BLACKFOG.COM

BLACKFOG®

The State of Ransomware

Q1 | 2026

FIGURES UP TO THE END OF Q1, 2026

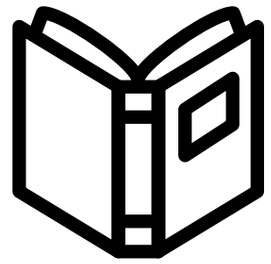
Q1 | 2026 Introduction

Welcome to BlackFog's first quarterly ransomware trend report for 2026.

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 trends and statistics, we continue to refine our data collection efforts. In 2023, we expanded our research 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, and actionable cybersecurity guidance.

Q1 | 2026
264 Publicly Disclosed Ransomware Attacks Underscore Persistent Threat Landscape



While publicly disclosed ransomware incidents declined year-over-year, the overall volume and consistency of activity reinforce that ransomware remains a persistent and highly active threat.

A total of 264 publicly disclosed ransomware attacks were recorded, representing a 15% decrease compared to the same period the previous year. Despite this decline, activity remained steady throughout the first quarter, with 91 attacks in January, 83 in February, and 90 in March.

Healthcare remained the most targeted sector, accounting for 72 attacks (27%), reflecting the continued focus on organizations with sensitive data and limited tolerance for operational disruption. Government entities experienced 32 attacks (12%), while the technology sector followed with 28 attacks (11%).

The ransomware landscape remains fragmented, with **Qilin** emerging as the most active variant, responsible for 22 attacks (8%). **Shiny Hunters** followed with 16 attacks (6%), and **INC** accounted for 11 attacks (4%). Notably, 38% of all publicly disclosed ransomware incidents were not attributed to any known group.

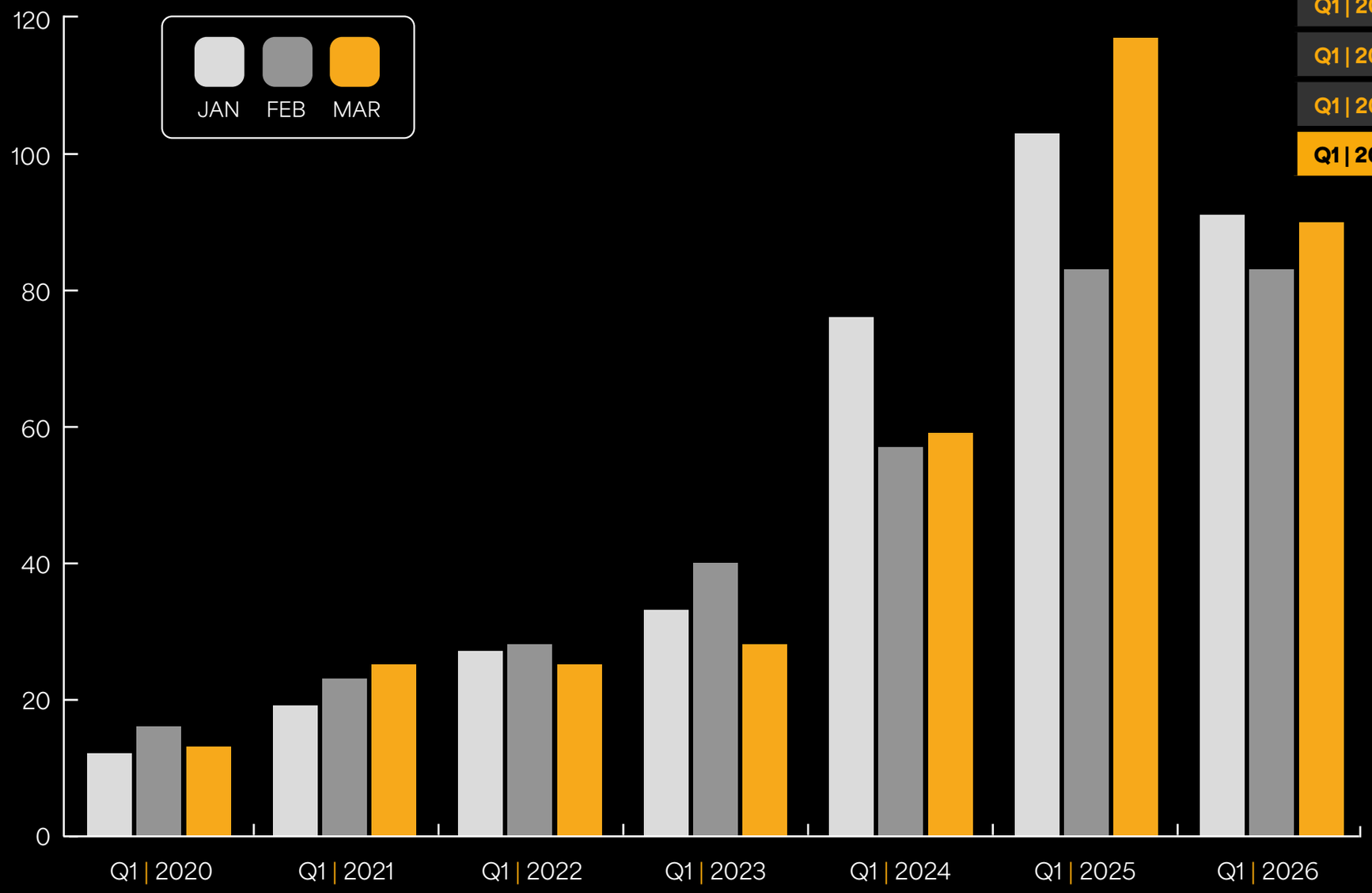
From a geographic perspective, the United States accounted for the majority of incidents, with 161 attacks (61%). Australia reported 14 attacks (5%), while Canada recorded 7 attacks (3%). Notably, ransomware activity was not limited to major economies. Smaller nations including Andorra, Mauritius, Panama, and Namibia also saw organizations impacted, highlighting the truly global reach of modern ransomware operations.

The rate of data exfiltration remained critically high at 96%, holding steady after a spike in 2025. This confirms that threat actors are prioritizing data theft to increase leverage and maximize financial returns.

Overall, while the decline in total attacks may suggest incremental progress, the sustained volume of incidents, high rate of data exfiltration, and significant proportion of unattributed activity demonstrate that ransomware continues to evolve and pose a significant risk to organizations worldwide.

Q1 | 2026 YOY

Disclosed Ransomware Attacks By Month



	TOTAL	YOY
Q1 | 2020	41	NA
Q1 | 2021	67	↑ 63%
Q1 | 2022	80	↑ 19%
Q1 | 2023	101	↑ 26%
Q1 | 2024	192	↑ 90%
Q1 | 2025	303	↑ 58%
Q1 | 2026	**264**	**↓ 15%**

DID YOU KNOW?

Disclosed average **ransom demand** exceeded

$1M

($1,028,214)

Data exfiltration remained at an all-time high of

96%

The average **organization size** jumped to **13,254** employees.

Organizations across **39 countries** were impacted by publicly **disclosed attacks**.

Logistics sector attacks surged **200%** YoY.

Q1 | 2026
Only 1 In 9 Ransomware Attacks Become Publicly Disclosed

The majority of ransomware activity continues to take place below the surface, with undisclosed attacks far exceeding those reported publicly.

A total of 2,160 undisclosed ransomware attacks were identified during the quarter, representing a 2% increase in attacks year-on-year. Monthly volumes varied, with January accounting for 711 attacks (33%), February 654 (30%), and March increasing to 795 (37%). This trend reflects sustained and scalable operations by threat actors.

The ransomware landscape remains diverse. **Qilin** led with 339 attacks (16%), followed by **The Gentlemen** with 200 (9%) and **Akira** with 190 (9%). A total of 79 ransomware groups claimed victims during the three-month period.

Geographically, the United States accounted for 1,070 attacks (50%), representing half of all undisclosed incidents. Canada followed with 103 (5%), and the United Kingdom with 79 (4%). This distribution highlights the continued concentration of ransomware activity in major Western economies. A slight increase in activity was also observed in regions experiencing geopolitical tension, reinforcing the link between instability and elevated threat levels.

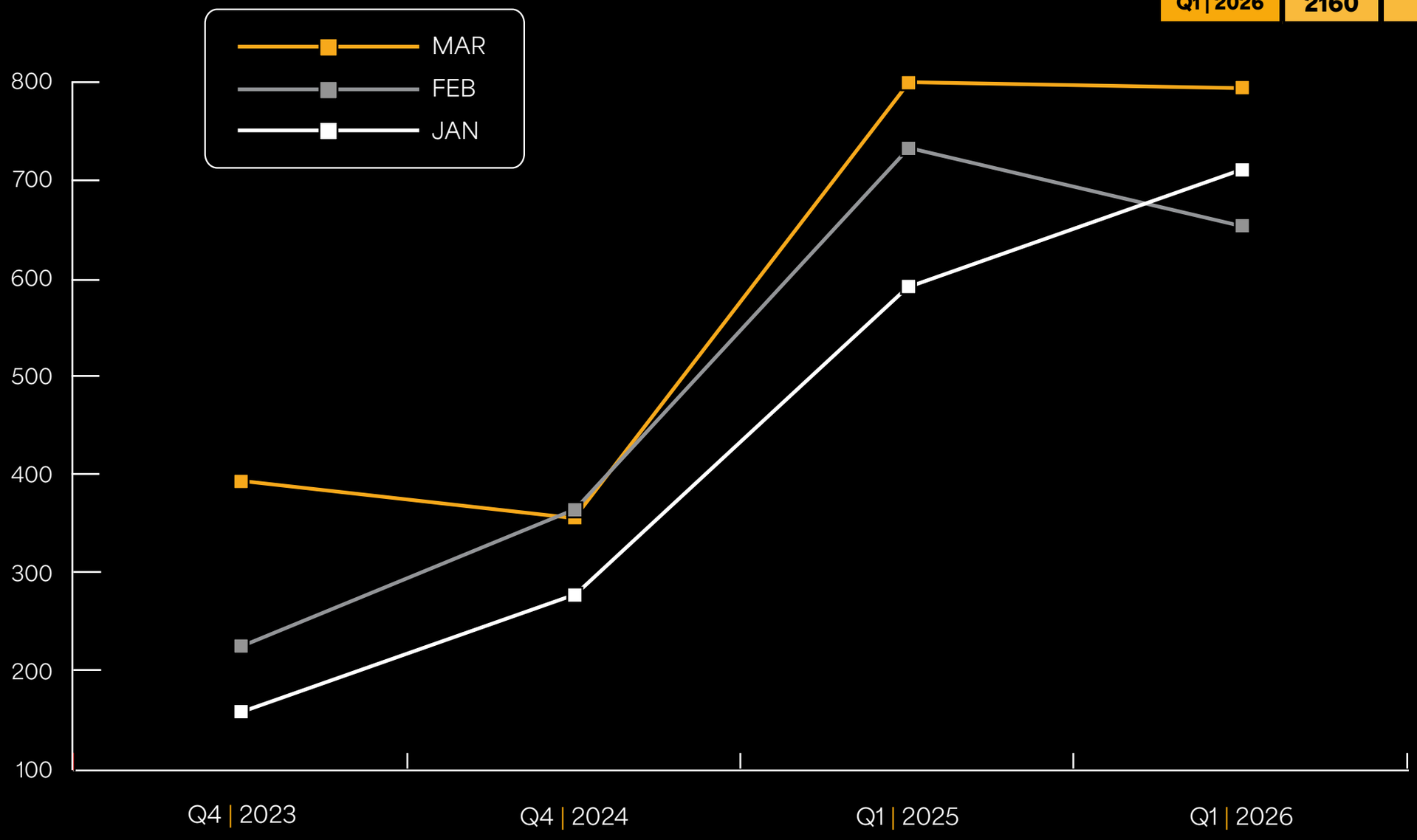
From an industry perspective, manufacturing was the most targeted sector with 466 attacks (22%), closely followed by services at 457 (21%). The construction industry also experienced notable activity, reinforcing the focus on sectors with operational dependencies and limited tolerance for disruption.

Overall, the disparity between disclosed and undisclosed attacks, where only 1 in 9 incidents becomes public, demonstrates the true scale of ransomware activity and reinforces the need for greater visibility and proactive defense strategies.

Q1 | 2026 YOY

Undisclosed Ransomware Attacks By Month

	TOTAL	YOY
Q1 | 2023	776	NA
Q1 | 2024	997	↑ 28%
Q1 | 2025	2125	↑ 113%
Q1 | 2026	**2160**	**↑ 2%**



DID YOU KNOW?

Undisclosed average **ransom demand** stands at **$353,666**

Average **Data exfiltration** reached **743GB**

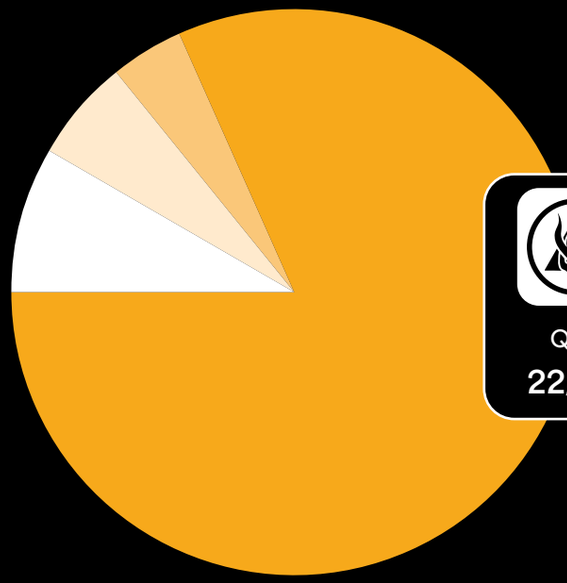
Ransomware groups claimed **victims** across **97** countries.

14 new ransomware groups emerged in **Q1, 2026**.

Average **negotiation deadline** was set at **7.7 days**.

Q1 | 2026
Disclosed Ransomware Attacks By Group

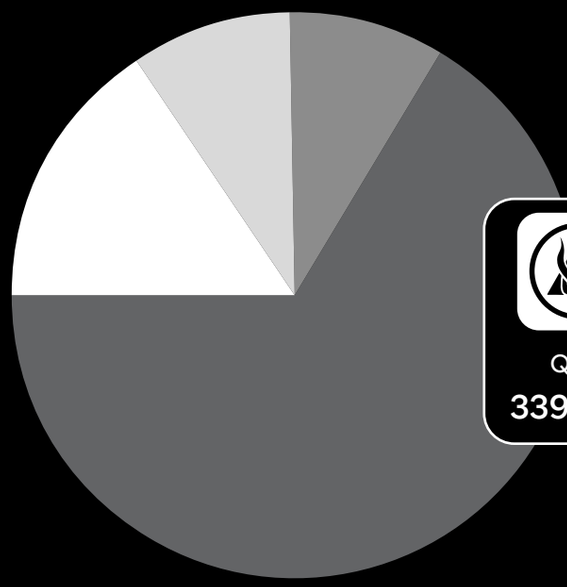
264
DISCLOSED
ATTACKS



Qilin	Shiny Hunters	INC	Other
22/8%	16/6%	11/4%	215/81%

Q1 | 2026
Undisclosed Ransomware Attacks By Group

2160
UNDISCLOSED
ATTACKS



Qilin	The Gentlemen	Sinobi	Other
339/16%	200/9%	190/9%	1431/66%

FEATURED GROUP

The Gentlemen:
A Growing Force in the Ransomware Landscape

The Gentlemen quickly established itself as one of the most active ransomware groups this quarter, ranking second by volume of attacks. Since its emergence in 2025 through to the end of Q1 2026, the group has claimed 273 attacks, reflecting a rapid scale-up in operations and a broader trend of new entrants operating with a high level of maturity from the outset.

The group leverages double extortion tactics, combining data exfiltration with encryption to increase pressure on victims. Their operations are global in scope, with a clear focus on mid- to large-sized organizations where disruption and data exposure can drive higher ransom outcomes.

The Gentlemen demonstrates a strong level of operational sophistication. Observed tactics include the abuse of legitimate administrative tools, lateral movement within networks, and efforts to evade detection. This indicates a more targeted approach rather than purely opportunistic attacks.

Sector targeting has aligned with high-impact industries such as manufacturing, construction, healthcare, and services. Their continued presence and volume of activity indicate sustained momentum, positioning **The Gentlemen** as a group to watch as the ransomware landscape continues to evolve.

Q1 | 2026 Ransomware in Focus: Key Incidents

Ransomware activity in Q1 2026 continued to demonstrate both the scale and diversity of modern attacks, with organizations across multiple sectors impacted by data theft, operational disruption, and supply chain compromise. Incidents ranged from platform-level breaches affecting thousands of downstream organizations, to attacks on critical payment infrastructure that halted business operations, and large-scale data exfiltration targeting millions of individuals. The following cases highlight some of the most significant publicly disclosed ransomware incidents from the quarter:

1. Vivaticket (SaaS)

In March 2026, Italian ticketing provider Vivaticket was targeted in a ransomware attack attributed to the **RansomHouse** group, impacting a platform used by more than 3,500 cultural institutions globally. The breach, linked to its subsidiary Irec SAS, affected organizations across over 50 countries, including the Louvre, Musée d'Orsay, and the Eiffel Tower. The incident disrupted online ticketing services, with some venues forced to suspend bookings during remediation. **RansomHouse** claimed to have exfiltrated customer data including names, email addresses, reservation details, and purchase history. While the total number of affected individuals has not been confirmed, the scale of Vivaticket's operations suggests potentially widespread exposure. Investigations were launched by relevant authorities, including ANSSI and the French Ministry of Culture.

2. BridgePay (Finance/Technology)

In February 2026, US-based payment processor BridgePay confirmed a ransomware attack had caused a system-wide outage across its payment gateway infrastructure. The incident began on February 6, with degraded performance escalating to a full shutdown of core services. The disruption affected merchants, municipalities, and service providers nationwide, forcing many organizations to revert to cash-only transactions and take payment portals offline. BridgePay engaged federal authorities, including the FBI and US Secret Service, alongside external cybersecurity and forensic teams to investigate the incident. Initial forensic analysis indicated that files within affected systems were encrypted, but there was no evidence that payment card data had been compromised or that usable data was exfiltrated. The threat actor responsible has not been publicly identified, and no ransomware group has claimed the attack at the time of reporting.

Bridgespeed (Telecommunications)

In January 2026, US telecommunications provider Brightspeed disclosed it was investigating a ransomware-related incident following claims by the **Crimson Collective** extortion group that it had breached company systems and stolen data on more than one million customers. The group announced the attack via Telegram, stating it had exfiltrated personally identifiable information (PII) including names, email addresses, phone numbers, billing and service addresses, account details, and partial payment data. The threat actors also claimed access to customer payment histories and service records, and alleged disruption to user connectivity, although this was not independently verified. Brightspeed confirmed it was investigating the incident but had not verified the full scope of the claims. Following disclosure, the company faced multiple class-action lawsuits alleging failure to adequately protect customer data.

Wynn Resorts (Hospitality)

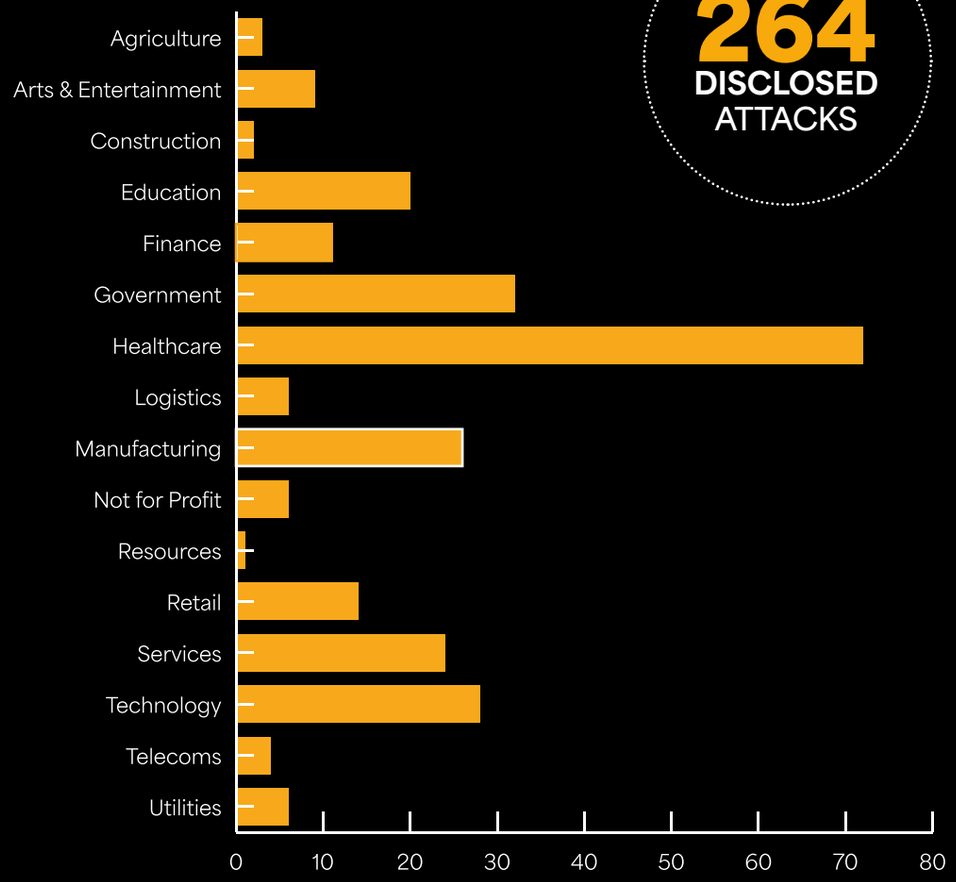
In February 2026, global casino and hospitality operator Wynn Resorts confirmed a data breach following an extortion attempt by the **ShinyHunters** group. The threat actors claimed to have exfiltrated data relating to more than 800,000 individuals, primarily impacting current and former employees. The compromised data reportedly included highly sensitive personally identifiable information (PII), such as Social Security numbers, dates of birth, contact details, and employment records. The breach was linked to unauthorized access to an internal HR system, with reports indicating threat actors may have exploited weaknesses in Oracle PeopleSoft software used for payroll and personnel management. **ShinyHunters** listed the company on its leak site and issued a ransom demand of approximately $1.5 million to prevent publication. Wynn Resorts acknowledged that employee data had been accessed and said threat actors later claimed it had been deleted, although this was not independently verified.

Telus Digital (Enterprise/Data)

In March 2026, Telus Digital, the business process outsourcing (BPO) arm of Canadian telecom provider Telus, confirmed it had been impacted by a cybersecurity incident following claims by **ShinyHunters**. The threat actors alleged they had exfiltrated nearly one petabyte of data, potentially making it one of the largest data theft claims to date, and issued a ransom demand in the tens of millions, which Telus declined to pay. **ShinyHunters** claimed the breach was enabled through compromised Google Cloud Platform credentials from a prior third-party incident, allowing access to multiple systems and additional credentials. Data allegedly included customer information from enterprise clients, such as call records, source code, background check data, and operational datasets, although Telus said its investigation was ongoing. The company confirmed only a limited number of systems were affected and operations remained fully functional, with no evidence of disruption to core services, highlighting the risk associated with BPO providers where a single compromise can expose data across multiple downstream organizations.

Q1 | 2026

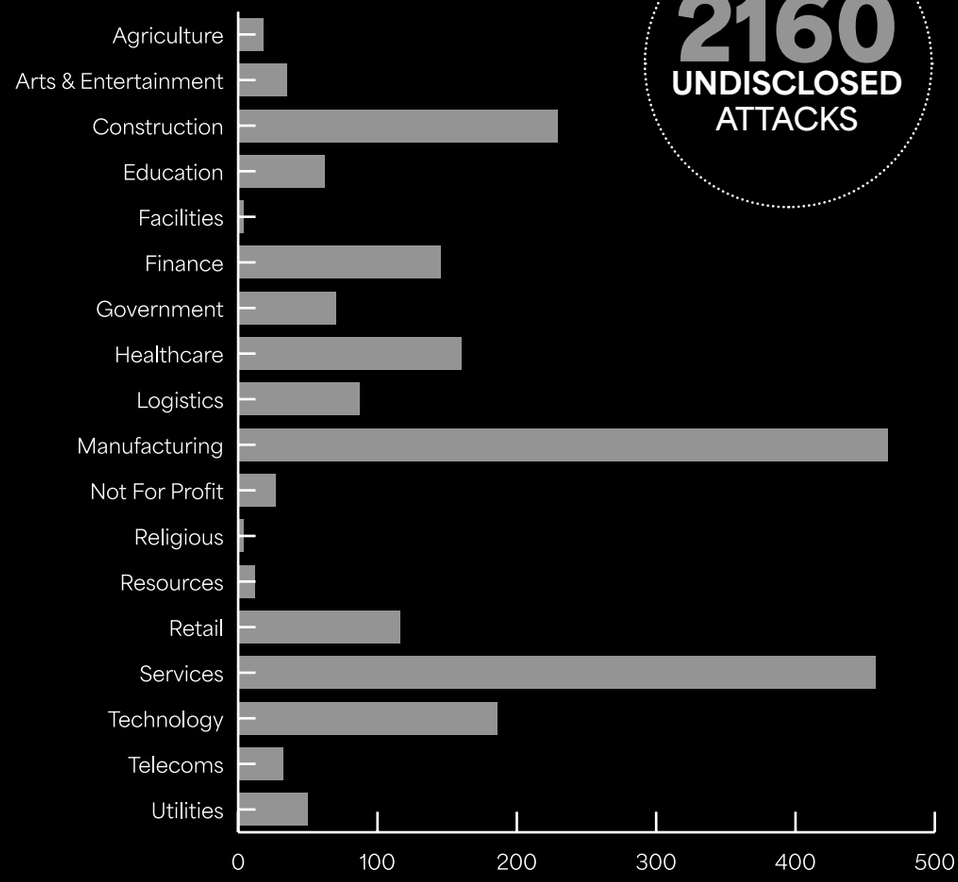
Disclosed Ransomware Attacks By Industry



264
DISCLOSED
ATTACKS

Q1 | 2026

Undisclosed Ransomware Attacks By Industry



2160
UNDISCLOSED
ATTACKS

Emerging Threats Enabling Data Exfiltration

Threat activity in Q1 2026 highlights a set of emerging threats that, while not always deploying ransomware directly, play a clear role in how attacks are executed and monetized. The focus continues to be on credential theft, persistent access and data exfiltration, capabilities that support double extortion and follow-on ransomware activity. The threats below, analyzed by BlackFog's threat intelligence team, reflect a shift toward more accessible and scalable tooling that reduces complexity and shortens the path from compromise to impact.

Venom Stealer (ClickFix Exfiltration Pipeline)

Identified in March 2026, Venom Stealer is a MaaS infostealer that turns social engineering into a continuous data exfiltration pipeline. Delivered via "ClickFix" lures like fake CAPTCHA or update prompts, it relies on user-assisted execution to bypass security controls. Once active, it targets browser credentials, session cookies and cryptocurrency wallets, while maintaining persistence to capture newly stored data in real time. Unlike conventional stealers, Venom enables ongoing compromise rather than a single theft event, increasing risk exposure and rendering remediation less effective.

Lotus C2 (Cybercrime Framework-as-a-Kit)

Lotus C2 is a newly observed command-and-control framework marketed as a ready-to-use cybercrime kit. Emerging in early 2026, it provides pre-configured infrastructure for managing infections, deploying payloads and maintaining persistence across compromised environments. Its modular design and ease of use lower the barrier to entry for less sophisticated actors, enabling broader adoption of advanced attack capabilities. This reflects the continued industrialization of cybercrime, where scalable, off-the-shelf infrastructure drives more frequent and coordinated attacks.

Steaelite RAT (Double Extortion from a Single Panel)

Steaelite RAT is an emerging all-in-one threat that combines remote access, data exfiltration and extortion within a single platform. Designed with a streamlined control panel, it enables threat actors to rapidly move from initial compromise to monetization without relying on multiple tools. By supporting both persistent access and immediate data theft, Steaelite facilitates double extortion from a single deployment. This convergence reduces threat actor effort while accelerating attack timelines, increasing both the speed and impact of breaches.

The Void (MaaS Infostealer)

The Void is a MaaS infostealer identified in 2026, focused on large-scale credential and data theft. Distributed via underground marketplaces, it enables threat actors to launch campaigns with minimal technical expertise. The malware targets high-value data including login credentials, browser information and financial assets, supporting rapid monetization through follow-on attacks such as ransomware and account takeover. Its accessibility and efficiency make it a high-volume threat, contributing to the growing scale of data exfiltration activity.

Q1 | 2026
Top 3 Targeted Countries

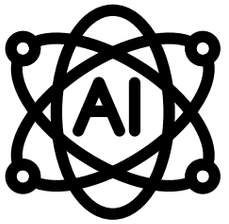
DISCLOSED

01	USA	161	61%
02	AUS	14	5%
03	CAN	7	3%

UNDISCLOSED

01	USA	1070	50%
02	CAN	103	5%
03	UK	79	4%

Q1 | 2026
Shadow AI and Uncontrolled Data Exposure



The rapid adoption of generative AI is introducing new data exfiltration risks, with shadow AI emerging as a key concern for organizations. The use of unsanctioned AI tools is creating uncontrolled pathways for sensitive data to leave the enterprise, often without visibility or oversight. Unlike traditional shadow IT, AI tools actively process and retain user inputs, making them a direct channel for data exposure.

Shadow AI: Expanding the Attack Surface

BlackFog research highlights the scale of shadow AI usage and the associated risk.

- **86%** of employees use AI tools weekly at work
- **49%** use AI tools not approved by their employer
- **60%** say speed is worth the security risk
- **51%** have integrated AI tools with other systems without IT approval

This widespread and often unsanctioned use of AI is creating new pathways for sensitive data to be exposed outside of organizational control.

Sensitive Data Exposure Through AI Tools

The data being shared through AI platforms is not limited to low-risk inputs. BlackFog research shows:

- **27%** have shared employee data
- **33%** have shared research or datasets
- **58%** rely on free AI tools lacking enterprise-grade protections

These behaviors significantly increase the risk of sensitive data being processed, stored or reused outside of approved environments.

AI Weaponized for Data Exfiltration

Threat actors are also leveraging AI to streamline and scale data theft. Campaigns such as LotAI demonstrate how AI tools can be used to automate data collection and exfiltration. Platforms like ClawdBot and OpenClaw further highlight how AI-driven infrastructure can aggregate, process and manage stolen data more efficiently, accelerating the path from compromise to monetization.

Exploiting User Interaction with AI

User trust in AI platforms is also being targeted. Prompt poaching campaigns, including fake ChatGPT browser extensions, are designed to capture sensitive inputs, credentials and proprietary data entered into AI tools. These attacks turn legitimate AI usage into an entry point for data exfiltration.

What This Means for Organizations

AI is rapidly becoming both a productivity tool and a data exfiltration vector. As adoption increases, the combination of shadow AI usage and AI-enabled threats is expanding the enterprise attack surface. Addressing this risk requires greater visibility into how AI tools are being used across the organization, alongside the ability to monitor and control the flow of sensitive data in real-time.

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 leaves 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 The BlackFog Console over the specific report period January-March 2026. 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

Contact us for a demo

Start your free trial

Visit blackfog.com