BLACKFOG.COM

BLACKFOG®

The State of Ransomware

Q2 | 2025

FIGURES UP TO THE END OF Q2, 2025

Introduction

Welcome to BlackFog's second 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.

Q2 | 2025
Ransomware: Record Breaking Surge Continues

Publicly disclosed ransomware attacks reached new heights in Q2 2025, with a total of 276 incidents. This represents a sharp 63% increase compared to the same period in 2024.

All three months set new records. June led with a 113% year-over-year spike in attack volume. April and May recorded 89 and 91 attacks respectively, the highest totals ever observed for those individual months since 2020.

Healthcare was the most targeted industry, reporting 52 attacks. Government and Services followed with 45 and 33 incidents respectively. Together, these three sectors accounted for 47% of all publicly disclosed attacks in the quarter.

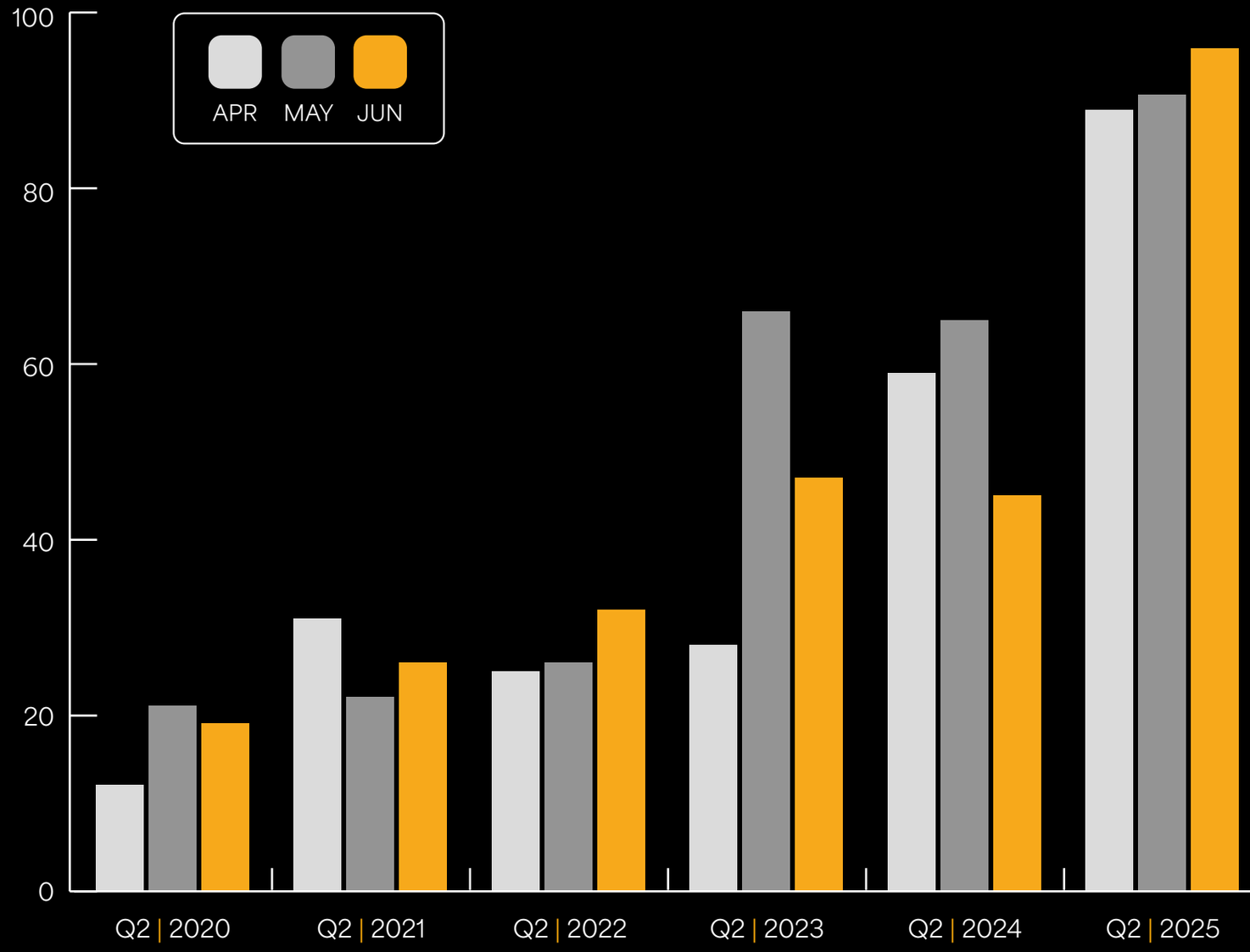
A total of 53 ransomware groups were active. **Qilin** was the most prominent, responsible for 10% of the claims. 11% of all publicly disclosed attacks were attributed to groups that emerged in 2025.

The use of data exfiltration remained consistently high, with 95% of publicly disclosed attacks involving the theft of sensitive information.

“The use of **data exfiltration** remained consistently high, with **95%** of **publicly disclosed attacks** involving the theft of sensitive information.”

Q2 | 2025 YOY

Disclosed Ransomware Attacks by Month



	TOTAL	INCREASE YOY
Q2 | 2020	52	
Q2 | 2021	79	↑ 52%
Q2 | 2022	83	↑ 5%
Q2 | 2023	141	↑ 70%
Q2 | 2024	169	↑ 20%
Q2 | 2025	**276**	**↑ 63%**

DID YOU KNOW?

Monthly Breakdown

(Q2 2024 vs Q2 2025)

APRIL
51%
INCREASE

MAY
40%
INCREASE

JUNE
113%
INCREASE

Q2 attacks have steadily increased each year, with % increases ranging from **5%** (2022 v 2021) to **70%** (2023 v 2022).

97 attacks remain unclaimed by ransomware gangs, representing **35%** of the total.

Ransomware remained a **global menace** with organizations in **40 countries** reporting incidents.

Retail and **Arts & Entertainment** sectors recorded **highest-ever** Q2 attack volumes.

Q2 | 2025
Undisclosed Attacks: Revealing the Hidden Ransomware Landscape

In Q2, 1,446 ransomware attacks were not publicly disclosed, reflecting a 19% increase compared to the same quarter in 2024.

The scale of hidden activity remains significant, with 80.9% of all ransomware attacks going unreported. For every 100 undisclosed incidents, only about 19 were publicly acknowledged, highlighting the substantial gap in visibility.

Qilin was the most active ransomware group in this segment, accounting for 15% of all incidents. **Akira** and **Play** followed closely, ranking as the second and third most active variants. Fourteen new ransomware groups emerged during the quarter; some linked to notable attacks on organizations.

The Services industry was the most targeted sector, accounting for 23% of all attacks in Q2. This was followed by Manufacturing, which experienced 301 incidents, representing 21% of the total.

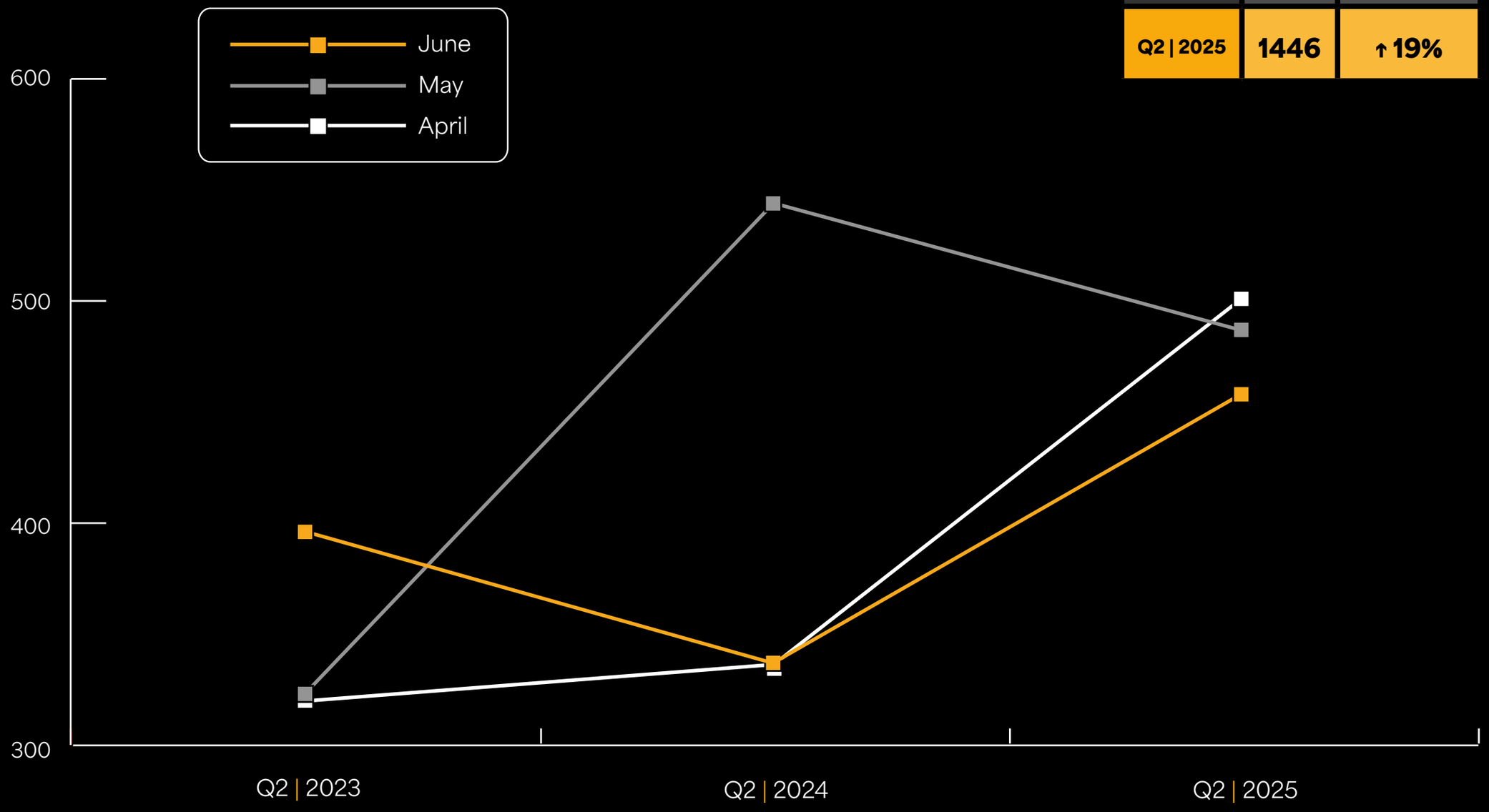
Among attacks where data theft details were available, the average volume of data exfiltrated was 858GB. This figure is based on 609 incidents where leak site posts included specific volume information. Ransom demands were disclosed in 44 cases, with the average demand exceeding $676,000.

“The **Services industry** was the most targeted sector, accounting for **23% of all attacks** in Q2.”

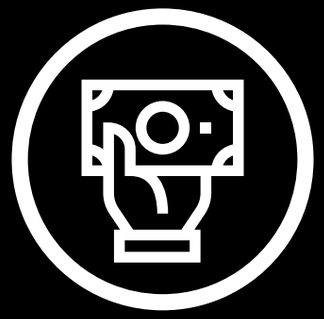
Q2 | 2025 YOY

Undisclosed Ransomware Attacks by Month

	TOTAL	INCREASE YOY
Q2 | 2023	1039	
Q2 | 2024	1217	↑ 17%
Q2 | 2025	1446	↑ 19%



DID YOU KNOW?



The highest ransom demand was **$4.5 million** issued by Devman following its attack on NSSF Kenya.

Construction and **Hospitality** recorded their highest-ever Q2 attack counts.

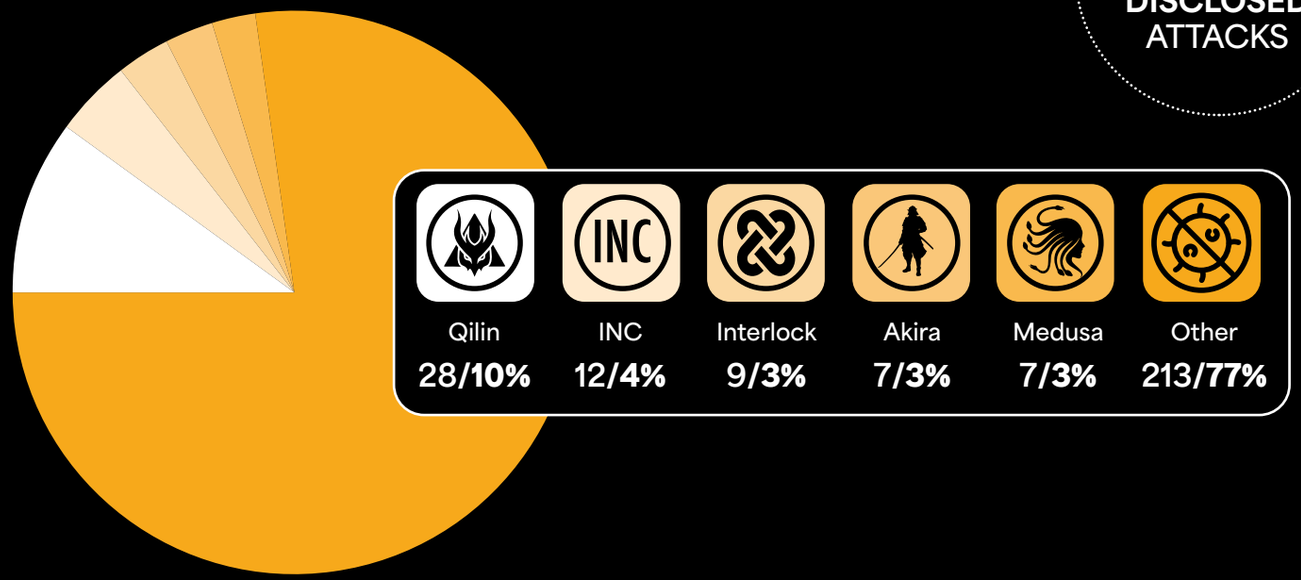
Companies in **88 countries** were targeted, including smaller nations such as Tonga, Haiti, Fiji, and Barbados, where attacks caused **significant organizational disruption**.

20% of **dark web leak** posts included visible proof of claims.

Average victim **organization size** is now **2719**.

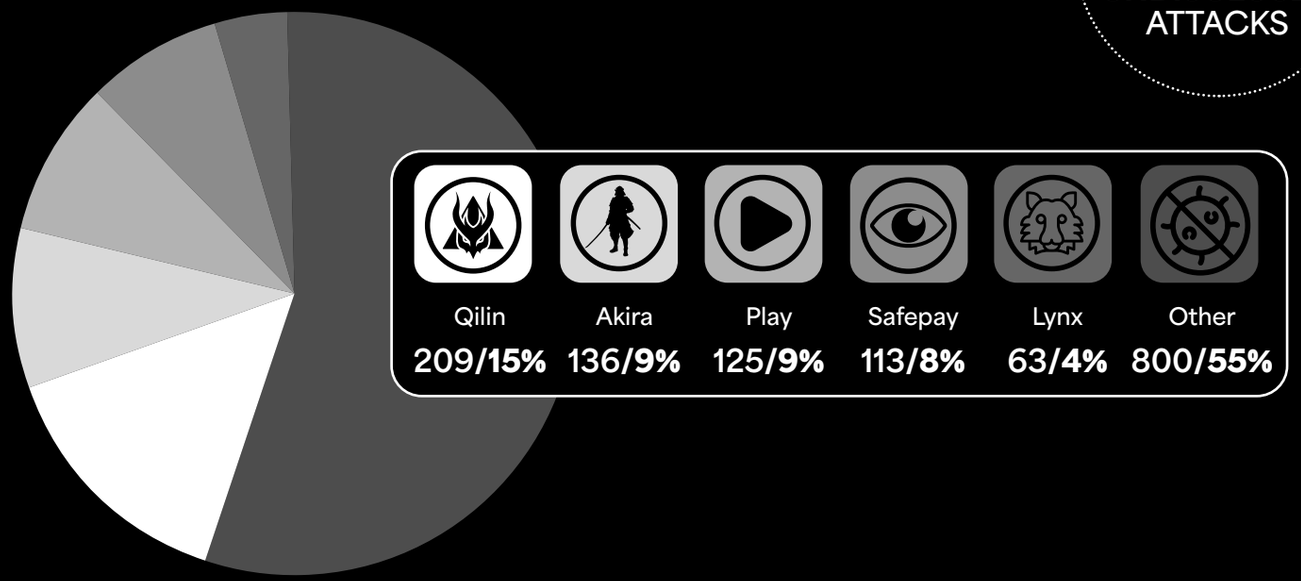
Q2 | 2025
Disclosed Ransomware Attacks by Variant

276
DISCLOSED
ATTACKS



Q2 | 2025
Undisclosed Ransomware Attacks by Variant

1446
UNDISCLOSED
ATTACKS



FEATURED GANG

Qilin Leads Global Ransomware Threat with a Strategic Shift

Qilin has long been a familiar name in the ransomware world, but in Q2 2025, the group shifted into overdrive, emerging as the most dominant threat on the global stage. Between April and June, **Qilin** was behind a staggering 10% of all disclosed ransomware attacks and 15% of those revealed on dark web leak sites, putting it at the top of both categories for attack volume.

The threat became so significant that earlier this year, CISA issued a formal warning after **Qilin** struck high-profile targets in the U.K. and the U.S., labeling the group a major risk to critical infrastructure.

As **Qilin** continues to evolve alongside other top ransomware gangs, it recently grabbed headlines by unveiling a new and unsettling tactic in its arsenal: affiliates now have access to lawyers who guide them on how to turn up the heat in ransom negotiations. These legal advisors offer intel on the stolen data's regulatory impact, potential violations, and projected fallout costs, turning every breach into a calculated campaign of psychological and financial pressure.

Armed with advanced techniques and bold new strategies, **Qilin** is no longer just keeping up with the ransomware landscape; it is setting the pace.

Q2 | 2025 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 mid-April 2025, Denver based DaVita Inc., one of the largest kidney dialysis providers in the U.S. with nearly 3,000 outpatient clinics serving around 200,000 patients, disclosed a ransomware attack that encrypted portions of its network. The breach, which the company reported via an SEC Form 8K on April 14, forced DaVita to isolate affected systems and invoke contingency protocols to maintain patient care, despite ongoing operational disruptions whose duration remains unclear. Additionally, **Interlock** ransomware gang has claimed responsibility, allegedly exfiltrating up to 1.5 TB of sensitive data, roughly 700,000 files, though DaVita is still investigating the extent of any data compromise and plans to notify impacted individuals as appropriate.

2.

In late April 2025, the U.K.'s Legal Aid Agency, responsible for administering legal aid applications and billing, was hit by a significant cyberattack. By mid-May, it emerged that attackers had accessed and stolen a "significant amount" of sensitive personal data dating back to 2010, including names, addresses, dates of birth, national insurance numbers, criminal history, employment status, financial contributions, debts, and payment information. In response, the LAA's digital services were taken offline and an injunctive order was obtained to prevent public disclosure of the stolen data. This disruption triggered administrative chaos, affecting over 1,700 attorneys and litigators, delaying payments, and piling pressure on firms already operating on tight margins. The Ministry of Justice, along with the NCA, NCSC, and ICO, are leading the investigation, urging affected individuals and providers to monitor for suspicious activity and update their credentials.

Q2 | 2025 Top 5 Reported Attacks

In May, Kenya's NSSF was struck by a ransomware attack orchestrated by the group **Devman**, which claimed to have locked down systems, stolen 2.5 TB of data from an image storage server, and demanded a ransom of approximately $4.5 million with a 24-hour ultimatum. Although the attackers alleged they had encrypted all devices and pilfered member data, the fund maintains that its core systems, containing personal and financial records, remained secure, stressing that only a non-critical image repository was affected. In a concerning twist, **Devman** released technical details on June 7 showing how they exploited forgotten RDP credentials and network misconfigurations, highlighting vulnerabilities around access controls, large-scale data exfiltration via Mega.nz, and modus operandi aligned with MITRE ATT&CK patterns. The incident underscores growing cybersecurity threats to public institutions and raises pressing questions about data integrity and member trust.

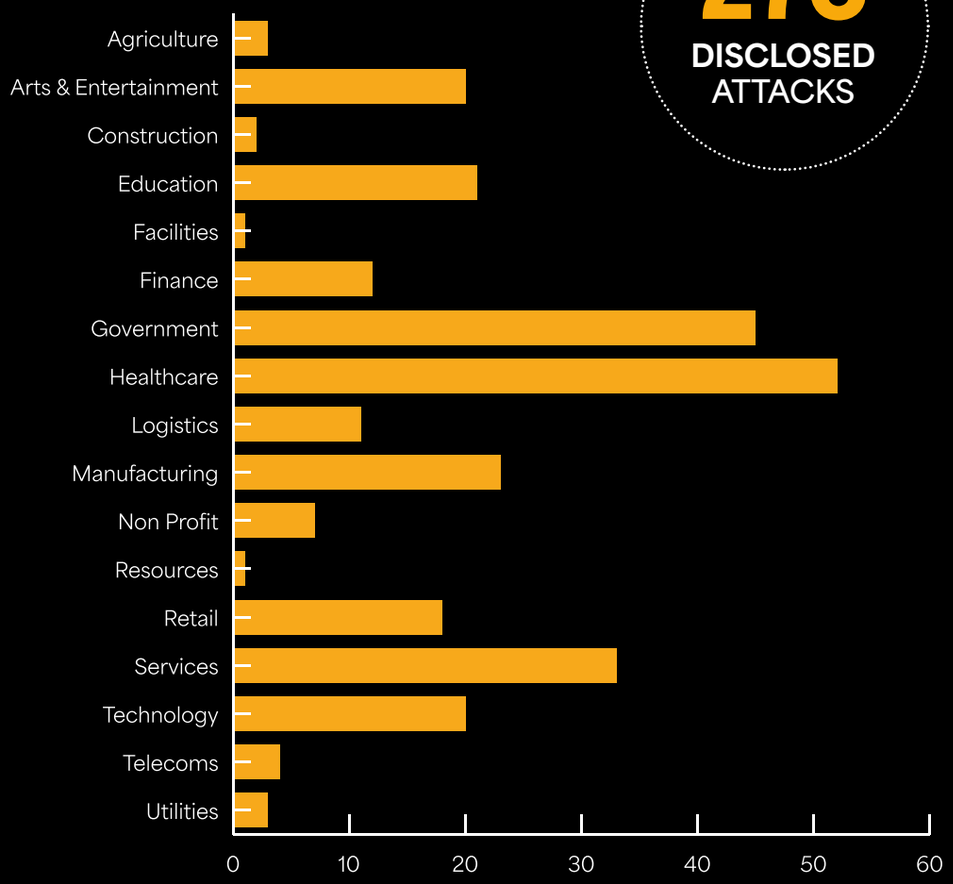
In late May 2025, Kettering Health, a major Ohio-based nonprofit operating 14 hospitals and over 120 outpatient sites, fell victim to a ransomware attack attributed to the **Interlock** gang. The incident forced a system-wide technology shutdown that halted elective procedures, disrupted call centers, and left staff relying on pen-and-paper systems. **Interlock** later claimed responsibility, leaking 941 GB of stolen data, about 732,000 files across 20,000+ folders, including sensitive patient records, employee info, financial documents, and identity scans. Since then, Kettering Health has restored core Epic EHR systems by early June and reinstated key services (surgery, imaging, MyChart portal), although some systems faced lingering limitations. The fallout includes a pending lawsuit alleging patient care disruptions, such as delayed chemotherapy and prescription access, stemming from the breach.

United Natural Foods Inc. (UNFI), the primary distributor for Whole Foods and over 30,000 grocery stores, was hit by a cyberattack detected on June 5, 2025. The company proactively shut down key IT systems to contain the breach, which severely disrupted order processing and outbound deliveries across its 53 distribution centers in the U.S. and Canada. The outage led to notable shortages, particularly in dairy, pantry staples, and frozen items, on supermarket shelves nationwide. UNFI has engaged third-party cybersecurity experts, notified law enforcement, and implemented manual workarounds to keep supply chains moving. No group has claimed responsibility. Recent reports suggest that the incident also spooked investors with UNFI's stock dropping more than 8% in the wake of the announcement.

Q2 | 2025

Disclosed Ransomware Attacks by Industry

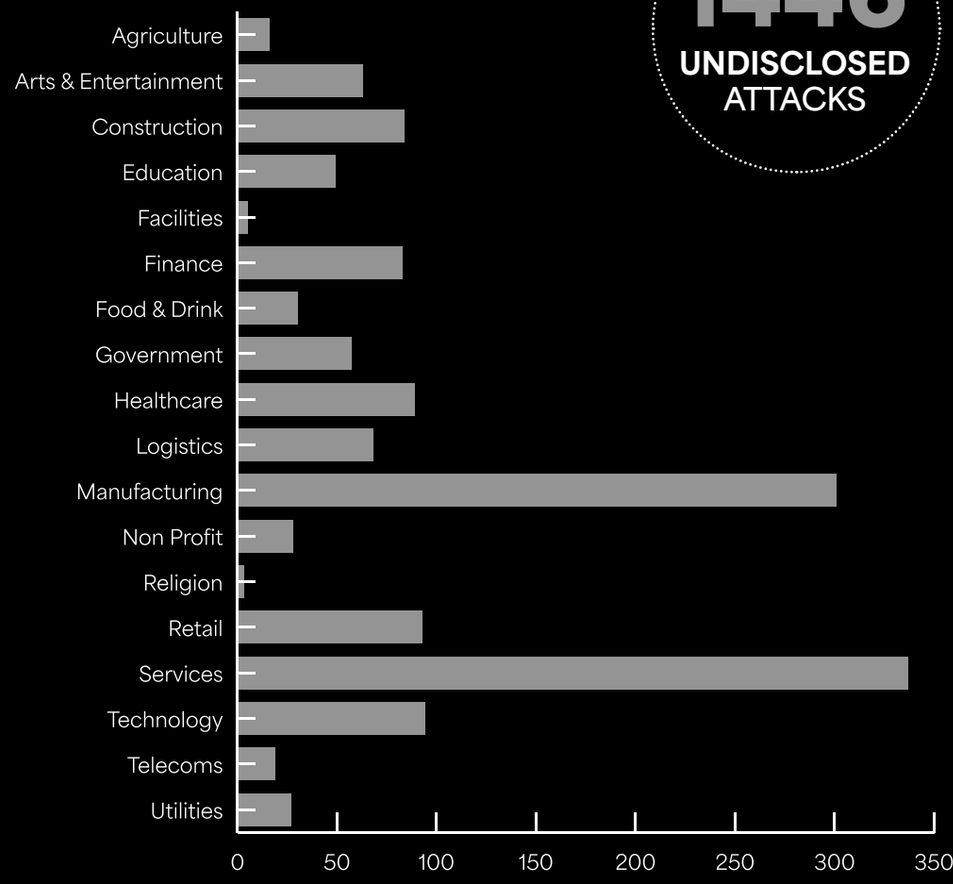
276
DISCLOSED ATTACKS



Q2 | 2025

Undisclosed Ransomware Attacks by Industry

1446
UNDISCLOSED ATTACKS



Retail Sector in the Ransomware Crosshairs

There's no doubt about it; no industry is safe from ransomware. Q2 has seen a sharp uptick in high-profile ransomware attacks across multiple verticals, but retail has clearly taken center stage. Despite not breaking into the top three industries for overall attack volume, publicly disclosed ransomware incidents in the retail sector surged by 58% compared to Q1.

U.K. retailers have borne the brunt of the ransomware assault this quarter. Marks and Spencer, a major high-street staple with over 1,400 stores and 65,000 employees, was forced to shut down automated ordering and stock systems following an attack that could cost the company an estimated £300 million in annual profits. Co-Op and Harrods also suffered attacks in April, highlighting a worrying cluster of breaches within U.K. retail. Beyond direct hits on storefronts, attacks on upstream suppliers, such as United Natural Foods and Peter Green Chilled, have added to the disruption, underscoring the fragility of retail supply chains.

Why Retail Is a Prime Target

Ransomware gangs are increasingly eyeing the retail industry due to its critical dependence on uptime and real-time data. With razor-thin margins and complex logistics, any disruption to inventory management, point-of-sale systems, or supply chains can bring operations to a standstill. The urgency to restore services often translates into a higher likelihood of ransom payment - an attractive incentive for cybercriminals. Additionally, retail companies handle vast troves of customer data and payment information, making them prime targets from both extortion and data theft perspectives.

Scattered Spider's Role in Q2

Scattered Spider has emerged as a notable threat actor in the retail ransomware landscape this quarter. Known for its advanced phishing tactics and social engineering capabilities, the group has been linked to several of the most disruptive campaigns targeting the sector. Their tactics often involve breaching internal systems through credential theft and leveraging legitimate IT management tools to expand their access before deploying ransomware payloads. Their focus on large, recognizable enterprises allows them to maximize both impact and ransom leverage.

High-Profile Brands Under Attack

This quarter has also seen a spate of attacks against high-profile retail brands, further raising the visibility of ransomware threats in this sector. Notable names impacted include Dior, Adidas, Tiffany & Co., Cartier, and Victoria's Secret. These brands typically operate expansive global footprints, meaning even short-term disruptions can cause significant logistical and financial fallout, making them especially attractive to ransomware groups.

Q2 | 2025
Top 3 Targeted Countries

DISCLOSED

01 U.S.A 150 54%

02 AU.S. 25 9%

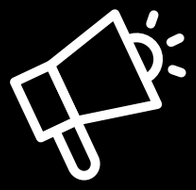
03 U.K. 16 6%

UNDISCLOSED

01 713 49% U.S.A

02 81 6% CAN

03 64 4% GER



In the News

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

How banks can fight the rising tide of data breaches in 2025

Banks are facing a growing threat from cyberattacks in 2025, driven by deeper digital integration and sprawling vendor networks. Malware remains the top attack type since 2021, with phishing rising rapidly, now ranking as the second-fastest growing method after ransomware. Hacktivists, those driven by political or social agendas, are identified as the primary external threat this year.

Our CEO warns that the barrier to entry for launching sophisticated cyberattacks has dropped significantly. "The barrier to entry has dropped, and a single actor with the right tools can now launch sophisticated campaigns that once required an entire team," he comments. There is an urgent need for enhanced threat intelligence sharing, stronger governance to oversee cyber risks, and proactive investments in cloud-based security solutions. Only by combining advanced technology with strategic oversight can banks hope to stay ahead of these evolving cyberthreats.

What would you do if you found your email address listed on the dark web?

That's exactly the situation PCMag journalist Kim Key faced. After a dark web monitoring tool flagged her email, she went down the rabbit hole, digging through years of digital history to uncover where the breach originated. Her investigation pointed to a company she hadn't interacted with in over ten years, highlighting how long-forgotten accounts can come back to haunt you.

The article explores how data ends up on the dark web and the hidden risks behind every day online behavior, from signing up for newsletters to answering online quizzes. It also features practical advice from cybersecurity experts, including our CEO Darren Williams, who notes that "everybody on planet Earth has had their data leaked at this point." The advice urges users to limit how much real information they share, embrace privacy tools like password managers and data removal services, and stay alert to avoid becoming easy targets for cybercriminals.

AI is rewriting the ransomware playbook - can businesses keep up?

AI is transforming ransomware, making attacks faster, more targeted, and harder to stop. Even small groups like **FunkSec** have used generative AI to craft convincing phishing emails, create malware, and automate ransom chats, allowing them to hit over 80 victims in a month. AI also enables polymorphic malware, which constantly changes to dodge traditional defenses.

Our CEO Darren Williams says the only way to counter this is to "fight AI with AI." That means using real-time behavioral monitoring, AI-driven detection, and anti data exfiltration tools. He also stresses the basics still matter: patch quickly, use MFA, apply Zero Trust, and limit user access.

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 April - June 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

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