BLACKFOG.COM

BLACKFOG®

The State of Ransomware

Q4 | 2025

FIGURES UP TO THE END OF Q4, 2025

Introduction

Welcome to BlackFog's fourth quarterly ransomware trend report for 2025.

Since 2020, BlackFog has been tracking and documenting publicly disclosed ransomware attacks through our award-winning State Of Ransomware blog. As a recognized leader in ransomware statistics, we continue to refine our data collection efforts. In 2023, we expanded our scope to include undisclosed attacks reported on dark web leak sites, allowing for a more complete view of the global ransomware landscape.

While our trend reports were shared monthly in previous years, 2025 marked our shift to a quarterly format, designed to deliver deeper analysis and richer insights. Each edition features a breakdown of ransomware activity and trends, key news stories, profiles of emerging ransomware groups, and actionable cybersecurity guidance.

Q4 | 2025
The Unrelenting Surge: Ransomware Closes Q4 At Record Levels

Publicly disclosed attacks continued to bring in record-breaking figures with 272 attacks, an 18% increase compared to the same quarter in 2024.

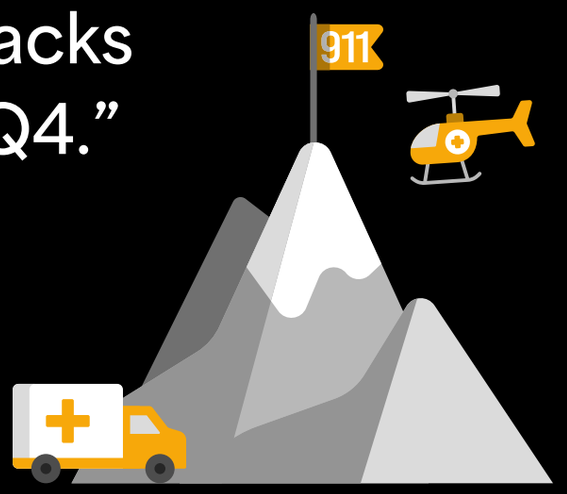
All months in Q4 recorded the highest levels for this quarter since tracking began in 2020, with year-on-year increases exceeding 10%. October saw both the highest number of attacks (102) and the largest percentage increase (28%), while November and December recorded increases of 11% and 16%, respectively.

Unsurprisingly, healthcare was the top targeted industry with 57 attacks, representing 21% of all disclosed attacks in Q4. It was followed by services with 44 and retail and government tying for third place with 27. These four industries account for 57% of the total disclosed attacks in the last three months of 2025.

48 ransomware groups were linked with attacks in Q4. For the third quarter running, **Qilin** was the most active group with 11% of attacks. 40% of disclosed ransomware attacks are yet to be publicly attributed to a known ransomware group.

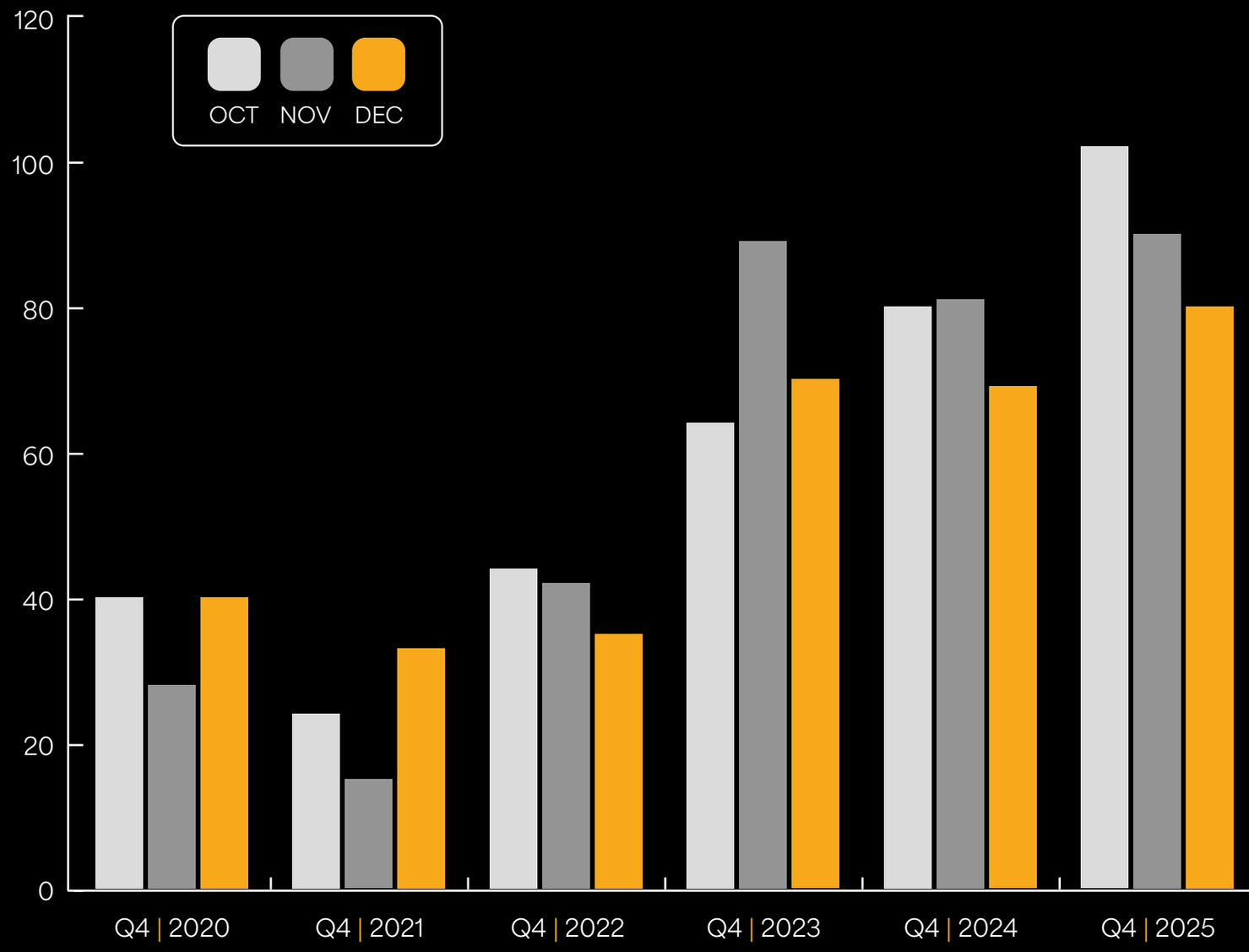
The rate of data exfiltration stood strong at 96% for the second quarter in a row, continuing the trend of data exfiltration as a top tactic for threat actors.

> Unsurprisingly, **healthcare** was the top targeted industry with **57 attacks**, representing 21% of all disclosed attacks in Q4.”



Q4 | 2025 YOY

Disclosed Ransomware Attacks By Month



	TOTAL	YOY
Q4 | 2020	95	NA
Q4 | 2021	72	↓ 24%
Q4 | 2022	121	↑ 68%
Q4 | 2023	223	↑ 84%
Q4 | 2024	230	↑ 3%
Q4 | 2025	**272**	**↑ 18%**

DID YOU KNOW?

Disclosed **ransomware attacks** have surged by

186%

SINCE 2020

Data exfiltration remained at an all-time high of

96%

40% of disclosed ransomware attacks this quarter have **not yet been claimed** by a known threat group.

Organizations in **37 countries** were impacted by publicly **disclosed attacks**.

The **utilities sector** recorded **10 attacks**, marking its highest quarterly total this year.

Q4 | 2025
The Unseen Scale: Only 1 In 7 Attacks Are Publicly Disclosed

In Q4 2025, an estimated 1,998 ransomware attacks went undisclosed, representing an 18% increase compared to the same period in 2024.

This highlights a persistent lack of transparency around the true scale of ransomware activity, with approximately 86% of attacks in Q4 remaining unreported publicly. Put into perspective, only around one in seven ransomware incidents become public knowledge.

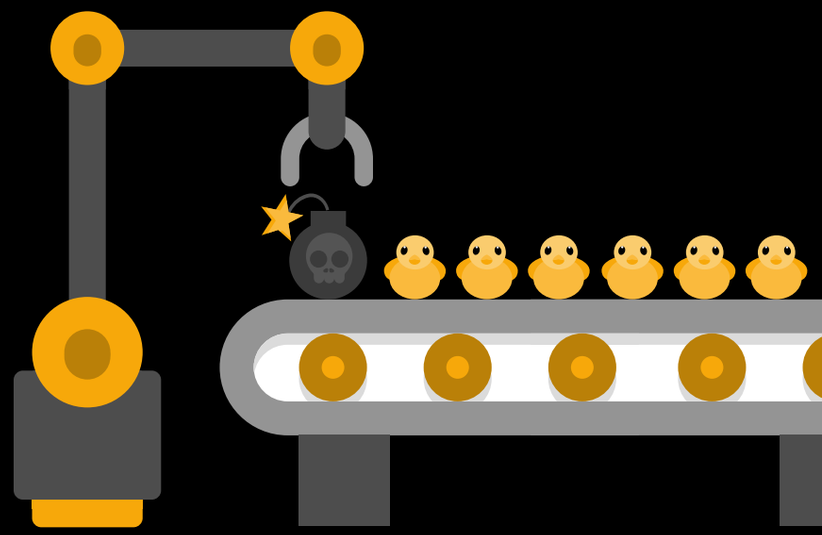
On a monthly basis, all three months of the quarter recorded year-on-year increases in undisclosed attacks. December saw the sharpest rise at 27%, followed by October with a 20% increase. November recorded a more modest increase of 8%, with 640 undisclosed attacks observed.

The manufacturing sector was the most heavily impacted, with ransomware groups claiming 487 undisclosed attacks. Services and construction followed, recording 406 and 230 attacks respectively, placing these industries among the most targeted during the quarter.

A total of 68 ransomware groups listed new victims on their dark web leak sites between October and December. **Qilin** was the most active variant, accounting for 23% of all undisclosed attacks. **Sinobi**, a newly emerged ransomware group in 2025, ranked third this quarter with 137 attacks, demonstrating that newer actors are capable of generating significant impact alongside established groups.

Based on dark web posts disclosing data volumes, the average amount of data exfiltrated per attack was approximately 423 GB. Meanwhile, the average ransom demand stood at around $355,000, based on the limited number of leak site posts that publicly revealed ransom demand figures.

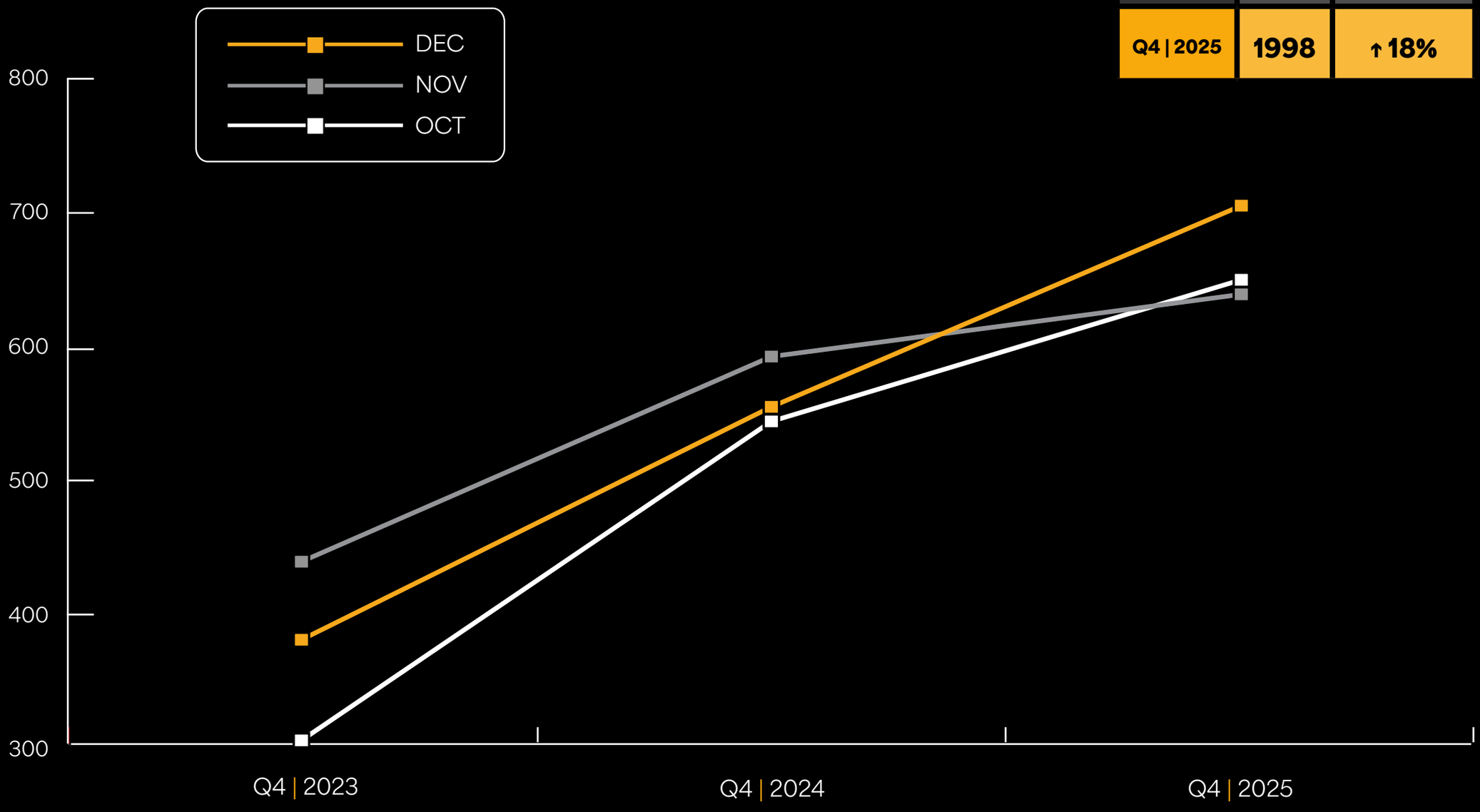
> The **manufacturing** sector was the most heavily impacted, with ransomware groups claiming **487 undisclosed attacks.**”



Q4 | 2025 YOY

Undisclosed Ransomware Attacks By Month

	TOTAL	YOY
Q4 | 2023	1120	NA
Q4 | 2024	1691	↑ 51%
Q4 | 2025	1998	↑ 18%



DID YOU KNOW?

The largest recorded **data exfiltration** totalled **35 TB** attributed to **Qilin** following an attack on **NovAtel**.

8 new ransomware groups emerged between October and December.

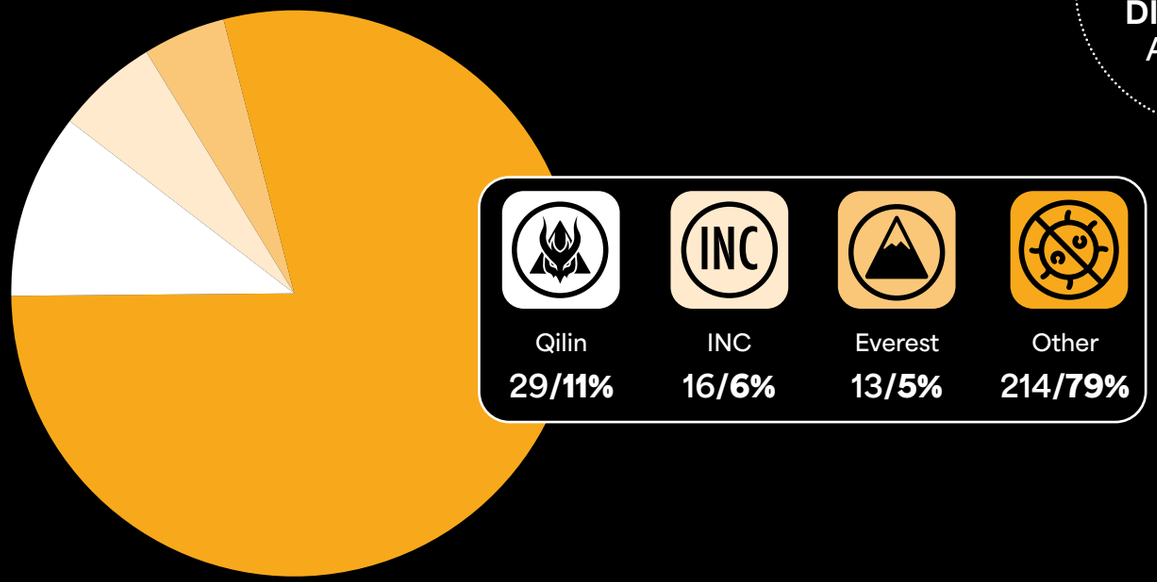
Ransomware groups targeted organizations across **94 countries**.

A total of **68** ransomware variants published victim data on **dark web leak sites** during the quarter.

The Arts and Entertainment sector was linked to **68 attacks**, marking a **record-breaking quarterly total** for the industry.

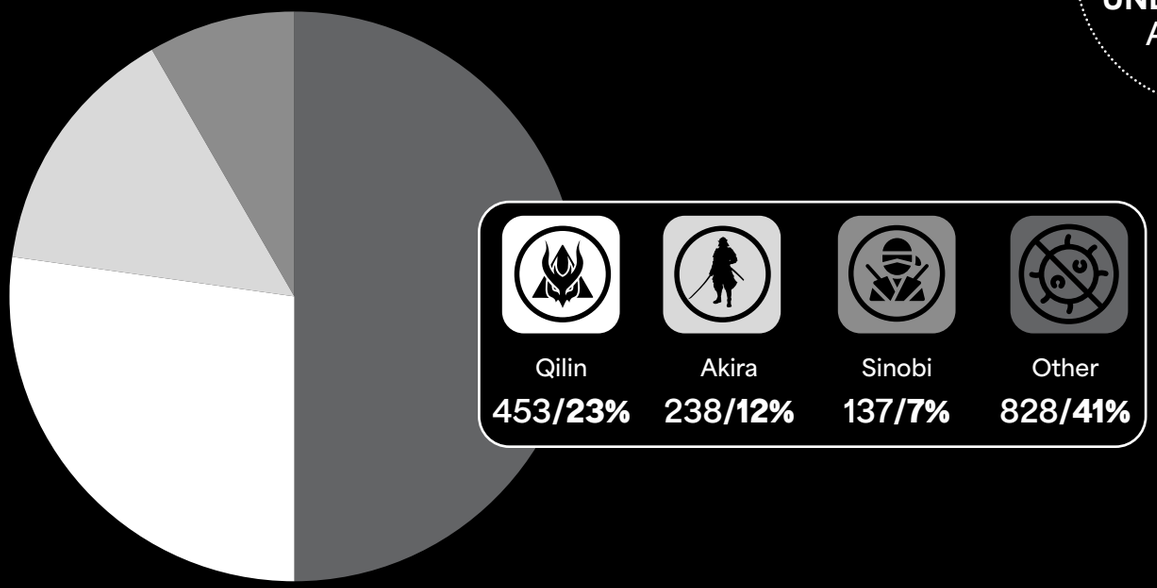
Q4 | 2025
Disclosed Ransomware Attacks By Group

272
DISCLOSED
ATTACKS



Q4 | 2025
Undisclosed Ransomware Attacks By Group

1998
UNDISCLOSED
ATTACKS



FEATURED GROUP

Sinobi: A Rapidly Emerging Ransomware Threat

Sinobi is a ransomware group that emerged in 2025 and has quickly become a prominent new entrant in the ransomware landscape. Despite its recent appearance, the group demonstrated a high level of operational activity in Q4, positioning itself among the more active ransomware operations observed during the quarter.

In Q4 alone, **Sinobi** was linked to 137 ransomware attacks, ranking third for undisclosed incidents. This level of activity is notable for a group in its first year of operation and highlights how rapidly new ransomware actors can scale. **Sinobi**'s rise reflects the increasingly low barrier to entry within the ransomware ecosystem, where access to tooling, infrastructure, and affiliate-style models allows newer groups to compete with more established operations.

Like many modern ransomware groups, **Sinobi** relies heavily on data exfiltration and the use of dark web leak sites to pressure victims. While detailed insight into its tooling, initial access methods, and potential affiliations remain limited, the group's consistent posting activity suggests a structured operation rather than a short-lived or opportunistic campaign.

Sinobi's emergence underscores a broader shift in the ransomware threat landscape, where new groups are capable of creating immediate and sustained impact. Its Q4 performance serves as a reminder that organizations must remain vigilant not only against well-known ransomware brands, but also against rapidly emerging actors that can gain traction in a matter of months.

Q4 | 2025
Top 5 Reported Attacks

Throughout Q4 2025, several high-profile targeted cyberattacks highlighted evolving ransomware and data extortion tactics. The following five publicly disclosed attacks stand out for their scale, visibility, and downstream impact across infrastructure, transportation, manufacturing, and technology.

1.

In late December 2025, the European Space Agency (ESA) confirmed a cybersecurity incident affecting a small number of external servers that were outside its core corporate network and used for unclassified collaborative engineering/scientific work. The incident followed claims by an actor using the alias “888” (reported as posted on cybercrime forums) alleging theft of 200 GB of data, with screenshots shared as proof. ESA said a forensic analysis was ongoing and stakeholders were notified, while noting the affected systems were external to its corporate network.

2.

On October 26, 2025, the Everest ransomware group claimed it had stolen 1,533,900 passenger records linked to Dublin Airport, listing the organization on its leak site, threatening publication. Reporting indicated the claim centered on a password-protected archive of data, with public statements and investigations continuing at the time of coverage. At the time of reporting, the full scope and impact of the alleged data theft had not yet been independently confirmed.

Q4 | 2025 Top 5 Reported Attacks

3.

LG Energy Solution confirmed a ransomware incident affecting one overseas facility, stating other sites (including headquarters) were not impacted and that operations were restored. The **Akira** ransomware group claimed responsibility and alleged the theft of approximately 1.7 TB of sensitive data, including employee details and corporate documents, with threats to publish if demands were not met. LG's confirmation of the incident, paired with **Akira**'s leak site claims, makes this one of the more consequential Q4 public disclosures involving a major global manufacturer.

5.

In early October 2025, reporting surfaced around a threat group referred to as **Crimson Collective**, which claimed access to Red Hat systems and shared evidence such as directory listings and screenshots. Red Hat confirmed a security incident, while noting it could not verify all attacker claims being circulated publicly at the time. The significance here is Red Hat's role in widely used enterprise infrastructure; even when the public narrative centers on repository access and data exposure claims, downstream trust and supply-chain concerns elevate the impact of the disclosure.

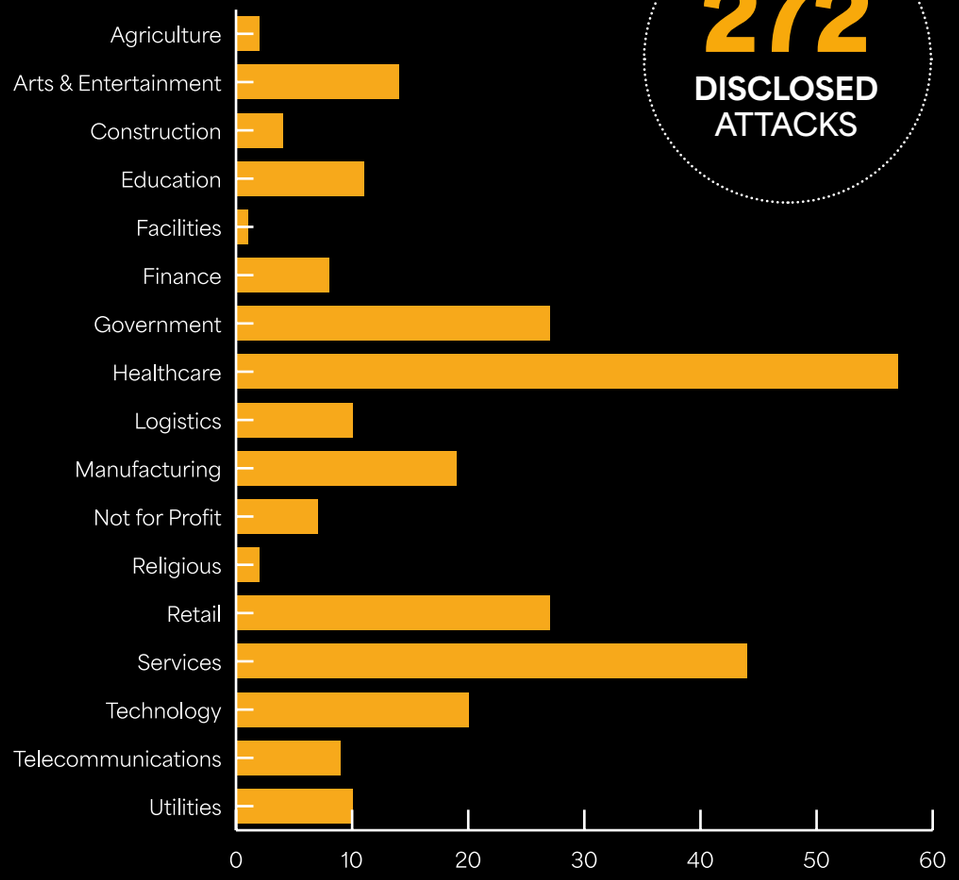
> Across Q4 2025, attackers claimed **large-scale data theft**, leveraged leak sites, and used **public pressure** tactics to amplify impact."

4.

Volkswagen Group France was posted to the **Qilin** ransomware group's leak site on October 14, 2025. **Qilin** claimed to have exfiltrated roughly 150 GB (around 2,000 files) containing sensitive client, employee, and business information, publishing sample files as proof. This incident stood out in Q4 due to the combination of brand profile, claimed data volume, and the use of leak-site pressure tactics.

Q4 | 2025

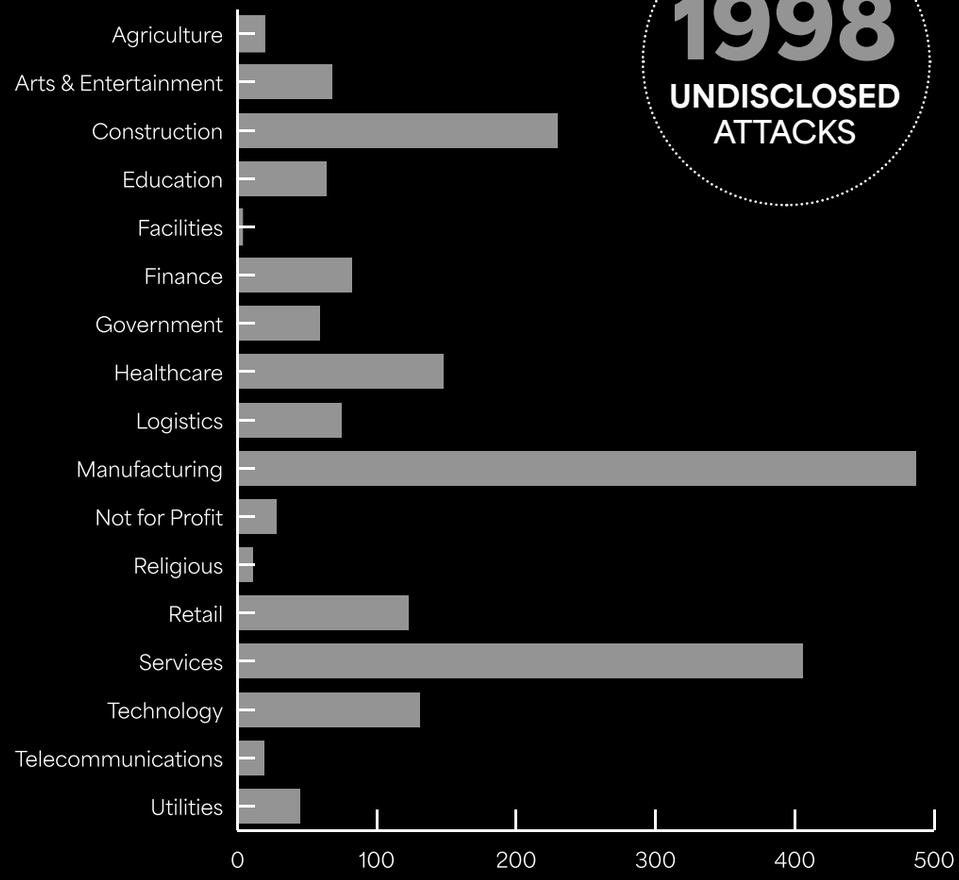
Disclosed Ransomware Attacks By Industry



272
DISCLOSED ATTACKS

Q4 | 2025

Undisclosed Ransomware Attacks By Industry



1998
UNDISCLOSED ATTACKS

Q4 | 2025
Evolving Legal Responses To Ransomware In 2025

As ransomware continues to grow in scale and impact globally, governments are increasingly acknowledging that guidance and voluntary best practices are no longer enough.

Ransomware has become a global, economically driven threat that disrupts critical services, exposes sensitive data, and sustains organized criminal networks. Persistent underreporting and unrestricted ransom payments have limited law enforcement visibility and allowed the ransomware economy to thrive, prompting policymakers in 2025 to pursue stronger legislative intervention.

Several countries introduced or advanced measures designed to improve transparency and disrupt ransomware's financial incentives. In the United Kingdom, proposed legislation seeks to ban ransom payments by public sector bodies and critical national infrastructure operators, introduce pre-payment notification requirements, and mandate ransomware incident reporting. Australia moved further by implementing mandatory ransomware payment reporting under its Cyber Security Act, requiring eligible organizations to report extortion payments within defined timeframes. Together, these developments signal a shift toward treating ransomware as a regulatory and national security issue rather than solely a technical problem.

What this means for organizations: ransomware response decisions are increasingly subject to legal and regulatory scrutiny. Organizations should expect greater expectations around disclosure, governance, and justification of payment decisions, alongside a growing emphasis on visibility into data exfiltration and attacker activity. As legislation evolves, proactive monitoring, accurate incident reporting, and a clear understanding of data movement will become critical components of ransomware preparedness and compliance.

> Ransomware is now being treated as a **regulatory and national security issue**, not just a technical problem."

Q4 | 2025
Top 3 Targeted Countries

DISCLOSED

01	USA	151	56%
02	AUS	33	12%
03	CAN	9	3%

UNDISCLOSED

01	USA	1065	53%
02	CAN	118	6%
03	GER	62	3%

In The News

Two developments in Q4 underscore how cyber risk is increasingly driven by the misuse of trusted technologies rather than traditional exploits. From the growing adoption of Shadow AI outside organizational oversight to the abuse of browser push notifications as a persistent attack channel, these trends highlight a widening visibility gap that security leaders must address to prevent data exposure and loss.

Shadow AI: The Hidden Threat Leaders Can No Longer Ignore

As AI adoption accelerates across enterprises, a new and often overlooked risk is emerging: Shadow AI. These unauthorized tools and models operate outside formal IT and security oversight, quietly accessing and processing sensitive data. Unlike traditional shadow IT, Shadow AI can ingest, learn from, and redistribute enterprise information, significantly increasing the risk of data leakage, intellectual property exposure, and compliance failures.

Dr. Darren Williams, our Founder and CEO, explains why Shadow AI is rapidly becoming a major blind spot for organizations. He highlights how productivity-driven AI use frequently outpaces governance and why traditional perimeter-based security controls are not designed to address AI driven data movement. The discussion reinforces the need for real-time visibility and proactive data protection to ensure AI innovation does not come at the expense of security.

'Matrix Push' C2 Tool Hijacks Browser Notifications

BlackFog threat intelligence highlighted how cybercriminals are increasingly weaponizing browser push notifications as a high-trust, persistent attack channel. Tools such as Matrix Push C2 demonstrate how attackers are abusing legitimate browser functionality to establish direct communication with victims, often without deploying malware or exploiting vulnerabilities. By prompting users to allow notifications on malicious sites, threat actors gain an ongoing delivery mechanism for phishing and malicious redirects that blends seamlessly into everyday browser behaviour.

A broader shift in attacker tactics has emerged, moving away from traditional email phishing toward browser-integrated command-and-control channels that bypass many conventional security controls. Because these notifications appear legitimate and impersonate trusted brands, they significantly increase user trust and click-through rates. This evolution reflects how attackers continue to adapt, repurposing trusted technologies to scale social engineering campaigns and maintain persistence, reinforcing the need for greater visibility and control over outbound data and user interactions.

BlackFog is a global leader in AI-based cybersecurity and the pioneer of anti data exfiltration (ADX) technology. Since inventing ADX, BlackFog has remained relentlessly focused in its mission to prevent unauthorized data from leaving the organization, well before data exfiltration became the primary driver of modern cyberattacks.

As threats evolve beyond traditional ransomware and spyware to include the rapid and ungoverned use of AI tools, BlackFog continues to innovate to keep customers ahead of emerging risks. With the expansion of its ADX platform to include advanced protections against Shadow AI, BlackFog empowers organizations to defend their data against both established and next-generation exfiltration threats.

BlackFog's award-winning ADX platform stops data loss at its source by preventing unauthorized data movement across every endpoint and every AI interaction. Operating directly on the device, BlackFog continuously analyzes behavioral signals using advanced AI algorithms, detects abnormal activity, and blocks outbound data flows in real-time. This ensures sensitive information, intellectual property, and other critical data never leave the environment, whether the risk originates from cybercriminals, malicious insiders, or unvetted AI tools.

Recognizing the limitations of perimeter-based defenses, BlackFog delivers a preventative, zero-trust approach that neutralizes attacks before they can be exploited. With unified visibility, automated governance enforcement, and on-device data protection, BlackFog enables organizations to embrace AI confidently while maintaining complete control over their data.

BlackFog's innovation has earned global industry recognition, including the Cybersecurity Breakthrough Award for AI-based Cybersecurity Innovation of the Year, multiple Globee Awards for AI-driven data protection, and continued acclaim for its influential State Of Ransomware research. Trusted by organizations worldwide, BlackFog is redefining modern cybersecurity for the AI era.

Methodology

This report was generated in part from data collected by BlackFog Enterprise over the specific report period July-September 2025. It highlights significant events that prevented or reduced the risk of ransomware or a data breach and provides insights into global trends for benchmarking purposes.

This report contains anonymized information about data movement across hundreds of organizations and should be used to assess risk associated with cybercrime.

Industry classifications are based upon the ICB classification for Supersector used by the New York Stock Exchange (NYSE).

All recorded events are based upon data exfiltration from the device endpoint across all major platforms.

BLACKFOG®

Follow Us

Award-winning Technology

MSP TODAY PRODUCT of THE YEAR 2025 · CYBERSECURITY BREAKTHROUGH AWARD 2024 · 2024 FORTRESS CYBER SECURITY AWARD · teiss Awards 2025 · GLOBEE AWARDS · CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2023

Contact us for a demo

Start your free trial

Visit blackfog.com