BLACKFOG.COM

BLACKFOG®

The State of Ransomware

Q1 | 2025

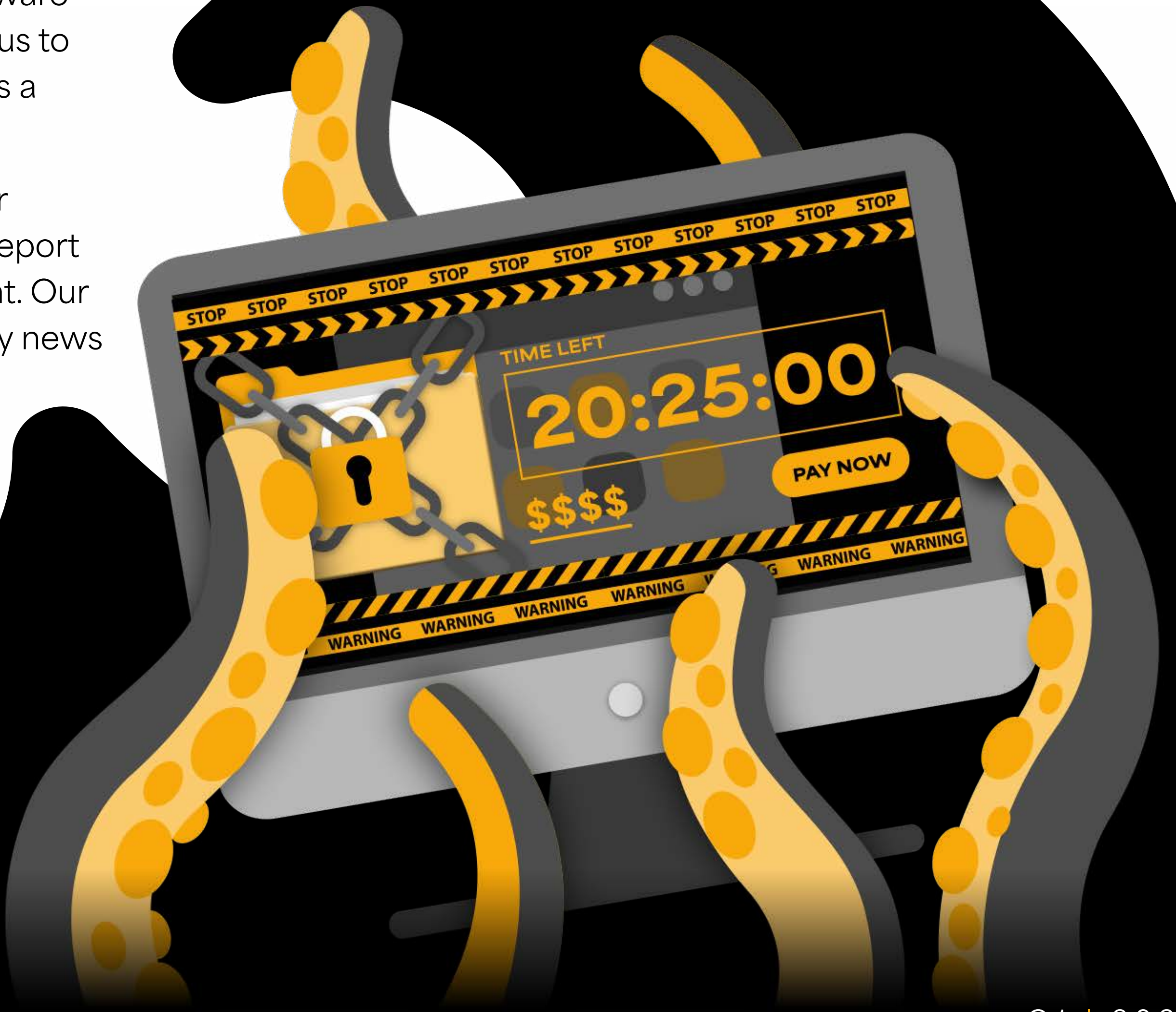
FIGURES UP TO THE END OF Q1, 2025

Introduction

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

Since 2020 BlackFog has been tracking and documenting publicly disclosed ransomware attacks in its award-winning State of Ransomware blog. As a market leader in ransomware statistics, we continually improve the data we collect, and in 2023 we added undisclosed ransomware attacks listed on dark web leak sites and the dark web, enabling us to provide a more detailed picture of the ransomware landscape as a whole.

In past years, our ransomware trend reports were emailed to our subscribers on a monthly basis. In 2025 we've transitioned this report to a quarterly format to enable us to share more detailed content. Our expanded reports will include ransomware trends, a look into key news stories, new ransomware groups on the horizon and valuable cybersecurity tips.



Disclosed Attacks: Q1 Breaks All Previous Records

The first quarter of 2025 saw record-breaking numbers of publicly disclosed ransomware attacks, with a total of 278 incidents, marking a notable 45% increase compared to Q1 2024.

March set a new high, recording the largest number of disclosed attacks since we began tracking in 2020, with 107 attacks. Both January and February also set new monthly records, seeing increases of 22% and 36%, respectively.

There was a slight shift in industry rankings, as education was moved out of the top three for the first time in five years, making room for the services industry to join healthcare and government on the podium. Together, attacks on these three sectors accounted for nearly half (47%) of all incidents in the quarter.

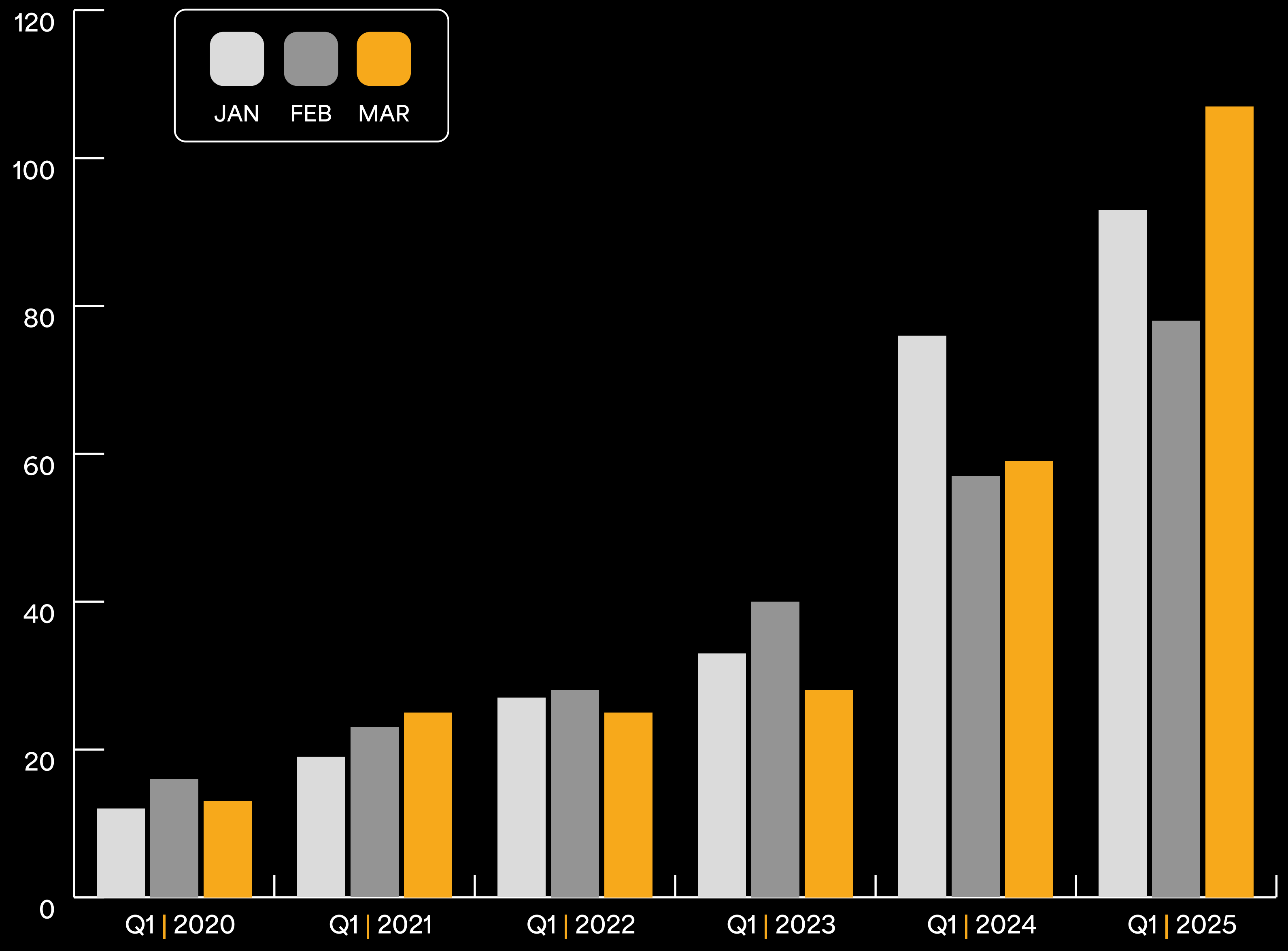
Following a particularly active 2024, it comes as no surprise that RansomHub was responsible for the majority of attacks in the first three months of 2025. Additionally, seven new ransomware gangs claimed high-profile attacks.

The rate of data exfiltration has continued to rise, with research revealing that 95% of all publicly disclosed attacks in Q1 2025 involved data exfiltration.

> “The rate of data exfiltration has continued to rise, with research revealing that 95% of all publicly disclosed attacks in Q1 2025 involved data exfiltration.”

Q1 | YOY

Disclosed Ransomware Attacks by Month



	TOTAL	INCREASE YOY
Q1 | 2020	41	
Q1 | 2021	67	↑ 63%
Q1 | 2022	80	↑ 19%
Q1 | 2023	101	↑ 26%
Q1 | 2024	192	↑ 92%
Q1 | 2025	**278**	**↑ 45%**

DID YOU KNOW?

Monthly Breakdown

(Q1 2024 vs Q1 2025)

JAN
22%
INCREASE

FEB
36%
INCREASE

MARCH
81%
INCREASE

Q1 attacks have dramatically increased each year, with % increases ranging from **19%** (2022 vs 2021) to **92%** (2024 vs 2023).

64 attacks making the news remain **unclaimed** by ransomware gangs, representing **23%** of the total.

Smaller countries such as **Turks and Caicos**, **Palau**, the **Bahamas** and even **Micronesia** were targeted by cybercriminals.

57% of all attacks use **PowerShell**.

Undisclosed Attacks: The True Representation of the Ransomware Rampage

As in the past two years, the number of unreported incidents continues to rise exponentially in 2025.

In Q1 alone, there were 2,124 undisclosed attacks, marking a staggering 113% increase compared to the same period in 2024. This indicates that the number of undisclosed attacks is approximately 764% higher than the number of disclosed attacks, highlighting that companies are still failing to publicly disclose ransomware incidents when they are targeted.

Clop emerged as the most prolific attacker, responsible for 12% of all incidents in the quarter, with the majority, if not all, of these attributed to the attack on Cleo. RansomHub followed closely behind with 234 victims. Additionally, 12 new ransomware groups posted about their victims on dark web blogs, with Frag, which appeared in March, leading the pack with 27 victims.

The services sector was the hardest hit, accounting for 22% of all undisclosed attacks in Q1. The manufacturing and technology sectors were also significantly impacted, with 434 and 210 attacks, respectively.

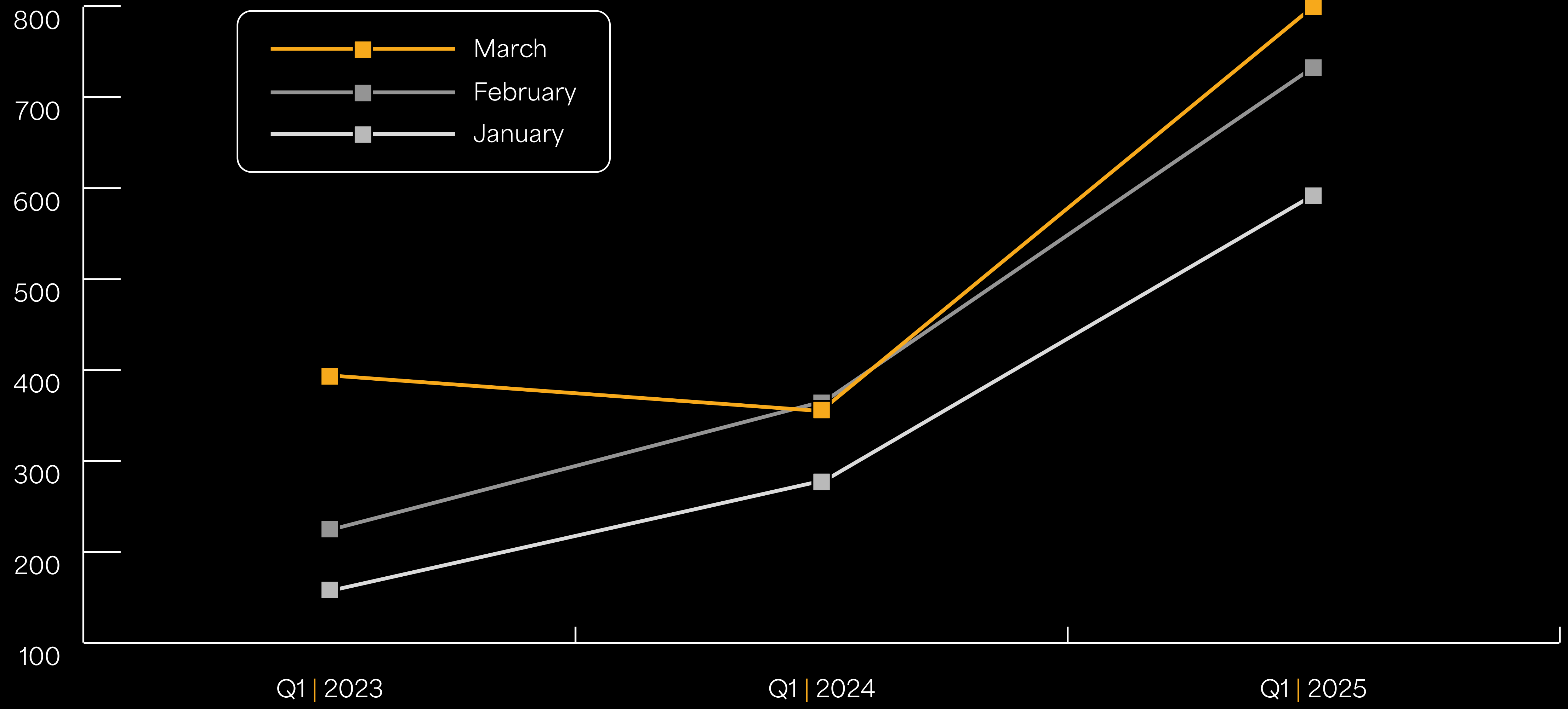
On average, 1.58TB of data was exfiltrated per attack, with 752 incidents revealing the volume of data taken in dark web postings. The average known ransom demand stood at approximately $663,000.

> “The **services sector** was the hardest hit, accounting for **22% of all undisclosed attacks** in Q1.”

Q1 | YOY

Undisclosed Ransomware Attacks by Month

	TOTAL	INCREASE YOY
Q1 | 2023	776	
Q1 | 2024	997	↑ 28%
Q1 | 2025	2124	↑ 113%



DID YOU KNOW?

The average ransom demand is now

$663,582

93 claims published ransom demands with Medusa accounting for the majority.

The **legal** and **logistics** industry suffered more attacks than recorded previously for Q1.

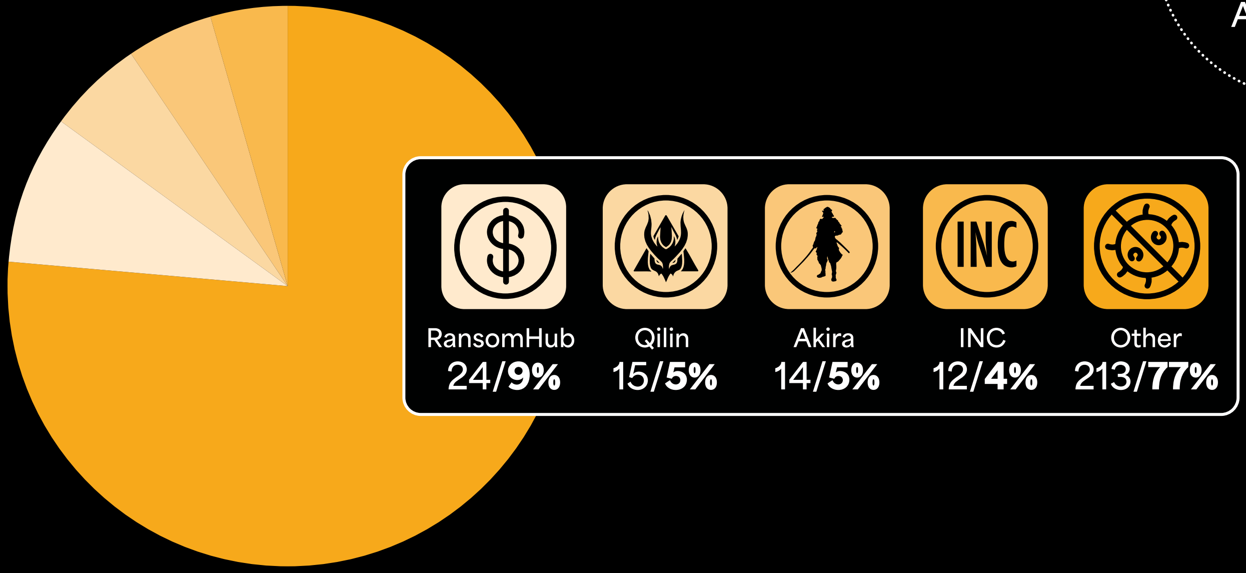
Canada was the second hardest hit country behind USA, with **124 companies** being targeted.

33% of attacks on the **government sector** targeted US municipalities or government bodies.

The **average company size** is now **3,700**.

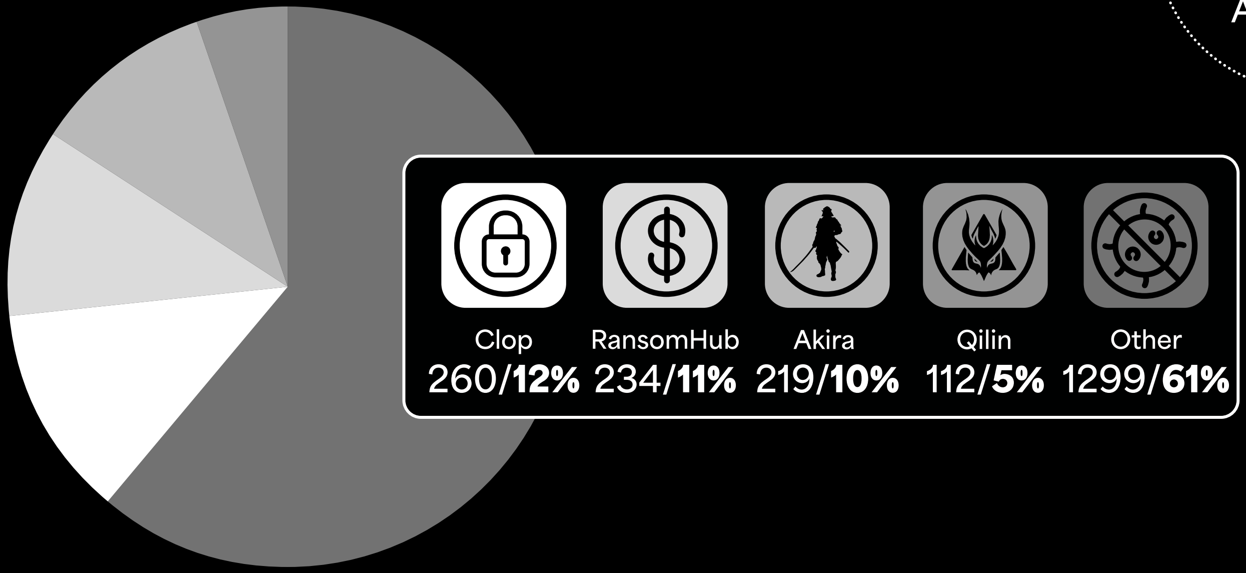
Q1 | 2025
Disclosed Ransomware Attacks by Variant

278
DISCLOSED
ATTACKS



Q1 | 2025
Undisclosed Ransomware Attacks by Variant

2124
UNDISCLOSED
ATTACKS



FEATURED GANG

Babuk - Real Threat or Fake News?

Babuk ransomware group, active since 2021, has experienced a noticeable resurgence in early 2025. After announcing their retirement from ransomware operations in mid-2021, they re-emerged with a new attack on Cync Solutions on January 27, 2025.

In late January 2025, Babuk's dark web leak site saw a surge in activity, with the group claiming over 64 victims across various sectors, including energy, manufacturing, government, IT, and healthcare. Although providing little information about the attacks, the gang appears to have exfiltrated data from all its claimed victims.

However, it appears that 90% of its listed victims were found to have been claimed by other groups such as LockBit, RansomHub and Funksec. Is this resurgence legitimate or is Babuk a fraud?

Top 5 Reported Attacks

We've looked at the attacks this quarter and highlighted five of the most significant ones - some stand out due to the information exfiltrated, others because of the ransom demands, and a few for the disruption they caused.

1

In January, a new ransomware campaign targeting Amazon Web Services users by a threat actor known as Codefinger dominated the news. The attack leveraged AWS's server-side encryption in order to encrypt data and then demand payment for decryption keys. The attack campaign relies upon obtaining an AWS customer's account credentials. Amazon stated that it is aware of exposed keys and that customers would be notified.

2

PowerSchool, an education software provider, informed individuals in the U.S. and Canada that their personal information was exposed in a ransomware attack that occurred in late December 2024. During the breach, attackers gained unauthorized access to one of the company's customer support portals, stealing sensitive data from 6,505 school districts. The stolen information included a variety of data including full names, physical addresses, contact details, Social Security numbers (SSNs), medical records, and academic results. A threat actor involved in the attack, claimed in their extortion demand to have stolen data on 62,488,628 students and 9,506,624 teachers, suggesting the breach affected a significant number of individuals.

Top 5 Reported Attacks

3

Qilin took responsibility for a cyberattack on Lee Enterprises which caused widespread network outages, disrupting many of the company's 70-plus newspapers and other publications. A SEC filing stated that threat actors had unlawfully accessed the organization's network, encrypted critical applications and exfiltrated certain files. The organization also commented that many operations including distribution, billing, collection and vendor payments had been impacted by the incident. Qilin claimed to have stolen 350GB of data including investor records and financial arrangements that would allegedly raise some questions.

4

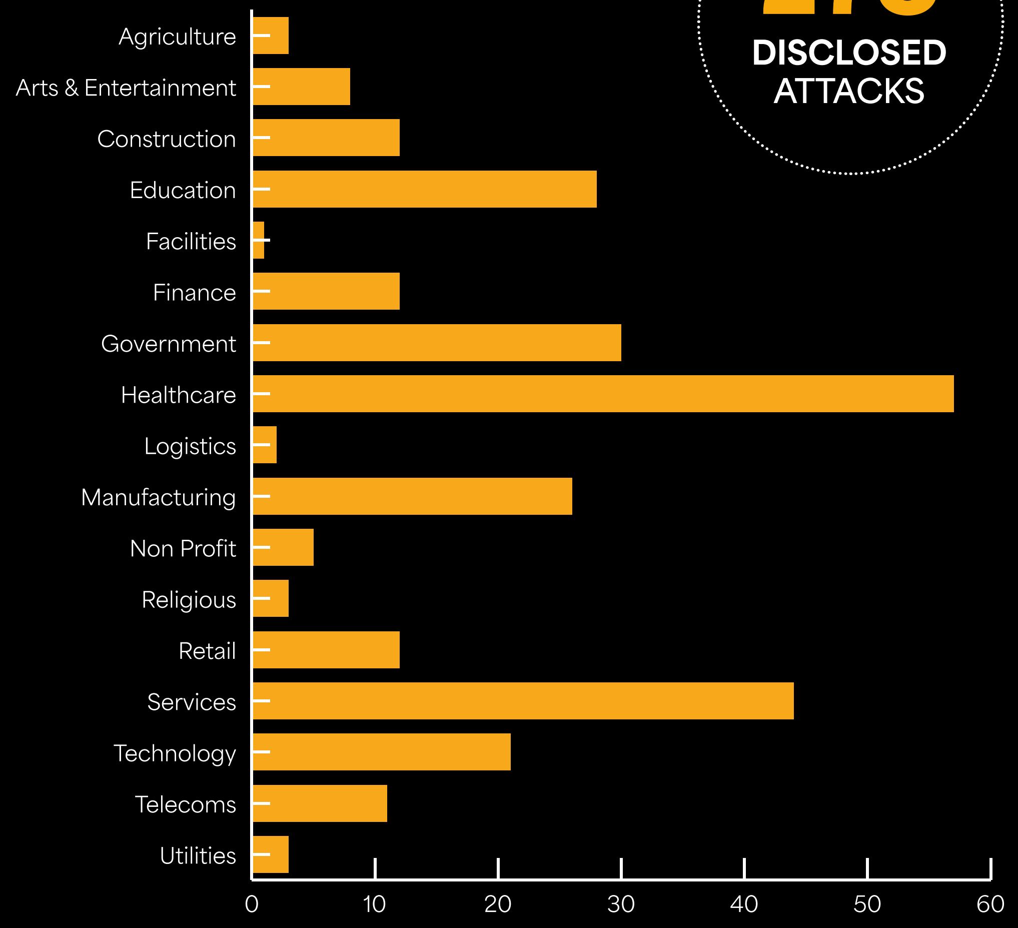
RansomHub took credit for a ransomware attack on the Sault Ste. Marie Tribe of Chippewa in Michigan. The attack forced multiple computer and phone systems out of operation for an indefinite period in a number of organizations including casinos, health centers and various other businesses. The threat actors claimed to have exfiltrated 119GB of confidential information from the tribe, with some news outlets reporting that the ransom demand stood at $5million.

5

Almost 2.3TB of data belonging to HCRG Care Group was held to ransom by Medusa ransomware gang. HCRG, which runs child and family health and social services in the UK, was added to the ransomware gang's leak site alongside a demand of $2 million in exchange for the stolen data. Samples of the data which included passports, driving license scans, staff rotas, birth certificates, and data from background checks, has already been released. HCRG is currently investigating these claims.

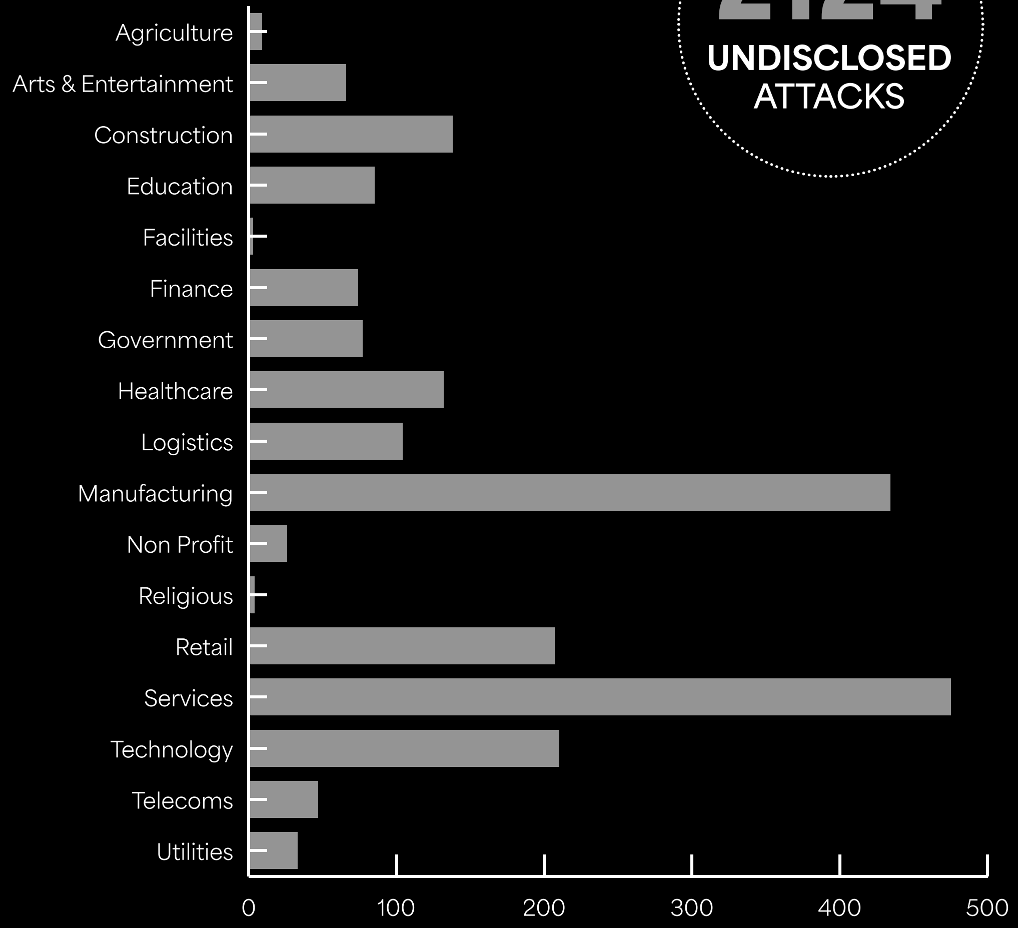
Q1 | 2025
Disclosed Ransomware Attacks by Industry

278 DISCLOSED ATTACKS



Q1 | 2025
Undisclosed Ransomware Attacks by Industry

2124 UNDISCLOSED ATTACKS



Q1 | 2025

Top 3 Targeted Countries

DISCLOSED				UNDISCLOSED		
USA	145	52%	01	1173	55%	USA
AUS	34	12%	02	124	6%	CAN
UK	9	3%	03	87	4%	UK

DATA HEIST

China, Russia, and Ukraine are the **top players in data exfiltration**, responsible for **22%**, **5%**, and **0.2%** of **global breaches**, respectively. These nations utilize illegal networks to **channel sensitive data** to remote servers.

In the News

As usual it's been a busy quarter for ransomware and cybersecurity news. Here's a snapshot of a few we thought you'd enjoy reading.

23andMe Files for Bankruptcy Protection: What Will Happen to Your Data?

The recent bankruptcy filing of 23andMe, a prominent genetic testing company, has attracted significant attention. But what will happen to the extensive genetic data the company possesses?

Many are concerned about where their data will end up, and if there is a chance that it will end up in the hands of cybercriminals. Our CEO shared his thoughts on this breaking story.

Shadow AI: The Silent Threat to Enterprise Data Security

As AI tools rapidly gain traction in the workplace, a new threat has emerged: Shadow AI. Our CEO highlighted the risks associated with employees using unsanctioned AI platforms, exposing sensitive company data to potential breaches.

With AI's ability to self-learn and integrate vast amounts of sensitive information, the dangers of data exfiltration are higher than ever.

This new threat emphasizes the need for robust AI governance policies and the importance of enterprise-grade security to combat this growing threat. Security leaders must not only react to current risks but also anticipate AI's evolving role in the workplace.

FBI Warning on the Medusa Ransomware Threat

The Medusa ransomware gang has triggered a new wave of concern for organizations globally, with their increasingly aggressive tactics and sophisticated ransomware-as-a-service (RaaS) model.

From targeting critical infrastructure to using AI-powered phishing and 'living off the land' techniques, Medusa's reach is vast and its impact severe.

Medusa's success is partly fueled by AI, which enables more targeted and effective attacks. They're not just encrypting data – they're stealing it and threatening to leak sensitive information unless the ransom is paid. The group's tactics are becoming a major test of resilience for critical organizations.

About BlackFog

Founded in 2015, BlackFog is a global AI based cybersecurity company that has pioneered on-device anti data exfiltration (ADX) technology to protect organizations from ransomware and data loss.

With more than 95% of all attacks involving some form of data exfiltration, preventing this has become critical in the fight against extortion, the loss of customer data and trade secrets.

BlackFog recently won the “Best Threat Intelligence Technology” in the 2024 Teiss Awards, “AI-based Cybersecurity Innovation of the Year” award in the CyberSecurity Breakthrough Awards, as well as the 2024 Fortress Data Protection award for its pioneering anti data exfiltration (ADX) technology.

BlackFog also won Gold at the Globee awards in 2024 for best Data Loss Prevention and the State of Ransomware report which recognizes outstanding contributions in securing the digital landscape.

Trusted by hundreds of organizations all over the world, BlackFog is redefining modern cybersecurity practices. For more information visit blackfog.com

Methodology

This report was generated in part from data collected by BlackFog Enterprise over the specific report period January - March 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 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