Q2 2026 | RANSOMWARE TRENDS REPORT

Beneath The Surface: Why Stable Attack Numbers Hide A Rapidly Escalating Data Theft Crisis

Welcome to BlackFog's Q2 2026 Ransomware Trend Report. This quarter's report examines the latest ransomware activity across publicly disclosed incidents and attacks identified on dark web leak sites, providing a comprehensive view of the evolving threat landscape. From emerging threat groups and sector-specific targeting to new techniques for data theft and extortion, we analyze the trends shaping ransomware today. As always, the report combines BlackFog's independent ransomware research with practical insights to help security teams understand where attackers are focusing their efforts and how organizations can better protect their data.

DISCLOSED ATTACKS

The New Normal: Stable Numbers, Escalating Risk

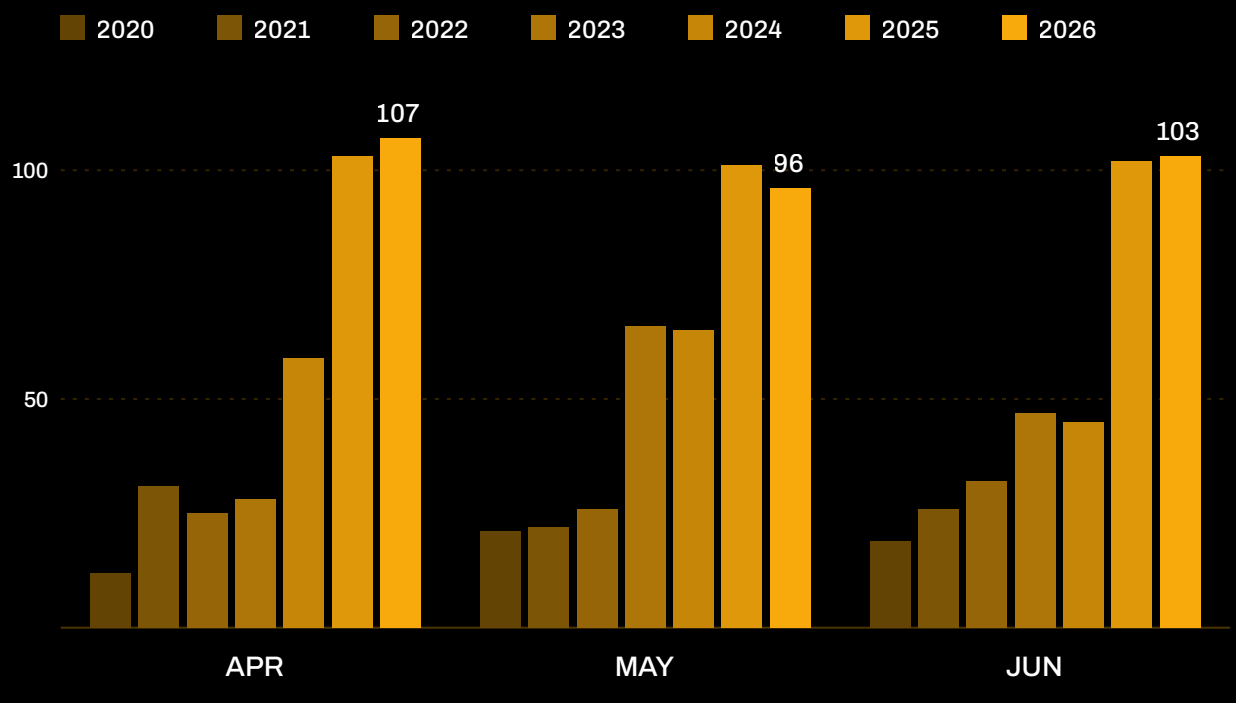
BlackFog tracked 306 publicly disclosed ransomware attacks during Q2 2026, covering April through June. Monthly activity remained remarkably consistent, with 107 attacks in April, 96 in May, and 103 in June, resulting in a quarterly total identical to Q2 2025. While the overall volume remained unchanged, the ransomware landscape did not. New ransomware variants, evolving attack methods, and shifting victim profiles continue to reshape the threat, even as disclosed attack numbers remain stable.

Healthcare remained the most targeted industry, accounting for more than one in four disclosed ransomware attacks (81 incidents, 26%). Services ranked second with 45 attacks (15%), followed by government with 30 attacks (10%). Technology and education rounded out the top five. Healthcare's continued prominence reflects both its attractiveness to attackers and the sector's stringent regulatory reporting obligations. Mandatory breach notification requirements ensure healthcare incidents are more likely to become public than attacks against organizations in less regulated industries, making the sector an important barometer for disclosed ransomware activity.

Attribution remains one of the industry's greatest challenges. 30% of all disclosed attacks (93 incidents) could not be linked to a known ransomware group, underscoring the growing difficulty of accurately identifying threat actors. In fact, unidentified actors accounted for more incidents than

Q2 · 2020–2026

Disclosed attacks by month

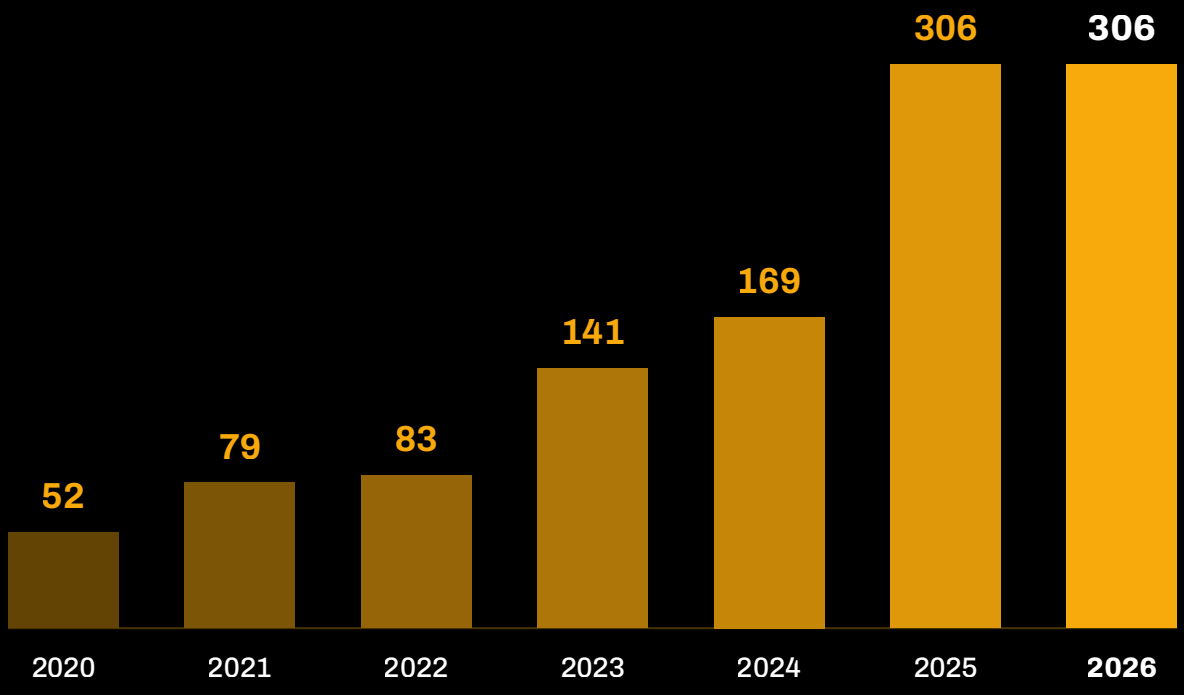


April 2026 was the busiest month on record for Q2 disclosures (107 attacks). White values mark 2026.

Q2 · YEAR OVER YEAR

Disclosed ransomware attacks

306
0% YoY



Attack volume held flat at 306 (0% YoY) after five consecutive years of growth.

any single named ransomware group. Of the attacks that could be attributed, Shiny Hunters led with 28 incidents, followed by Qilin (19), INC (13), and Safepay (11). In total, 57 ransomware groups were associated with disclosed attacks during Q2, a 21% increase over Q1, highlighting an increasingly fragmented ransomware ecosystem with new ransomware groups emerging at a rapid pace.

The United States remained the primary target, accounting for 169 disclosed attacks (55%). Australia ranked second with 54 incidents (18%), a disproportionately high figure that reflects the country's robust mandatory breach disclosure requirements. As with healthcare, stronger reporting obligations make Australian ransomware incidents significantly more likely to become public than attacks in jurisdictions with less stringent disclosure laws. Germany, India, and the United Kingdom followed well behind, together representing less than 7% of disclosed attacks.

BlackFog confirmed data exfiltration in 97% of all disclosed ransomware attacks, the highest rate ever recorded. Data theft is no longer a secondary tactic. It is now the primary objective of modern ransomware operations. As organizations improve their ability to recover encrypted systems, threat actors have shifted their leverage to what organizations cannot easily recover: stolen data. Extortion today is driven less by encryption and more by the threat of public exposure, regulatory penalties, and reputational damage.

Q2 2026 · DISCLOSED ATTACKS

Did you know?

$25M

HIGHEST RANSOM DEMAND

Demanded in the Novo Nordisk attack, claimed by FulcrumSec.

97%

INVOLVED DATA EXFILTRATION

The highest rate ever recorded.

57

RANSOMWARE VARIANTS

Associated with disclosed attacks, up 21% vs Q1.

12

ORGANIZATIONS HIT BY "2019"

Every disclosed victim was based in Australia.

+221%

SERVICES SECTOR VS Q1

The steepest sector rise in disclosed attacks this quarter.

Figures cover disclosed ransomware attacks recorded April–June 2026.

UNDISCLOSED ATTACKS

The Invisible Majority

BlackFog identified 2,027 undisclosed ransomware attacks during Q2 2026 through continuous monitoring of ransomware leak sites. Compared to just 306 publicly disclosed incidents, this means that for every ransomware attack that became public, more than six others remained undisclosed. The disparity underscores the vast gap between reported incidents and the true scale of ransomware activity.

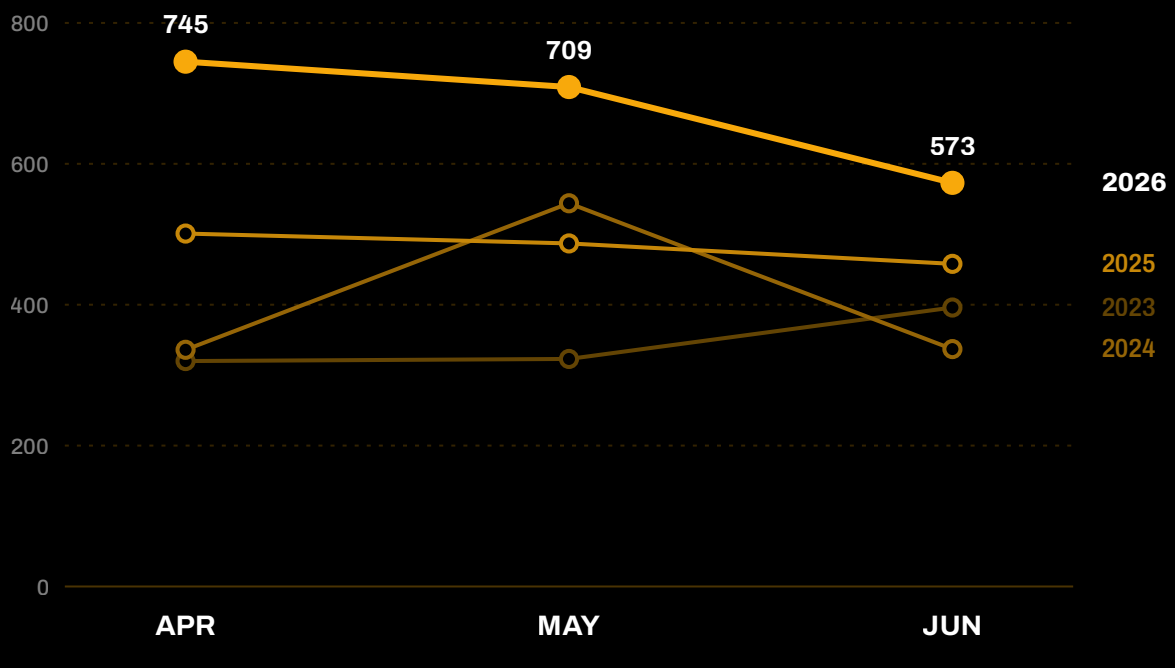
Monthly activity remained consistently high throughout the quarter, with 745 attacks in April, 709 in May, and 573 in June. Despite the decline toward the end of the quarter, overall activity increased significantly year over year, rising from 1,446 attacks in Q2 2025 to 2,027 in Q2 2026, a 40% increase.

The industry landscape differed considerably from the disclosed data. Services was the most targeted industry, accounting for 509 attacks (25%), followed by Manufacturing with 422 attacks (21%). Technology, Healthcare, Construction, Finance, and Retail formed a closely grouped second tier, each accounting for between 7% and 9% of activity.

Unlike the disclosed data, where Healthcare dominated due in part to mandatory reporting requirements, the undisclosed dataset provides a broader view of ransomware targeting across industries. The contrast reinforces an important point: sectors with fewer disclosure obligations remain significantly underrepresented in public ransomware reporting.

Q2 · 2023–2026

Undisclosed attacks by month

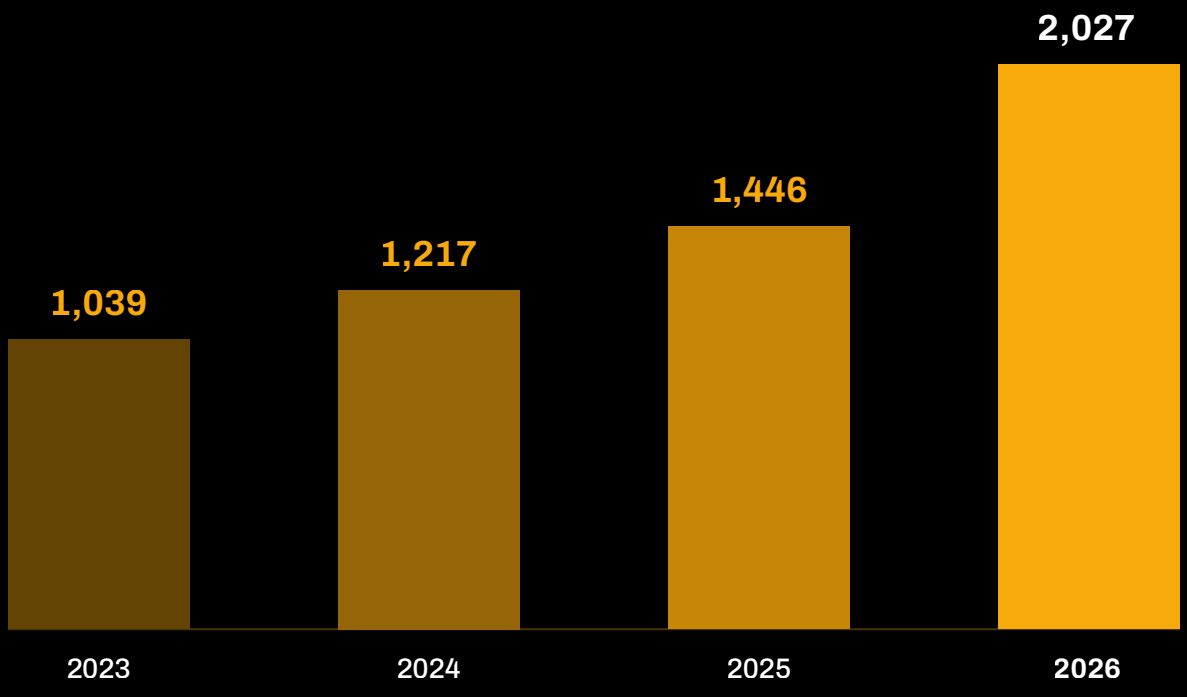


2026 volumes ran well above every prior year in each month, easing from April's peak of 745.

Q2 · YEAR OVER YEAR

Undisclosed ransomware attacks

+40%
2,027 attacks



Undisclosed activity identified on dark web leak sites surged 40% YoY, the sharpest rise since tracking began in 2023.

Ransomware activity remained highly fragmented throughout Q2. Qilin was the most active group, claiming 285 attacks, followed by The Gentlemen (219), DragonForce (137), and Akira (120). In total, 93 ransomware groups were active during the quarter, including 28 new groups that emerged during Q2, twice as many as in Q1. The continued emergence of new ransomware groups, combined with the large number of active groups, highlights how resilient and decentralized the ransomware ecosystem has become. As established operations are disrupted, new groups continue to emerge, ensuring the overall threat remains persistent.

The United States remained the most targeted country, accounting for 855 attacks (42%). While still representing the largest share of global activity, this is notably lower than the 55% observed in disclosed attacks, illustrating the broader geographic distribution of ransomware activity captured through leak site monitoring. Germany, the United Kingdom, and Canada followed, each accounting for approximately 4% to 5% of attacks.

Taken together, the undisclosed data provides a more complete picture of today's ransomware landscape than public reporting alone. While disclosed attacks remain essential for understanding the impact on victims, leak site intelligence reveals the true scale, diversity, and persistence of ransomware activity. The gap between disclosed and undisclosed incidents continues to widen, reinforcing the need for organizations to focus not only on recovery, but on preventing the data theft that fuels modern ransomware operations.

Q2 2026 · UNDISCLOSED ATTACKS

Did you know?

$496,384

AVERAGE RANSOM DEMAND

Across undisclosed attacks recorded in Q2 2026.

508.48 GB

AVERAGE DATA EXFILTRATED

Per victim, identified via dark web leak sites.

98

COUNTRIES AFFECTED

Organizations suffered attacks worldwide in Q2.

28

NEW RANSOMWARE GROUPS

Emerged during Q2, twice as many as Q1.

7 days

AVERAGE PAYMENT DEADLINE

Given to victims before stolen data is published.

Figures cover undisclosed ransomware attacks recorded April–June 2026.

EMERGING THREAT

Settra's Rapid Rise

Settra was first observed in June 2026 and quickly became one of the quarter's most active new ransomware groups. Within the final four days of Q2, it claimed 22 victims, more than any other newly identified group during the quarter.

What makes Settra particularly notable is not only the speed of its emergence, but also the breadth of its operations. Rather than concentrating on a single country or region, the group targeted organizations across seven countries within its first four days of activity, including the United States, France, Portugal, Singapore, South Korea, Taiwan, and the United Kingdom. This level of geographic reach is unusual for a newly observed ransomware operation and suggests the group entered the landscape with a high degree of operational maturity.

Settra's victims also reflect a broad targeting strategy. The median victim employed 97 people, consistent with the small and mid-sized organizations frequently targeted by ransomware groups. At the same time, Settra claimed responsibility for an attack on Doosan Corporation, a South Korean industrial conglomerate with approximately 43,000 employees, reporting the theft of 3.2 TB of data. The combination of smaller organizations and large enterprise targets suggests a group willing to pursue opportunities across a wide range of victim profiles rather than focusing on a single industry or organization size.

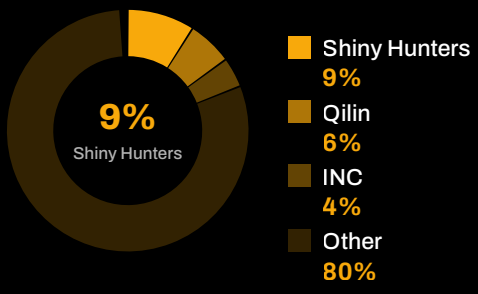
The group's activity also evolved rapidly. The first 11 victims, published on June 27, included reported data volumes and supporting proof of compromise across six countries. A second wave of 11 victims, published on June 30, consisted primarily of U.S. organizations and did not yet include supporting evidence. This pattern is consistent with an active leak site where claims are published first and supporting evidence follows as negotiations progress. Overall, 50% of Settra's listed victims already included proof of compromise, a level more commonly associated with established ransomware operations than newly emerging groups.

Although Settra's activity was limited to the final four days of Q2, its rapid growth, international reach, and apparent operational maturity distinguish it from most newly observed ransomware groups. Whether this pace continues into Q3 remains to be seen, but Settra has already established itself as one of the most closely watched emerging ransomware threats.

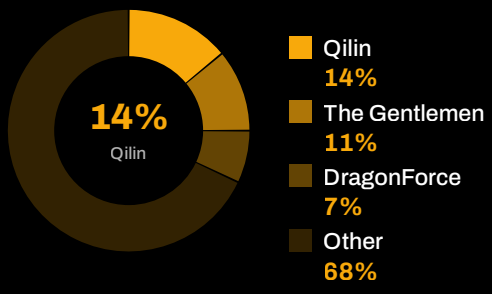
Q2 2026 · SHARE OF ATTACKS

Most active variants

DISCLOSED



UNDISCLOSED



94 ransomware groups claimed victims in Q2 2026. The landscape remains highly fragmented.

QUARTER IN FOCUS

Five Attacks That Shaped the Quarter

LOS ANGELES POLICE DEPARTMENT (WORLDLEAKS) | APRIL 2026

Rather than targeting the Los Angeles Police Department directly, WorldLeaks compromised a third-party file-sharing system operated by the Los Angeles City Attorney's Office, exposing approximately 7.7 TB of sensitive data. The leak included officer disciplinary records, internal affairs investigations, and legal documents related to ongoing civil litigation. The incident demonstrates how third-party systems can expose highly sensitive law enforcement information, even when the intended target's own network remains uncompromised.

> **KEY TAKEAWAY:** THIRD-PARTY EXPOSURE CONTINUES TO CREATE SIGNIFICANT ORGANIZATIONAL RISK, PARTICULARLY WHERE HIGHLY SENSITIVE INFORMATION IS SHARED ACROSS AGENCIES.

THE SHINY HUNTERS RETAIL CAMPAIGN | APRIL 2026

Within the space of a single week, Shiny Hunters compromised multiple well-known retail brands by exploiting vulnerabilities across shared cloud platforms. Victims included Zara, 7-Eleven, Ralph Lauren, Carnival Corporation, Hallmark Cards, and Pitney Bowes, among others. Zara and Ralph Lauren were linked to a compromised Anodot analytics integration connected to Snowflake, while 7-Eleven's exposure originated through its Salesforce environment. After negotiations failed, Shiny Hunters leaked the stolen 7-Eleven data and separately offered approximately 600,000 records for sale on a hacking forum.

> **KEY TAKEAWAY:** A SINGLE COMPROMISE OF A SHARED SAAS PLATFORM CAN EXPOSE MULTIPLE ORGANIZATIONS SIMULTANEOUSLY, DEMONSTRATING HOW VENDOR CONCENTRATION CONTINUES TO AMPLIFY RANSOMWARE RISK ACROSS ENTIRE INDUSTRIES.

CANVAS (SHINY HUNTERS) | APRIL-MAY 2026

The attack on Canvas, Instructure's learning management platform, was one of the quarter's most significant ransomware incidents. By exploiting weaknesses in the platform's Free-for-Teacher environment, Shiny Hunters claimed to have accessed approximately 275 million records affecting nearly 9,000 educational institutions worldwide. The campaign escalated when attackers replaced Canvas login pages with ransom messages during university finals, disrupting teaching at several major institutions. Instructure later confirmed it had reached an agreement with the attackers to remove the stolen data.

> **KEY TAKEAWAY:** A SINGLE COMPROMISE OF A WIDELY ADOPTED CLOUD PLATFORM CAN EXPOSE THOUSANDS OF ORGANIZATIONS SIMULTANEOUSLY, REINFORCING THE GROWING RISK POSED BY VENDOR CONCENTRATION.

FOXCONN (NITROGEN) | MAY 2026

Nitrogen claimed responsibility for an attack against Foxconn, the world's largest contract electronics manufacturer, alleging the theft of approximately 8 TB of data across 11 million files. The group claimed the stolen information included engineering documentation and intellectual property associated with several global technology companies, highlighting the far-reaching consequences of attacks against critical manufacturing suppliers.

> **KEY TAKEAWAY:** SUPPLY CHAIN ATTACKS CONTINUE TO EXPAND THE IMPACT OF RANSOMWARE FAR BEYOND THE INITIAL VICTIM, PLACING CUSTOMERS, PARTNERS, AND INTELLECTUAL PROPERTY AT RISK.

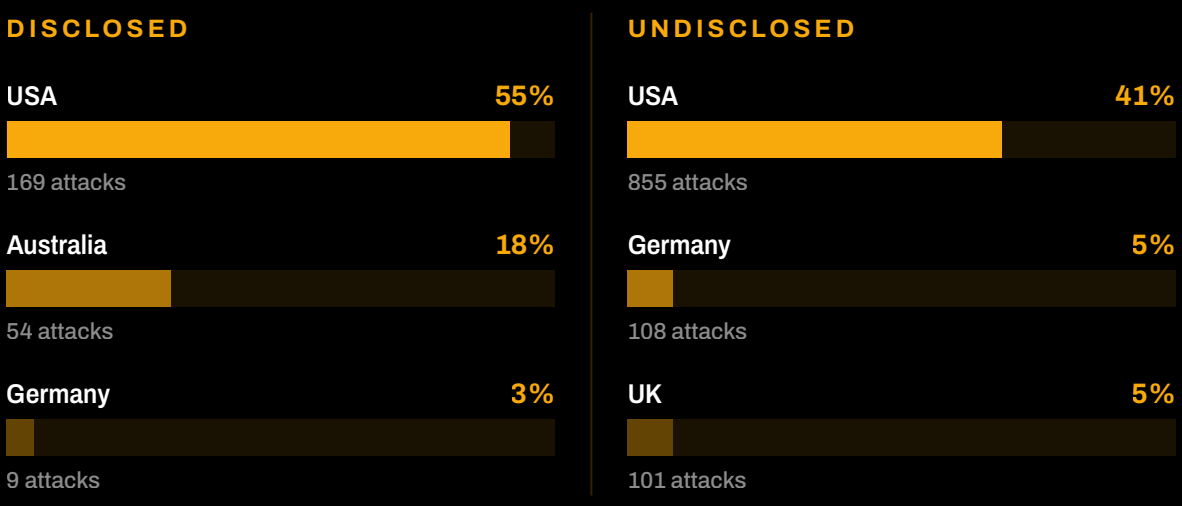
NOVO NORDISK (FULCRUMSEC) | JUNE 2026

The attack on Novo Nordisk featured the largest publicly disclosed ransom demand of the quarter, with FulcrumSec demanding $25 million after claiming to have spent more than two months inside the company's network. The group claimed it had exfiltrated approximately 1.3 TB of sensitive information, including clinical research data, manufacturing information, and proprietary AI assets.

> **KEY TAKEAWAY:** MODERN RANSOMWARE GROUPS ARE INCREASINGLY TARGETING INTELLECTUAL PROPERTY AND AI ASSETS ALONGSIDE TRADITIONAL SENSITIVE DATA, SIGNIFICANTLY RAISING THE STAKES FOR ORGANIZATIONS OPERATING IN RESEARCH-INTENSIVE INDUSTRIES.

Q2 2026 · TOP THREE, DISCLOSED VS UNDISCLOSED

Attacks by country

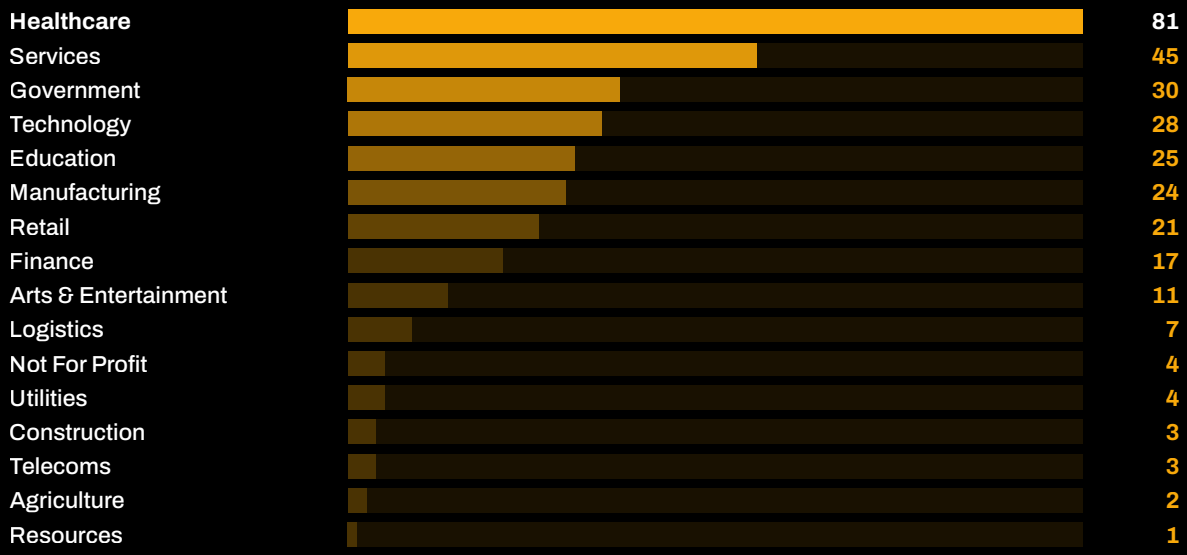


The US dominates both datasets. Bars are scaled to share of total.

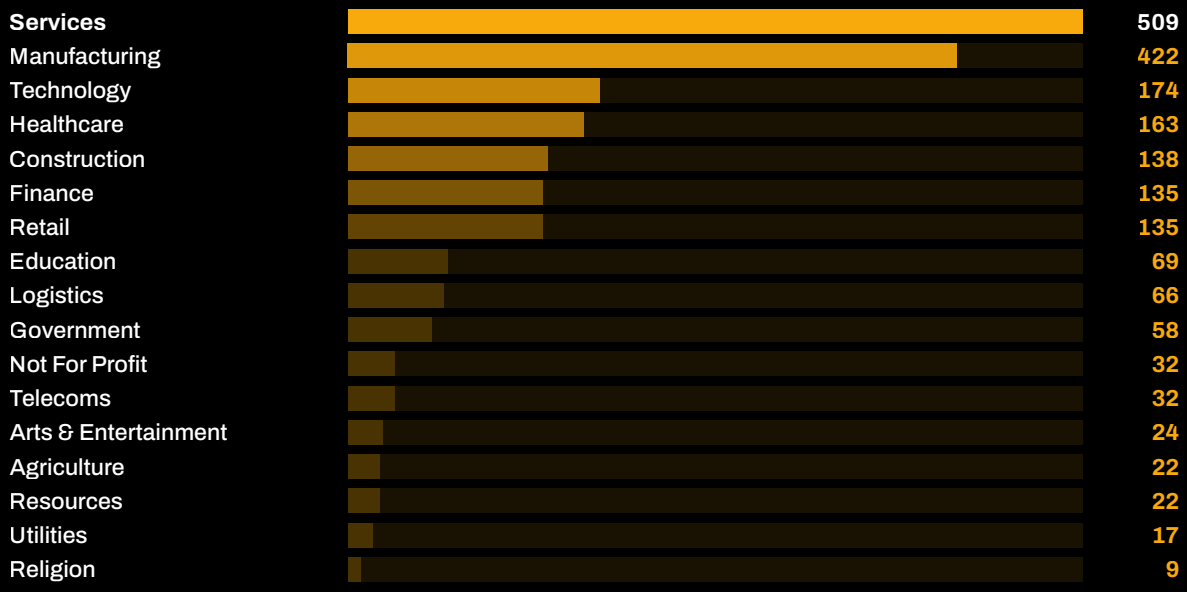
Q2 2026 · ATTACKS BY SECTOR

Attacks by industry

DISCLOSED · 306 ATTACKS



UNDISCLOSED · 2,027 ATTACKS



Healthcare leads disclosed attacks (26%);
services and manufacturing dominate undisclosed activity (46% combined).

AI ATTACK SURFACE

The New Exfiltration Economy

Throughout this report, one theme has remained consistent: modern ransomware is no longer defined by encryption alone. Data theft has become the primary objective, providing attackers with the leverage to extort victims even when systems can be restored. That evolution extends well beyond traditional ransomware. During Q2, BlackFog researchers identified several emerging techniques that use AI platforms, enterprise knowledge bases, and advanced information stealers to quietly extract sensitive corporate data. Together, these developments demonstrate how data exfiltration continues to evolve beyond conventional ransomware operations.

CAMOLEAK

BlackFog researchers uncovered CamoLeak, a novel attack technique that turns trusted AI coding assistants into covert data exfiltration channels. By combining prompt injection with GitHub's image proxy infrastructure, researchers demonstrated how GitHub Copilot could be manipulated into leaking sensitive information from private code repositories without triggering traditional security controls. The research highlights a growing challenge for organizations adopting AI development tools: trusted AI applications can unintentionally become trusted pathways for data theft.

RAG POISONING

As organizations increasingly deploy Retrieval-Augmented Generation (RAG) systems, attackers are shifting their focus from endpoints to the knowledge repositories that power enterprise AI. BlackFog demonstrated how poisoned documents and hidden prompts can manipulate AI responses, bypass safeguards, and expose sensitive corporate information through otherwise legitimate interactions. Unlike traditional attacks, RAG poisoning requires no malware and leaves few conventional indicators of compromise, making it particularly difficult to detect using existing security controls.

As enterprise AI adoption accelerates, organizations must begin treating AI applications and their underlying knowledge bases as potential data exfiltration pathways rather than simply productivity tools.

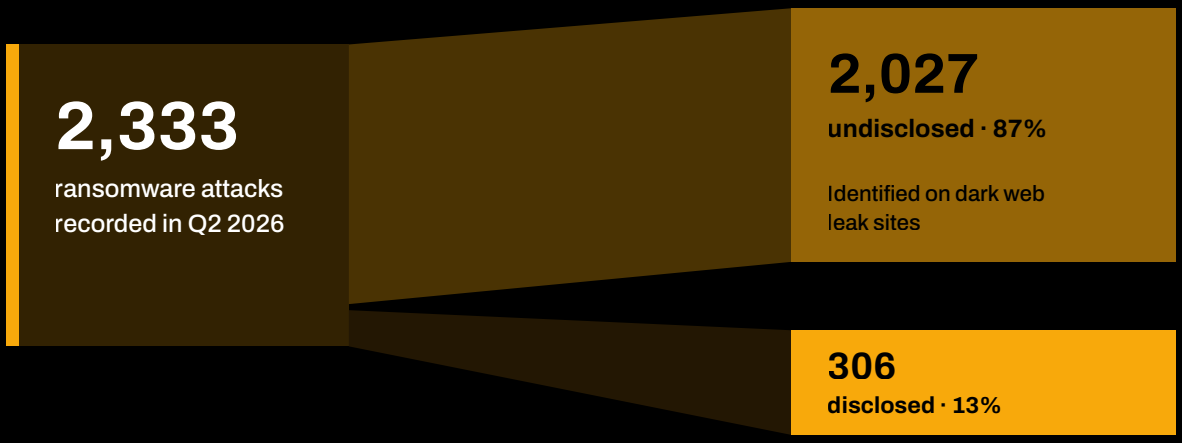
ONYXC2: INDUSTRIALIZING DATA THEFT

While AI introduces new opportunities for data theft, credential stealers continue to evolve just as rapidly. OnyxC2 represents a new generation of information-stealing malware designed to harvest credentials and sensitive data from more than 210 applications, including browsers, password managers, VPNs, messaging platforms, cryptocurrency wallets, and email clients. Rather than encrypting systems, its objective is to quietly collect the information that enables follow-on attacks, including ransomware, business email compromise, and account takeover.

The emergence of OnyxC2 reflects the growing professionalization of the cybercriminal ecosystem. Information stealers are increasingly being marketed as commercial services, lowering the barrier to entry for attackers. As these capabilities become more accessible, the theft and resale of corporate credentials and sensitive information continues to accelerate. Data theft is increasingly occurring before ransomware is ever deployed, making data exfiltration prevention a critical layer of modern cyber defense.

Q2 2026 · DISCLOSED VS UNDISCLOSED

The visibility gap



Only 1 in 8 ransomware attacks becomes publicly disclosed.

Public disclosures capture a fraction of real activity, the majority surfaces only through leak-site monitoring.

CONCLUSION

What Comes Next

Q2 2026 confirmed that ransomware continues to evolve, even when the headline numbers appear stable. While publicly disclosed attacks remained unchanged from a year ago, BlackFog's research revealed a far more dynamic threat landscape. Undisclosed attacks continued to rise, new ransomware groups emerged at an accelerating pace, and data exfiltration reached its highest level ever recorded in publicly disclosed incidents. Together, these trends demonstrate that modern ransomware is increasingly driven by the theft and exploitation of data rather than encryption alone.

The quarter also underscored how rapidly the attack surface is expanding. From trusted SaaS platforms and global supply chains to AI assistants, enterprise knowledge bases, and advanced information stealers, attackers are finding new ways to access sensitive information and use it for extortion. As organizations embrace new technologies and increasingly interconnected ecosystems, preventing unauthorized data movement has become just as important as protecting the systems that store it.

The message is clear: recovery is no longer enough. Organizations must focus on preventing data exfiltration before it occurs, reducing attackers' ability to monetize stolen information and limiting the impact of both ransomware and the next generation of cyberthreats. Those that prioritize data protection at the point of exit will be best positioned to stay ahead of an increasingly sophisticated and data-driven threat landscape.

BLACKFOG TRACKS

About the data

BlackFog has tracked and analyzed global ransomware activity since 2020 through its award-winning State of Ransomware research, providing ongoing insight into the evolution of the threat landscape. Our research combines publicly disclosed ransomware incidents with independent analysis to identify emerging trends, threat actors, industry targeting, and changes in attacker tactics.

Recognizing that many ransomware attacks are never publicly reported, BlackFog expanded its research in 2023 to include incidents disclosed on dark web leak sites operated by ransomware groups. This broader methodology captures both publicly acknowledged attacks and those that remain undisclosed by victims, providing a more comprehensive view of global ransomware activity and the growing role of data extortion in modern cybercrime.

The data presented in this report is compiled from a combination of publicly available sources, ransomware group leak sites, open-source intelligence, and BlackFog's ongoing threat research. Incidents are validated, categorized, and analyzed to identify meaningful trends across industries, regions, organization size, and ransomware operators.

While every effort is made to verify the accuracy of reported incidents, ransomware remains an evolving threat, and some attacks may never become public or be claimed by threat actors. As a result, the figures presented should be viewed as a conservative representation of overall ransomware activity rather than a complete count of every attack.

ABOUT BLACKFOG

Real-Time, On-Device, Data Exfiltration Prevention

BlackFog helps organizations reduce modern cyber risk by stopping data exfiltration, the common factor behind ransomware, insider threats, zero-day attacks, and Shadow AI exposure. Our anti data exfiltration (ADX) platform delivers real-time, on-device prevention. It stops sensitive data from leaving endpoints and networks without authorization and blocks ransomware communication, data theft, and AI driven leakage before damage occurs. By focusing on prevention instead of just detection, BlackFog helps organizations strengthen compliance, protect privacy, and improve operational resilience.

Contact us for a demo

blackfog.com/contact

Start your free trial

14-day assessment

Visit blackfog.com

Explore the platform