomware groups,** with more rebranding and copycat activity
- **More affiliate-driven chaos,** where operators reuse access or double-target victims
- **Increased focus on vendors and IT service providers** as high-leverage points
- **Shorter dwell times** between initial access and data theft or extortion
- **More automation and AI-assisted reconnaissance,** accelerating group agility

At the same time, we anticipate continued **progress in law enforcement disruption**, more **cyber insurance scrutiny**, and growing pressure on vendors to demonstrate resilience.

For defenders, this means shifting posture:

- **From visibility to anticipation**
- **From response to resilience**
- **From compliance checklists to adversary modeling**

Ransomware is evolving—but so is the intelligence to fight it. Tools like the Ransomware Susceptibility Index® (RSI™), combined with supply chain monitoring, early warning signals, and proactive outreach, provide the advantage organizations need to hold the line in a battle that is far from over.

The war isn't ending. But the winners will be the ones who see it coming.

Learn more about how Black Kite helps you stay on top of your cyber ecosystem risk.

LEARN MORE

Understand the scope and analytical integrity of this report.

PREVIOUS NEXT

Appendix: Methodology

The findings in this report are the result of a comprehensive year-long investigation conducted by the **Black Kite Research & Intelligence Team (BRITE)**, covering the period between **April 1, 2024, and March 31, 2025**. The methodology combines continuous monitoring of ransomware operations with detailed victim analysis and dark web intelligence gathering.

1. Ransomware Group Monitoring

BRITE monitored activity from over 150 ransomware groups, tracking their leak sites, extortion posts, and public disclosures. A group was considered “active” if it published at least one victim within the last 12 months. By March 2025, 96 groups met this threshold.

2. Victim Enumeration and Analysis

A total of **6,046 victims** were identified through leak site monitoring, cross-validated with open-source intelligence and internal telemetry. For each victim, BRITE analysts determined:

- **Industry classification** using **NAICS codes**
- **Headquarters location** by country

Estimated company size based on publicly available financials or trusted databases

BRITE also leveraged the Black Kite platform to assess each victim’s **cybersecurity posture before and after the incident**, helping to identify patterns in susceptibility and exposure.

3. Dark Web and Telegram Intelligence

To complement leak site tracking, BRITE actively monitored **ransomware blogs**, **Telegram channels**, and **dark web forums** to identify group narratives, affiliate activity, and coordination patterns. This enabled the team to detect new groups quickly and contextualize victim disclosures beyond surface-level postings.

4. Limitations

The dataset reflects **only publicly disclosed victims**. Many incidents—especially those involving smaller companies or settled quietly—are never made public. As a result, this report represents a **conservative baseline**, with the actual number of ransomware attacks likely much higher.

BRITE uses standardized methodology to avoid overcounting. For example, attacks affecting **chains of clinics**, **dealer networks**, or **affiliated subsidiaries** are treated as a single victim where appropriate, unless separate disclosures exist.