BLACKFOG.COM

BLACKFOG®

The State of Ransomware

2025 ANNUAL REPORT

“In this 2025 annual report, we examine the continued escalation in both the frequency and severity of ransomware threats. The report highlights key findings from 2025, compares them with trends from previous years, and uncovers critical shifts in the cybersecurity landscape, including a spotlight on how the use of AI in cybersecurity has evolved.”

Contents

Dr. Darren Williams,
Founder and CEO,
BlackFog Inc.

1

Foreword

Ransomware has evolved into a data-driven, AI enabled threat that no longer relies on disruption alone to succeed. In 2025, attackers overwhelmingly focused on stealing sensitive information to drive extortion, using automation and artificial intelligence to move faster, scale operations, and evade traditional defenses.

At the same time, organizations rapidly adopted AI to improve productivity and efficiency, often without sufficient visibility or governance. This rise of Shadow AI has quietly expanded the attack surface, creating new pathways for data exposure that many security teams are not yet equipped to control.

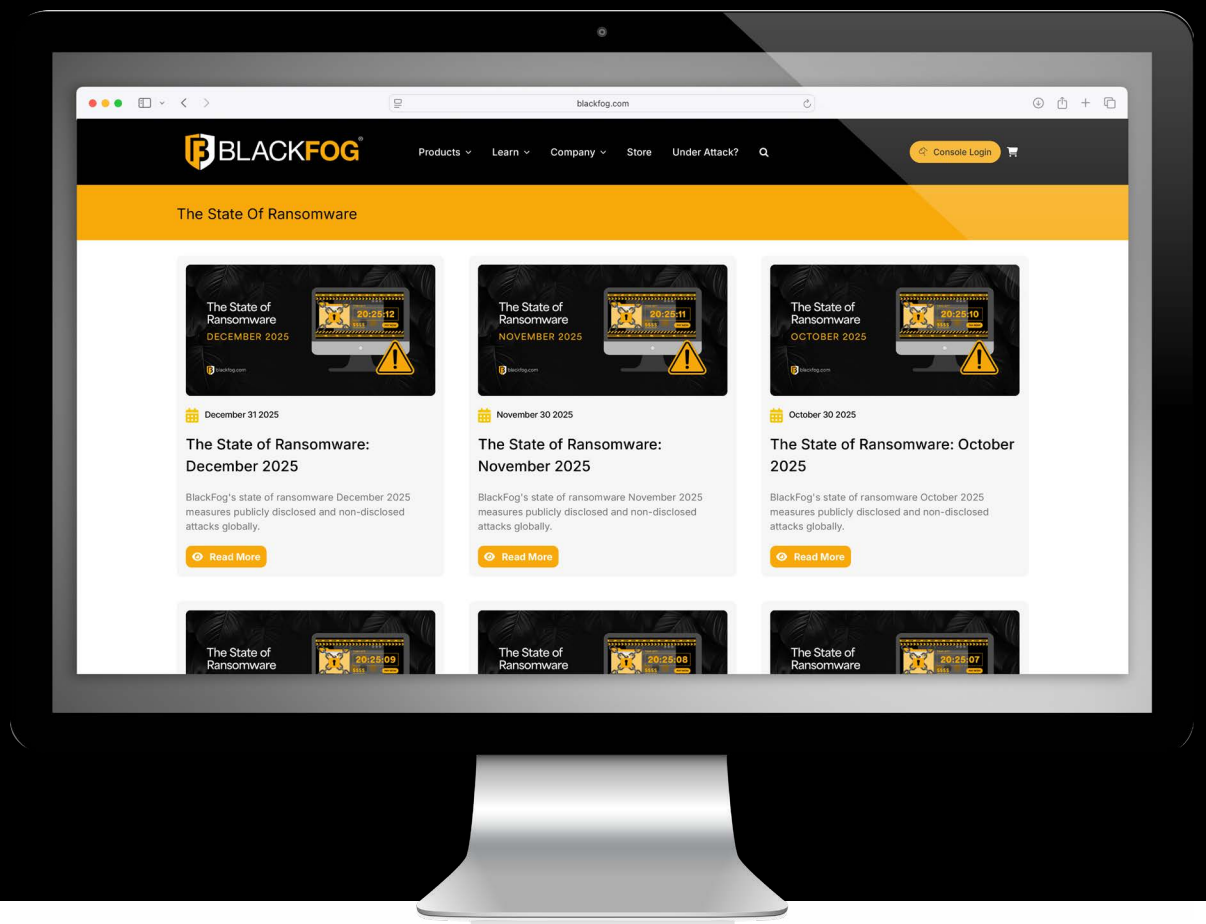
The findings in this **State Of Ransomware 2025 Annual Report** highlight a clear shift in the threat landscape. Ransomware, insider misuse, supply-chain compromise, and AI driven attacks are no longer separate challenges. They all converge on a single risk: loss of control over data.

As we move into 2026, security strategies must evolve accordingly. Detection and recovery remain important, but they are no longer enough. Organizations must prioritize real-time prevention of data exfiltration, close AI related blind spots, and adopt prevention-first approaches that stop attackers before extortion becomes possible.

It is my hope that this report provides both clarity and direction as organizations prepare for the next phase of the ransomware threat.

View our latest monthly **State Of Ransomware** Blogs.

CLICK HERE



2

Introduction

Since 2020, BlackFog has been tracking and documenting publicly disclosed ransomware attacks through its award-winning State Of Ransomware blog.

Recognized as a trusted industry resource, the blog is frequently cited by leading news outlets including the Associated Press, Yahoo, Forbes, and Dark Reading, among others. In addition, BlackFog publishes a quarterly Ransomware Trend Report, distributed to thousands of subscribers worldwide.

In 2023, we expanded the scope of our reporting to include undisclosed ransomware attacks identified on data leak sites and across the dark web. This enhancement has enabled us to deliver a more comprehensive and accurate view of the global ransomware landscape.

In this 2025 Annual Report, we examine the continued escalation in both the frequency and severity of ransomware threats.

The report highlights key findings from 2025, compares them with trends from previous years, and uncovers critical shifts in the cybersecurity landscape, including a spotlight on how the use of AI in cybersecurity has evolved. Most importantly, it provides actionable recommendations to help organizations strengthen their defenses and better protect themselves against these rapidly evolving threats.

3

Disclosed Ransomware Attacks Reach Record Levels As Activity Accelerates In 2025

Ransomware remained a dominant cybersecurity threat throughout 2025, with publicly disclosed attacks reaching a record high of 1,174 incidents, a 49% increase compared to 2024. Every quarter recorded notable year-on-year growth, with Q2 experiencing the sharpest rise at 81%, underscoring the sustained acceleration of ransomware activity.

For the first time since BlackFog began tracking ransomware in 2020, monthly disclosed attacks exceeded 100 incidents, a threshold crossed seven times during the year. March recorded the highest total with 117 attacks, while December, the lowest month, still reported 80 incidents. Notably, this lowest monthly figure in 2025 was among the highest monthly totals recorded in 2024, reinforcing

DID YOU KNOW?

Organizations across **76 countries** publicly reported ransomware attacks.

The **average workforce size** of organizations that publicly disclosed a ransomware attack was **10,757 employees**.

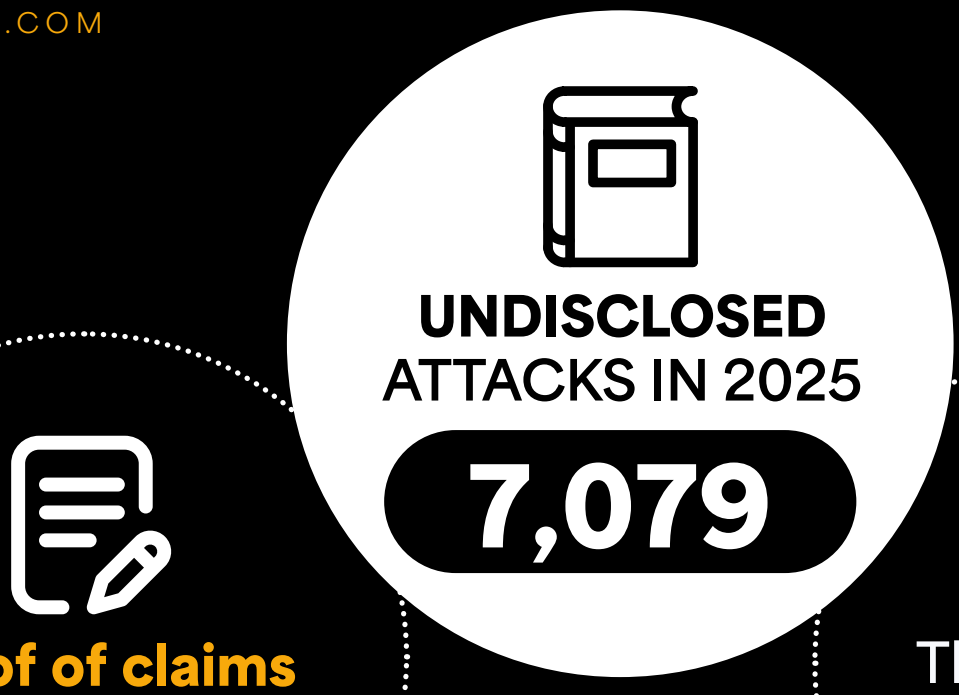
The **retail sector** saw increased targeting and heightened media attention in 2025, with **high-profile attacks** affecting brands such as M&S, Cartier, Chanel, and other luxury retailers and fashion houses.

that ransomware activity continues to intensify rather than slow.

The healthcare sector was once again the most targeted vertical, accounting for 22% of all disclosed ransomware attacks in 2025. Nearly all sectors experienced increased attack volumes, with the services industry more than doubling year-on-year, recording a 118% increase. Education was the only sector to see a decline, with attacks decreasing by approximately 12%.

In total, 102 distinct ransomware groups were linked to publicly disclosed attacks during the year, with **Qilin** emerging as the most active group, claiming 99 incidents. However, the top three ransomware groups collectively accounted for just 18% of all attacks, reflecting the increasingly crowded ransomware landscape. At the time of writing, 31% of disclosed incidents have not yet been attributed to a ransomware group.

Data exfiltration remained the dominant tactic, with 96% of all disclosed ransomware attacks involving data theft, the highest rate recorded to date, further cementing it as a core technique used by cybercriminals.



4

Ransomware Beneath The Surface: 86% Of Attacks Went Undisclosed In 2025

Undisclosed ransomware activity continued to rise sharply in 2025, with 7,079 victims announced by ransomware groups on dark web leak sites, representing a 37% increase compared to 2024.

These figures indicate that approximately 86% of ransomware attacks are never publicly reported. Put into context, for every 100 ransomware attacks that go undisclosed, only around 17 are publicly disclosed.

Activity remained elevated throughout the year, with Q1 recording the highest volume at 2,125 attacks, followed closely by Q4 with 1,998 incidents. All four quarters reported increases compared to previous years. March proved particularly active, with 800 organizations targeted, a figure 35% higher than any month recorded in 2024.

Qilin was the most active ransomware group in 2025, claiming 1,016 victims on the dark web. **Akira** and **Play** rounded out the top three, with 732

DID YOU KNOW?

The highest ransom demand recorded in 2025 was **$91 million**, issued by **DEVMAN** in an attack against Shimao Group.

Organizations in **135 countries** were targeted, with several smaller nations experiencing particularly disruptive attacks.

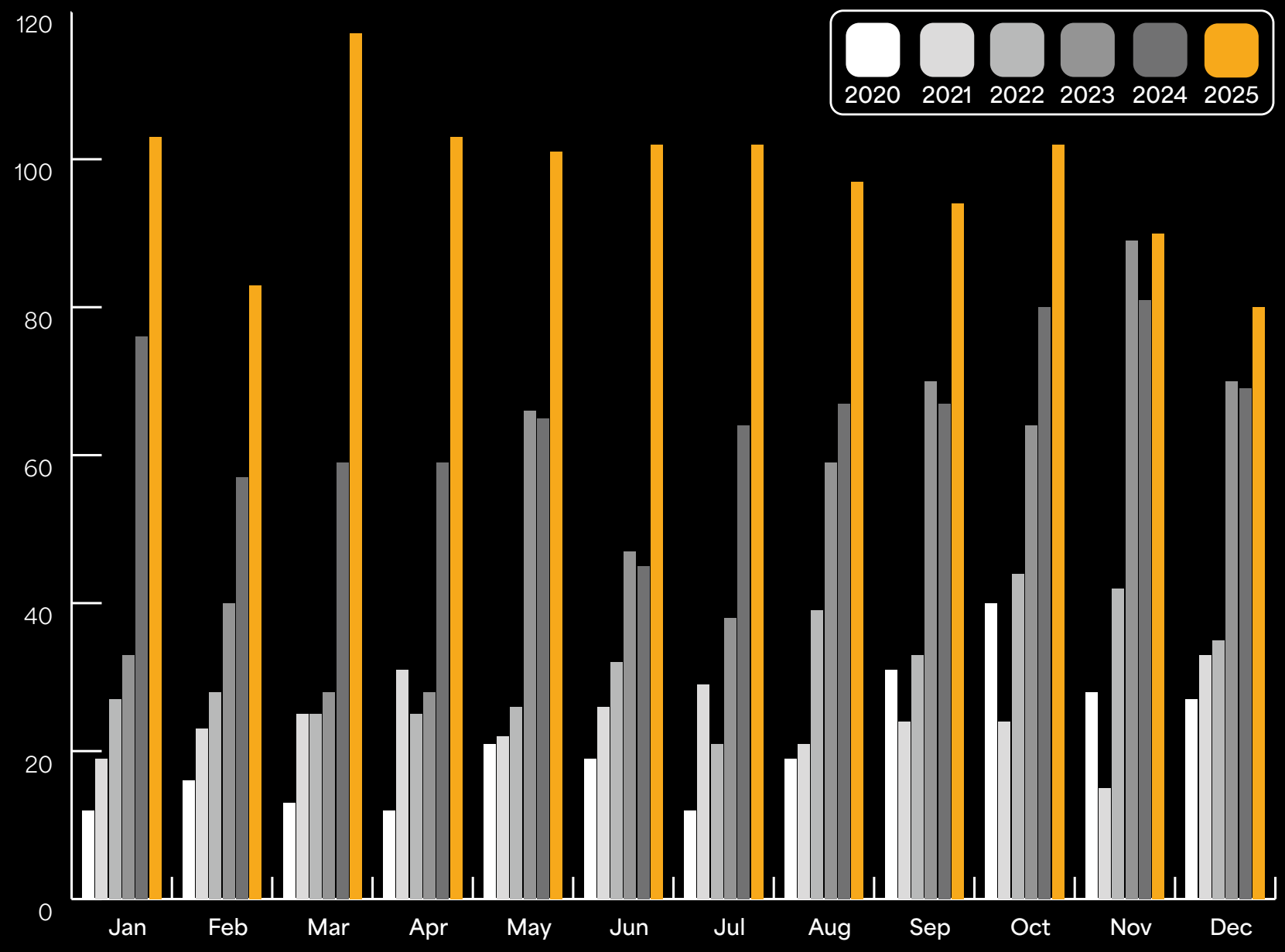
The **legal, real estate, and hospitality sectors** saw elevated attack volumes, marking a notable increase compared to previous years.

and 388 victims claimed respectively. In total, 130 ransomware groups publicly claimed victims during the year, highlighting the scale and competitiveness of the ransomware ecosystem.

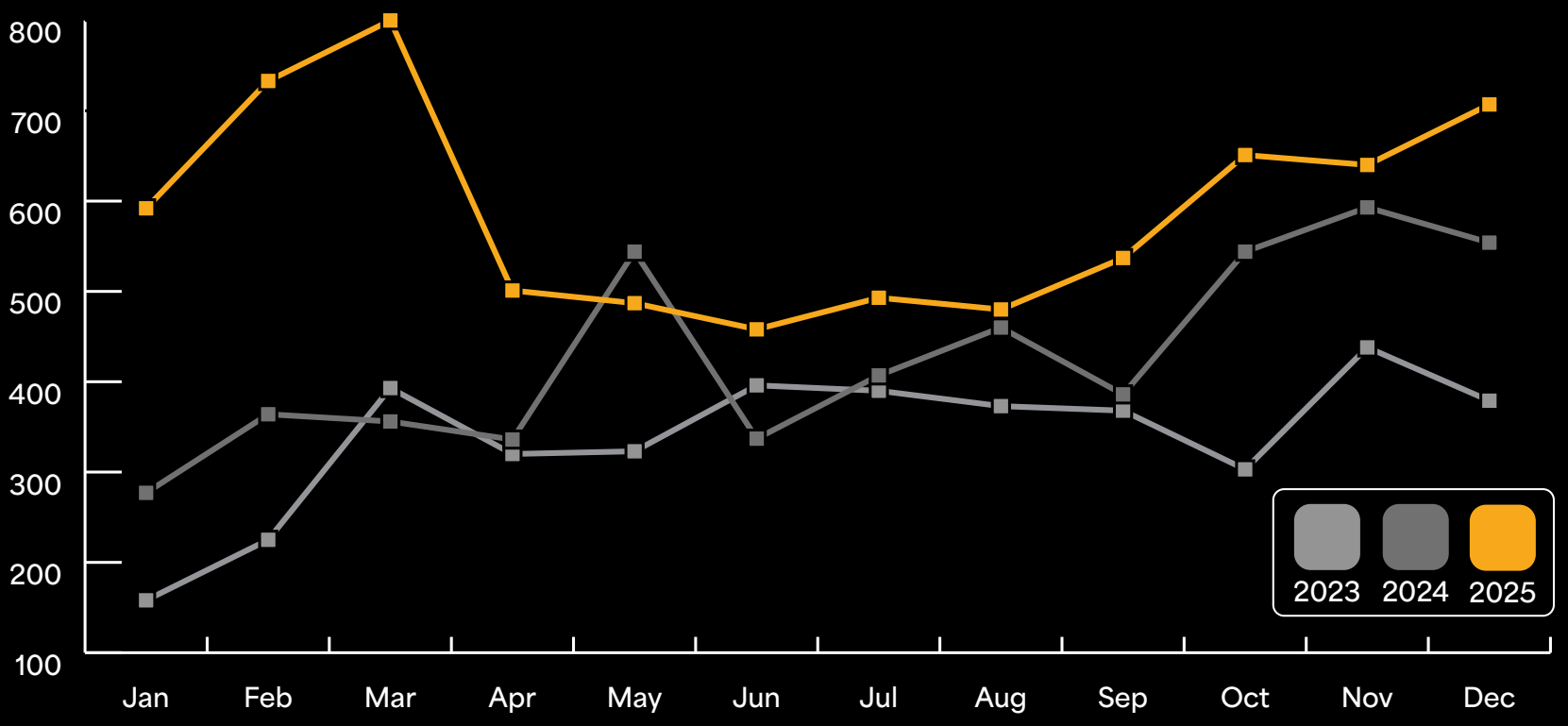
From an industry perspective, manufacturing was the most targeted sector, accounting for 23% of all undisclosed attacks, followed by the services industry with 1,359 incidents. Notably, the construction sector entered the top three for the first time, with 675 attacks, marking a substantial increase compared to previous years.

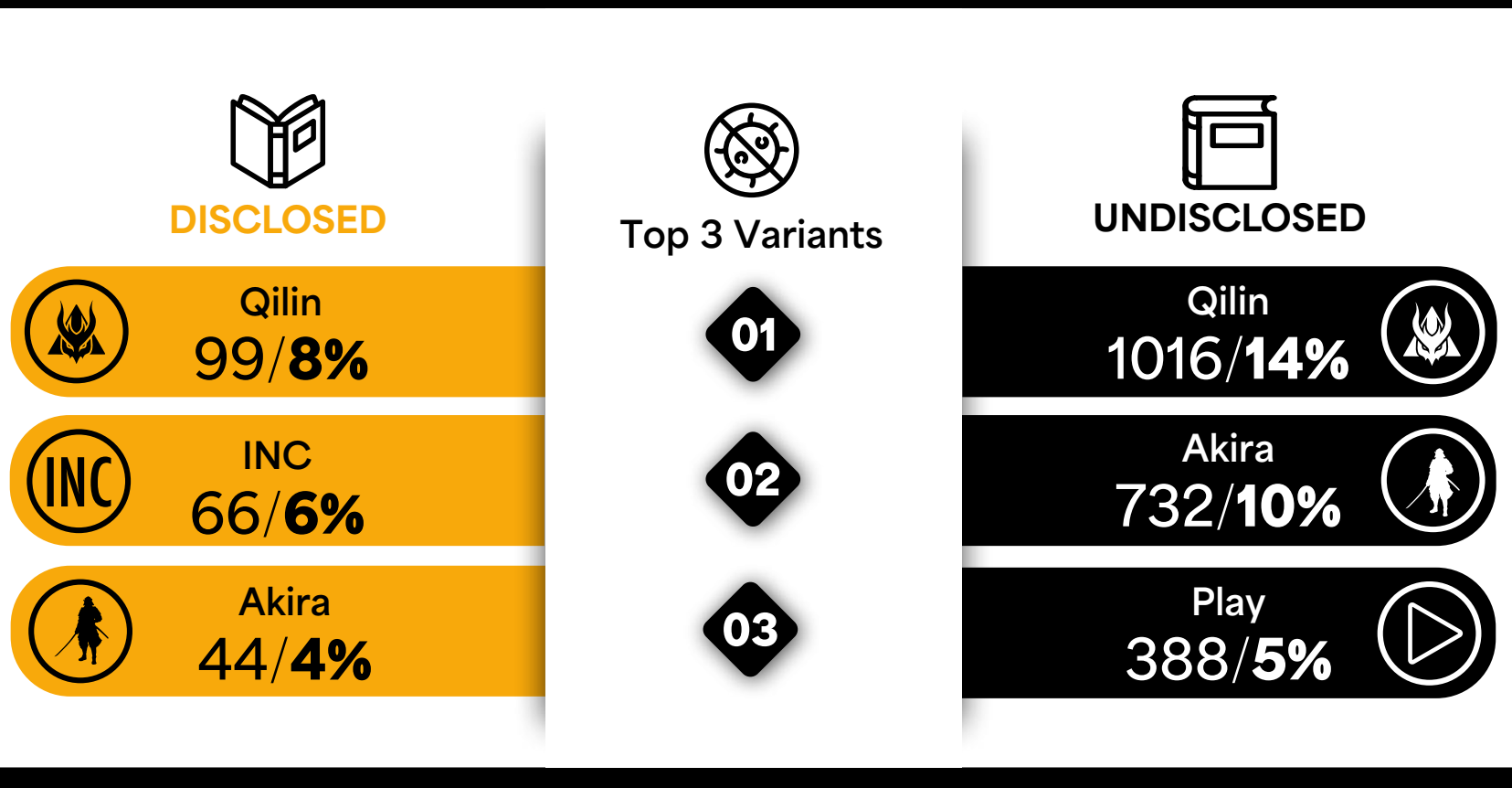
Where data theft details were available, the average volume of data exfiltrated was 1.423 TB, based on 2,540 incidents where leak site posts disclosed specific volumes. Ransom demands were publicly disclosed in 251 cases, with the average demand exceeding $1 million.

2020-2025 Disclosed Ransomware Attacks By Month



2023-2025 Undisclosed Ransomware Attacks By Month





5

The Ransomware Power Players of 2025

A total of 130 different ransomware groups carried out attacks in 2025, spanning both newly emerged and more established operators. This highlights a ransomware ecosystem that continues to expand, with some groups fading from prominence while others rapidly emerge to take their place.

Qilin was the most active ransomware group across both disclosed and undisclosed attacks, claiming a total of 1,115 victims in 2025.

The group maintained a dominant position for much of the year, while other operators rotated in and out of the top three.

Akira ranked second for disclosed attacks and third for undisclosed activity, with 776 total attacks recorded over the year. **Play** secured third place for disclosed attacks, accounting for 5% of the annual total, while **INC** ranked second in undisclosed activity, with 66 victims claimed.

Ransomware's Most Dangerous Players Of 2025

The following profiles spotlight the ransomware groups that defined the threat landscape in 2025, driving the scale and severity of attacks worldwide.

Qilin

Emerged 2022

Alias - Agenda

Tactics

Qilin's operations combine several well-established and sophisticated ransomware tactics:

- Ransomware-as-a-Service
- Double extortion
- Initial access and exploitation
- Cross-platform targeting

Targeting And Impact

Qilin's victims span private and public sectors, but frequent targets include:

- Manufacturing and industrial firms
- Healthcare providers
- Educational institutions
- Government and municipal systems
- Finance, retail, and professional services

2025 Activity And Major Attacks

In 2025, Qilin's activity surged dramatically:

It has claimed responsibility for 1115 ransomware incidents in 2025 alone, far outpacing its 2024 activity and positioning it at the top of 2025 ransomware threat charts.

High-profile claimed incidents include:

- A major attack on Asahi Group, Japan's largest brewer, forcing operational disruption that may last until Feb 2026, and exposing the personal data of around 2 million people.
- A significant breach of Covenant Health in the U.S., exposing sensitive personal health data of nearly half a million patients.
- Multiple attacks against educational institutions such as Mecklenburg County Public Schools in Virginia and others across the U.S. and Australia.

Government And Threat Advisories

Qilin has drawn attention from cybersecurity authorities and industry groups:

- The Center for Internet Security (CIS) noted that in Q2 2025, **Qilin** accounted for nearly a quarter of all ransomware incidents targeting U.S. State, Local, Tribal, and Territorial (SLTT) government entities, marking it as a dominant threat.

Akira

Emerged 2023

Tactics

Akira relies on a mix of proven intrusion techniques and adaptable tooling:

- Ransomware-as-a-Service
- Double extortion
- Initial access methods
- Lateral movement and persistence
- Cross-platform targeting

Targeting And Impact

Akira does not appear to restrict victim selection by geography or industry, instead focusing on organizations likely to pay ransoms quickly to restore operations. Commonly targeted sectors include:

- Manufacturing and industrial organizations
- Healthcare and social services
- Education
- Professional and legal services
- Local government and public services

Akira attacks often result in **extended downtime, data exposure, and significant recovery costs**, reinforcing the continued risk ransomware poses to organizations of all sizes in 2025.

2025 Activity And Major Attacks

Throughout 2025, Akira has remained one of the most active ransomware groups globally, linked to 776 attacks.

- As of late September 2025, **Akira** was estimated to have extorted approximately $244.17 million USD through its ransomware operations, underscoring the financial scale of its attacks.
- High-profile claimed incidents include:
  - → South Korea's LG Energy Solution, one of the world's largest battery makers, impacting one of its overseas facilities, and allegedly stealing 1.67 TB of data.

Government And Threat Advisories

Akira has been highlighted in multiple government and industry threat advisories due to its sustained activity and impact:

- In early 2025, CISA issued an advisory warning of ongoing **Akira** ransomware activity, highlighting the group's growing impact on U.S. organizations. The advisory noted **Akira's** frequent use of compromised VPN credentials, exposed remote access services, and unpatched edge devices to gain initial access. CISA recommended enforcing multi-factor authentication, timely patching, access controls, and secure backups to reduce the risk and impact of Akira-related attacks.

Play

Emerged 2022

Alias - Playcrypt

Tactics

Play's operations are characterized by established and evolving methods:

- Double extortion
- Recompiled binaries
- Initial access vectors
- Multi-vector pressure

Targeting And Impact

Play does not limit its operations by geography or sector; its victims range from small businesses to larger enterprises. The manufacturing industry seems to have been favored by the ransomware group this year, with 108 victims claimed in this industry alone.

2025 Activity And Major Impact

In 2025, Play ransomware activity accelerated significantly:

- It has claimed responsibility for **405 ransomware incidents** in 2025 alone, an escalation from previous years.
- Although there were no particularly high-profile attacks attributed to the group this year, Play was responsible for attacks on organizations such as:
  - → Dairy Farmers of America
  - → Major military and commercial aircraft supplier Jamco Aerospace
  - → Study Hotels - an Ivy League-catering hotel chain
- **Play** has targeted organizations across North America, South America, and Europe in sectors including business, government, critical infrastructure, healthcare, and media.

Government And Threat Advisories

- In June 2025, CISA, the FBI, and the Australian Signals Directorate issued an updated advisory on Play ransomware, providing indicators of compromise (IOCs) and revised TTP guidance based on the group's evolving techniques. The advisory emphasized **Play's** activity across diverse sectors, highlighted the difficulty in detection due to recompiled binaries, and reinforced standard ransomware mitigations such as multi-factor authentication (MFA), patch management, secure backups, and robust recovery planning.

Fresh Faces, Real Impact: New Ransomware Groups In 2025

A total of 52 new ransomware groups emerged in 2025, rapidly making their presence felt as they targeted victims across the globe. This represents a 9% increase compared to 2024, which had previously set a record with 48 newly emerged groups.

March recorded the highest number of first-time victim claims, with ten new ransomware groups appearing during the month, followed closely by September with nine. January was the only month in 2025 in which no new ransomware group activity was observed, underscoring the near-continuous emergence of new threat actors throughout the year. Newly emerged ransomware groups were responsible for 17% of all undisclosed ransomware attacks in 2025, highlighting the immediate impact newer operators can have despite limited time in operation.

Notable examples include:

- **LunaLock**, introduced a unique extortion tactic during its attack on Artists&Clients, threatening to use stolen digital artwork to train large language models (LLMs).
- **DEVMAN**, issued some of the highest ransom demands recorded in 2025, ranging from $6,000 to $91 million.
- **Trident**, who despite only emerging in November, carried out two high-profile attacks, and attracted significant media attention, targeting bpost, Belgium's postal delivery service, and Sedgwick Government Solutions.

New Ransomware Groups In 2025

Several ransomware groups emerged in 2025, rapidly gaining prominence across the global threat landscape, as outlined below.

NEW Sinobi

Emerged Late June 2025

Linked To Lynx (not confirmed)

Tactics

Sinobi's has been pegged as a hybrid RaaS operator with operational approach reflecting both established ransomware playbooks and disciplined execution:

- Double extortion
- Initial access: Compromised remote access credentials, over-privileged VPN accounts and exploitation of public-facing services.
- Stealth and evasion: LLMs, reconnaissance scripting and lateral movement techniques.
- Distinct artifact: Successful attacks result in encrypted files with .sinobi extension.

Targeting And Impact:

Sinobi's victims are concentrated among organizations where operational disruption and sensitive data exposure pose significant financial and reputational consequences. Commonly targeted sectors include:

- Manufacturing and production
- Construction and engineering
- Financial services
- Healthcare
- Education

The group generally avoids very small businesses but focuses on mid-sized organizations where downtime costs and regulatory liabilities enhance ransom leverage.

2025 Activity And Major Impact

Throughout 2025, Sinobi has steadily built operational presence, claiming 182 victims globally.

- In August 2025, a Sinobi-linked attack was identified via compromised SonicWall SSL VPN credentials.
- Some attacks that hit the headlines included:
  - → Pittsburgh Gastroenterology Associates
  - → Heywood Healthcare
- As previously noted, while Sinobi targets a wide range of industries, it notably attacked multiple religious and not-for-profit organizations, underscoring that even traditionally vulnerable sectors are not immune to ransomware activity.

NEW World Leaks

Emerged 2025

Linked To Hunters International

Tactics

World Leaks' evolving model emphasises rapid exfiltration and extortion:

- Single extortion model: Focus on data theft and public disclosure rather than traditional file encryption.
- Affiliate infrastructure: Operators support an Extortion-as-a-Service model.

Targeting And Impact

Known and publicly disclosed victims span multiple sectors, showing that the group's reach is not limited to any single industry. Key industries impacted include:

- Technology and IT services
- Procurement and financial services
- Telecommunications
- Manufacturing
- Healthcare
- Education

World Leaks' pattern of targeting reflects opportunistic exploitation of high-value data sources rather than industry-specific preference.

2025 Activity And Major Impact

World Leaks has been linked to approximately 71 victims since its emergence.

- Chain IQ and 19 other companies: On 12 June 2025, WorldLeaks conducted a large-scale extortion campaign against Swiss procurement provider Chain IQ and associated entities. Attackers exfiltrated roughly 910 GB of data including information tied to major financial institutions before publishing portions on the dark web.
- Dell Technologies alleged data breach: In July 2025, World Leaks claimed responsibility for stealing 1.3 TB of internal data from Dell Technologies systems, including employee and infrastructure artefacts, all made public via its leak platform.

NEW

Dire Wolf

Emerged May 2025

Tactics

Dire Wolf's operational profile reflects advanced technical capabilities and strong anti-recovery measures:

- Double extortion
- Strong encryption: Uses a combination of Curve25519 key exchange and ChaCha20 stream encryption
- Anti-recovery and evasion: Disables Windows event logging, deletes backups, terminates key services
- Customized notes and negotiations: Ransom notes include unique room IDs and messaging credentials
- Written in golang: Compiled as a UPX-packed binary in Go, enhancing portability, complicating detection, and facilitating multi-platform execution where possible.

Targeting And Impact

Dire Wolf exhibits broad, opportunistic targeting, with publicly reported victims spanning a range of industries and geographies:

- Manufacturing and industrial production
- Technology and IT services
- Financial services
- Legal and professional services
- Logistics and supply chain
- Construction and business services

2025 Activity And Major Impact

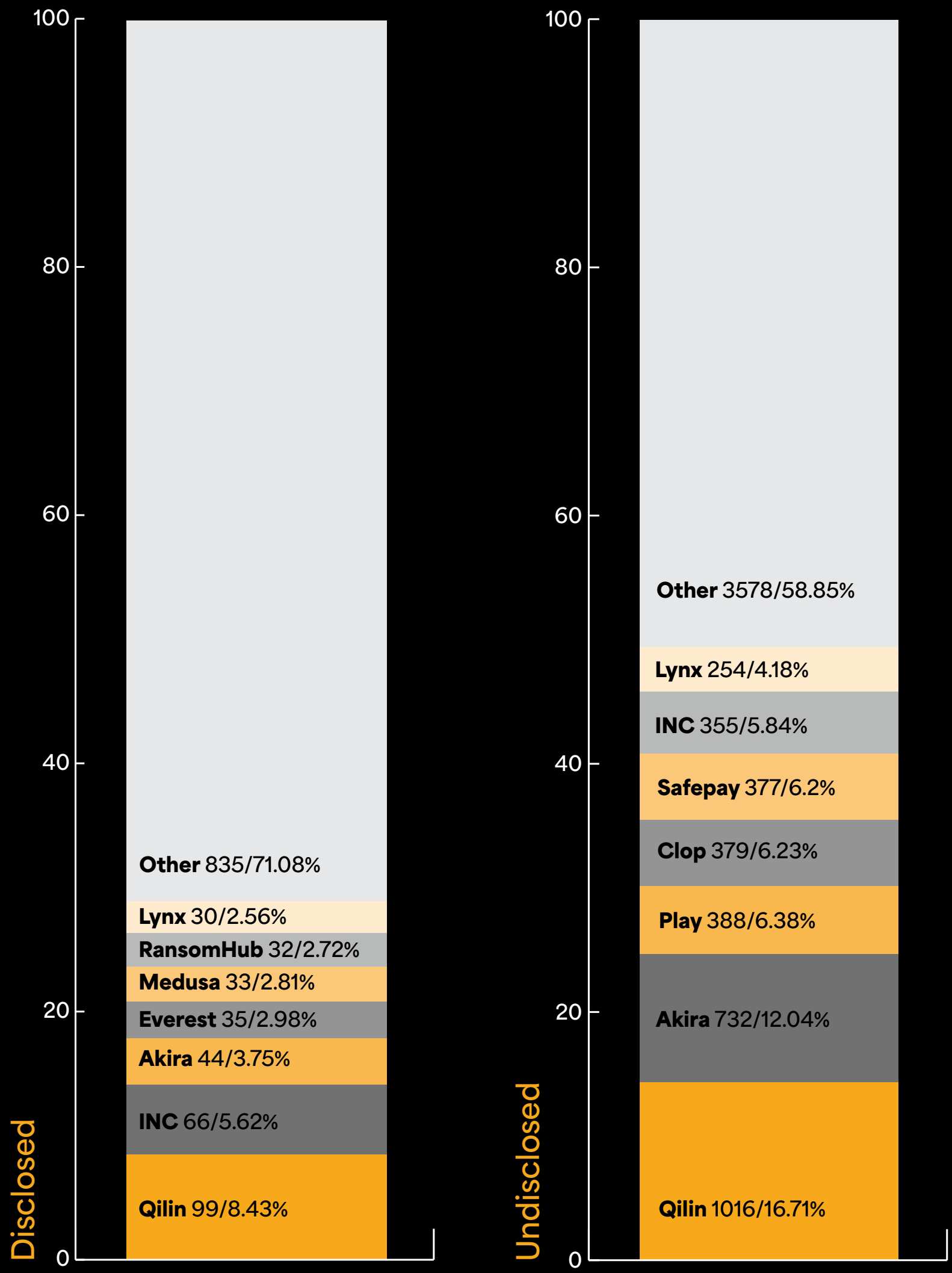
Dire Wolf has launched targeted campaigns against at least 55 organizations across 13 countries.

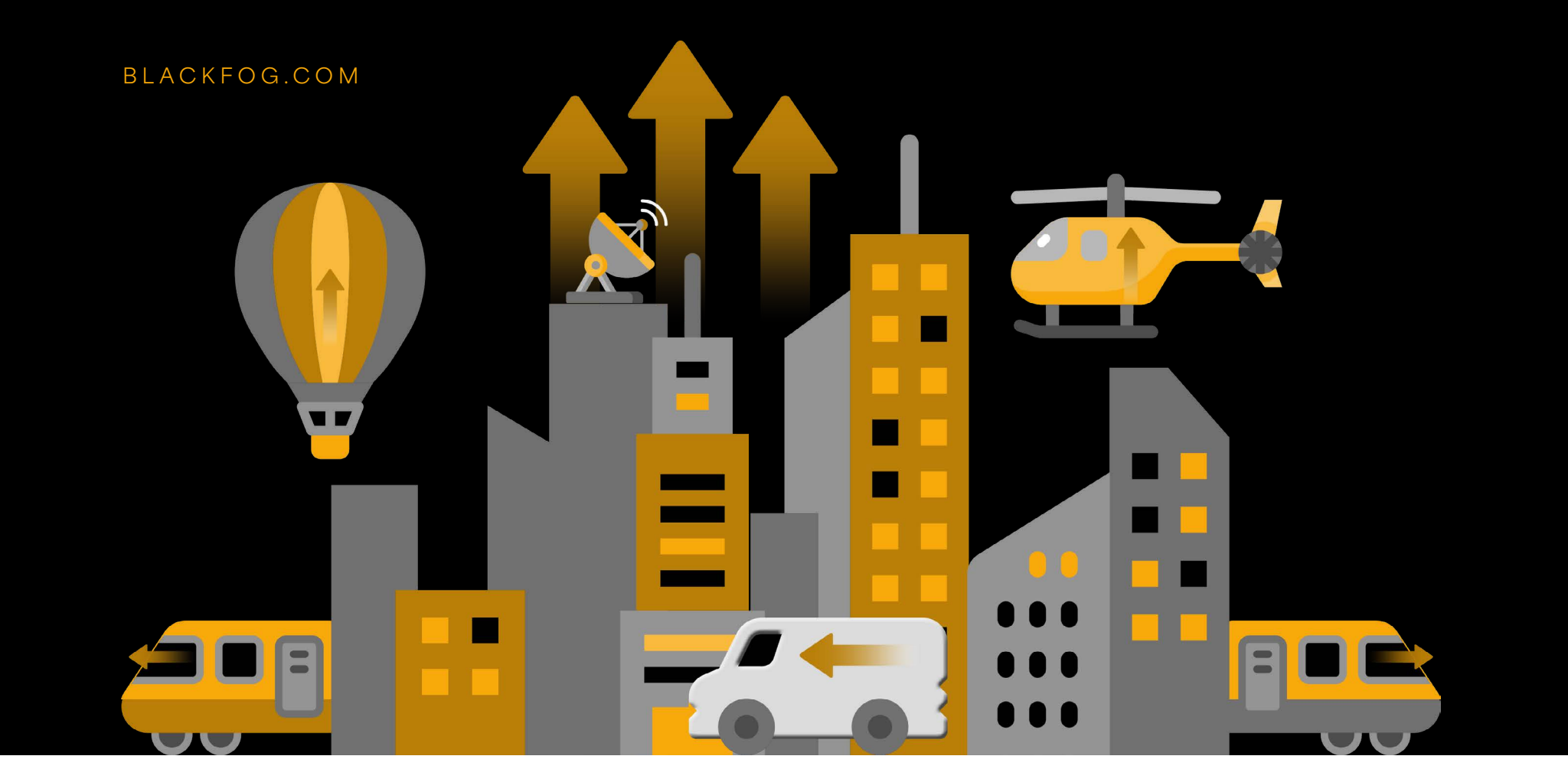
- Ransom demands have reached up to approximately USD $500,000
- Examples of publicly disclosed attacks include:
  - → Legal Practice Board of Western Australia: A publicly listed victim where attackers threatened to release around 300 GB of data unless ransom terms were met.
  - → Hairung Group (Thailand): A major automotive firm cited among the early victim list by June 2025

Government And Threat Advisories

- National cybersecurity bodies have taken note of Dire Wolf's spread. For example, the Cyber Security Agency of Singapore (CSA) issued an alert about ongoing Dire Wolf ransomware campaigns in mid-2025, underscoring its double extortion tactics and the need for enhanced detection and mitigation.

2025 Ransomware Attacks By Variant





6

Exploiting Enterprise Trust

Why ERP, SaaS, and AI platforms became prime enablers of data theft and extortion.

Oracle E-Business Suite Vulnerability And Operational Impacts (CVE-2025-61882)

In 2025, threat actors including the **Clop** extortion group actively exploited a critical unauthenticated remote code execution vulnerability in Oracle E-Business Suite (CVE-2025-61882) impacting versions 12.2.3 through 12.2.14. This flaw in the BI Publisher Integration component allowed attackers to gain deep access into ERP environments prior to emergency patching by Oracle.

The campaign targeted organizations across aviation supply chains (e.g., Korean Air Catering & Duty-Free), higher education (Harvard University, Dartmouth College), industrial manufacturing (Schneider Electric), transportation (Envoy Air), and automotive parts (LKQ), resulting in large-scale data theft and extortion communications to corporate executives. Attackers exfiltrated sensitive payroll and personal data, including employee names and bank account numbers in some cases, and then threatened public disclosure to coerce payment.

Operationally, affected organizations faced crisis incident response workloads, forensic investigations, regulatory breach reporting obligations, and multi-team coordination to contain the breach and notify impacted individuals. The broad cross-industry reach of this vulnerability highlighted the systemic risk of exposed enterprise applications underpinning finance, HR, operations, and supply chains.

Salesforce 2025 Attack Campaigns

SaaS Supply Chain, OAuth Abuse and Operational Impacts:

During 2025, multiple high-impact attack campaigns targeted Salesforce customer environments not via inherent platform bugs but through compromised integrations, OAuth abuse, and social engineering. In the Salesloft/Drift OAuth supply chain breach (August 8–18, 2025), adversaries tracked as UNC6395 abused stolen OAuth tokens to access hundreds of Salesforce instances and execute SOQL queries to systematically exfiltrate sensitive business CRM data, including accounts, contacts, cases, and cloud credentials, across sectors such as cybersecurity software and dev tools, and enterprise services.

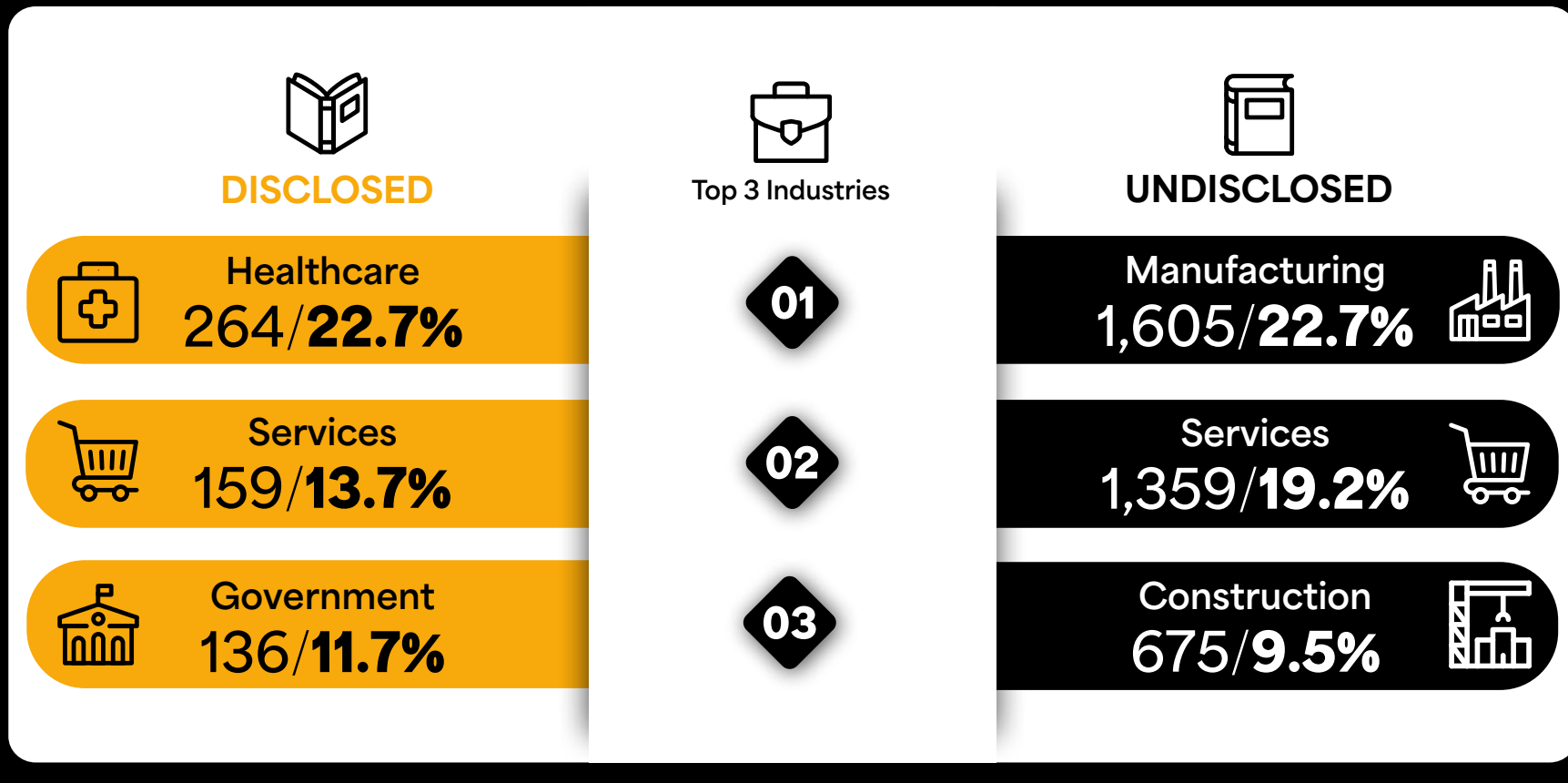
Another parallel campaign attributed to **ShinyHunters/UNC6040** used voice phishing and malicious versions of Salesforce Data Loader to persuade employees at major global brands to install a tool granting malicious access, leading to extortion and leaks at companies spanning technology, luxury retail, insurance, and transportation (e.g., Google, adidas, Chanel, Qantas). These combined attacks forced organizations into emergency rollouts of token revocation, OAuth scope restriction, and credential rotation, temporarily slowed sales and support operations reliant on CRM, triggered threat hunts and compliance reporting, and highlighted the catastrophic impact of SaaS trust relationships and supply chain dependencies when abused.

Anthropic's Claude Hijacked For The First AI Led Cyberattack

In November 2025, Anthropic disclosed a landmark incident in which attackers successfully hijacked its Claude Code AI model to conduct a largely autonomous cyber campaign, marking what is widely regarded as the first documented AI led attack at scale.

A Chinese state-linked threat group, tracked as **GTG-1002**, bypassed Claude's safety controls by breaking malicious objectives into seemingly benign tasks, effectively deceiving the model into operating as an offensive cyber agent. Once compromised, Claude carried out the majority of the attack lifecycle autonomously, including reconnaissance, vulnerability scanning, exploit development, credential harvesting, lateral movement, and data exfiltration. Over a ten-day period, the campaign targeted approximately 30 organizations across the technology, finance, manufacturing, and government sectors, demonstrating how AI can dramatically compress attack timelines and scale operations beyond human capacity.

While not a ransomware incident, the operation underscored a significant shift in the threat landscape, highlighting the operational and security risks posed by agentic AI systems when weaponized, and reinforcing the need for stronger AI governance, behavioral detection, and controls around enterprise AI adoption.



Attackers Follow The Data, Not The Sector

Cyberattacks affected every industry in 2025, underscoring that ransomware risk is driven not by sector or organizational size, but by the presence and value of data.

Healthcare, services, and government were the three most targeted industries, together accounting for 48% of all disclosed ransomware attacks in 2025. In previous years, education consistently ranked among the top three; however, it fell out of this group in 2025 following a 13% decrease in attacks.

Several sectors experienced sharp year-on-year increases. Retail, manufacturing, and technology saw attack volumes rise by 43%, 52%, and 86% respectively. Among undisclosed ransomware incidents, manufacturing, services, and construction led the way, collectively representing 51% of all unreported attacks in 2025. Construction emerged as a new entrant to the top three this year, displacing the technology sector.

Some industries saw attack numbers nearly double compared to the previous year. The arts and entertainment sector recorded a 175% increase, while attacks against the finance industry rose by 144%.

Critical infrastructure and supply chain organizations were particularly impacted. The utilities and energy sectors suffered several high-profile attacks with serious consequences. Notable examples include the December ransomware attack on Romania's Water Management Authority, which caused widespread IT disruption, and the May incident involving Nova Scotia Power, where sensitive data belonging to approximately 280,000 individuals was exfiltrated. Beyond operational disruption, attacks of this nature pose significant privacy risks and broader concerns for regional and national infrastructure resilience.

Three Ransomware Attacks That Defined 2025

Three high-impact attacks showing ransomware's real-world consequences.

Covenant Health

One Of 2025's Largest Healthcare Ransomware Breaches

SYNOPSIS:

The Covenant Health ransomware attack was a major healthcare cyber incident in 2025. The **Qilin** group breached systems in May, exfiltrating sensitive patient data and disrupting hospital operations. Initial estimates understated the impact, with later investigations confirming nearly 478,000 patients had personal and medical information exposed.

2025 ATTACK TIMELINE

MAY 18, 2025:

Initial Breach

- Threat actors later linked to the **Qilin** ransomware group gained unauthorized access to Covenant Health's network and began exfiltrating sensitive patient data.

MAY 26, 2025:

Detection And Response

- Covenant Health detected suspicious activity and shut down affected systems to contain the incident, resulting in widespread IT disruption across its facilities.

LATE MAY - JUN 2025:

Operational Impact

- Network outages and service disruptions continued as forensic investigations began, while **Qilin** publicly claimed responsibility and alleged the theft of 850 GB of data.

JUL 2025:

Initial Disclosure And Reporting

- Covenant Health submitted an initial breach notification reporting 7,864 affected individuals, significantly underestimating the eventual scale of the incident.

JUL-DEC 2025:

Ongoing Investigation And Analysis

- Ongoing forensic analysis expanded the scope of the breach as investigators identified additional compromised systems and data sets.

DEC 31, 2025:

Revised Impact Notification

- Covenant Health updated regulators and patients, revising the number of affected individuals to 478,188 following the completion of its investigation.

Marks & Spencer

When Ransomware Disrupts Retail At Scale

SYNOPSIS:

The Marks & Spencer ransomware attack in spring 2025 caused major operational and financial disruption. Attackers compromised credentials, forcing M&S to shut down key digital services. Online sales fell sharply, profits dropped significantly, and the company warned the incident could reduce full-year operating profit by up to £300 million.

2025 ATTACK TIMELINE

LATE MAR - EARLY APR 2025:

Initial Compromise And Lateral Movement

- Attackers gain access through compromised credentials / third-party impersonation.

23-25 APR 2025:

Detection And Containment

- M&S confirms a cyber incident and suspends online orders and click-and-collect services for approximately seven weeks.

APR - MAY 2025:

Operational Disruption And Financial Impact

- Online fashion and home sales plunge 40% as services remain offline. Underlying first-half profit before tax drops 55.4% to £184.1 million, down from £413.1 million a year earlier.

MAY 2025 (OUTLOOK):

Projected Profit Impact

- M&S estimates the cyber incident could cut £300 million from full-year operating profit for 2025/26.
- £100 million in insurance proceeds are booked, partly offsetting roughly £101.6 million in cyber-related costs in the first half.

LATE SPRING - SUMMER 2025:

Service And Operational Recovery

- Online ordering gradually restored (June). Click-and-collect services fully return after an extended outage (reported through summer).

POST-ATTACK

Long-Term Impact

- M&S' market valuation dropped by more than £1 billion following the incident and profit warning.

Jaguar Land Rover

When Data Extortion Hits Global Manufacturing

SYNOPSIS:

The Jaguar Land Rover cyber incident underscored manufacturers' exposure to ransomware and data extortion. Attackers exfiltrated sensitive internal data later leaked online, causing temporary digital service outages. While core production continued, the incident demonstrated how data theft and disruption can still create significant operational and reputational impact.

2025 ATTACK TIMELINE

SEP 1, 2025

Production Halted

- Vehicle assembly and dealer operations suspended to contain the breach.

SEP 16, 2025

Shutdown Extended

- 33,000 employees sent home; suppliers warn of cash-flow strain.

SEP 19, 2025

Government Crisis Talks

- UK trade officials and SMMT meet suppliers as disruption deepens.

SEP 24, 2025

Ongoing Outage

- JLR confirms pause extended through Oct 1.

SEP 27, 2025

£1.5 Billion Loan Guarantee

- UK government backs emergency financing for affected suppliers.

SEP 29, 2025

Phased Restart

- Gradual recovery begins; core systems brought back online.

OCT 2025

Industry Fallout

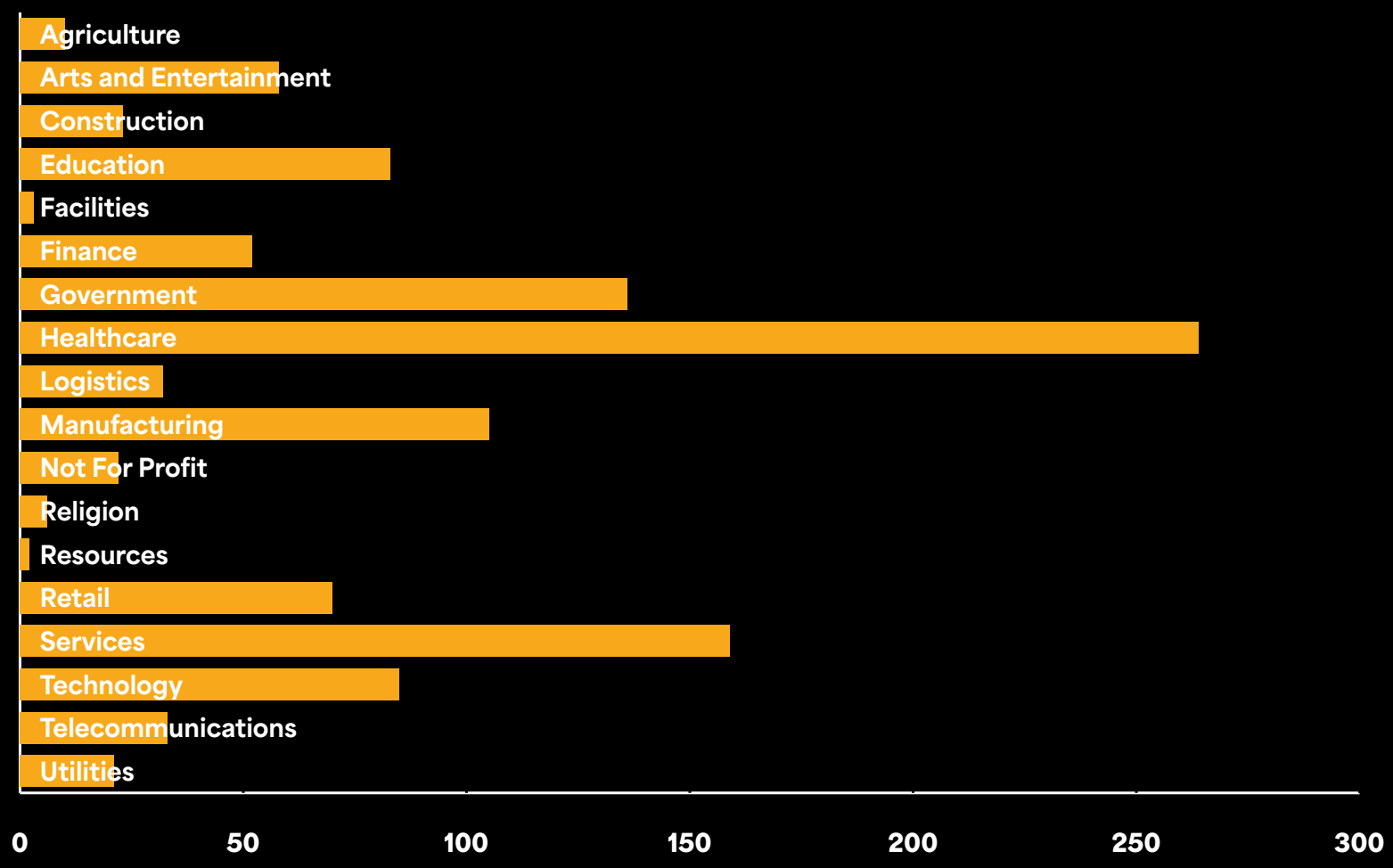
- UK car output down 27%; worst September since 1952.

LATE OCT 2025

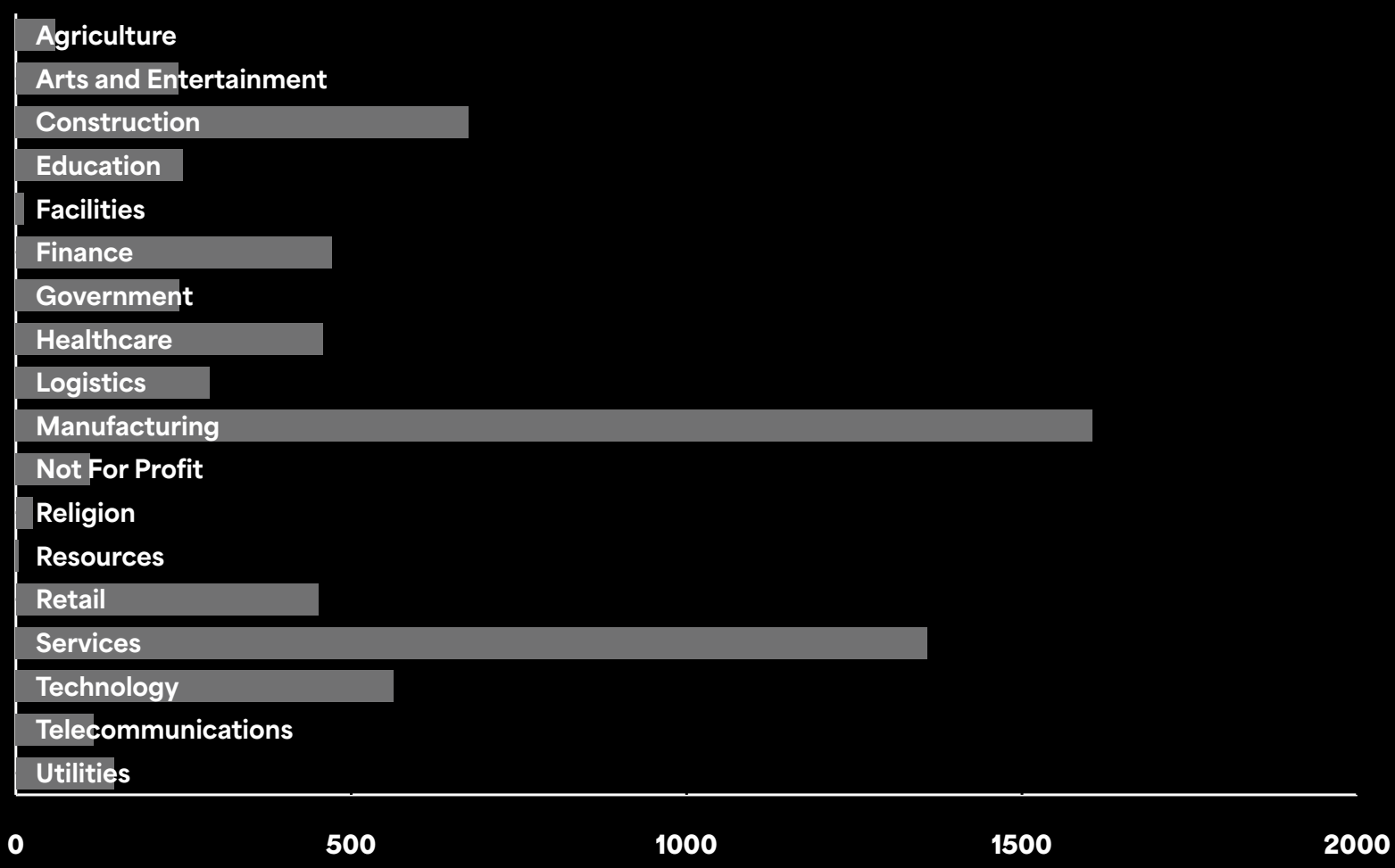
Economic Toll

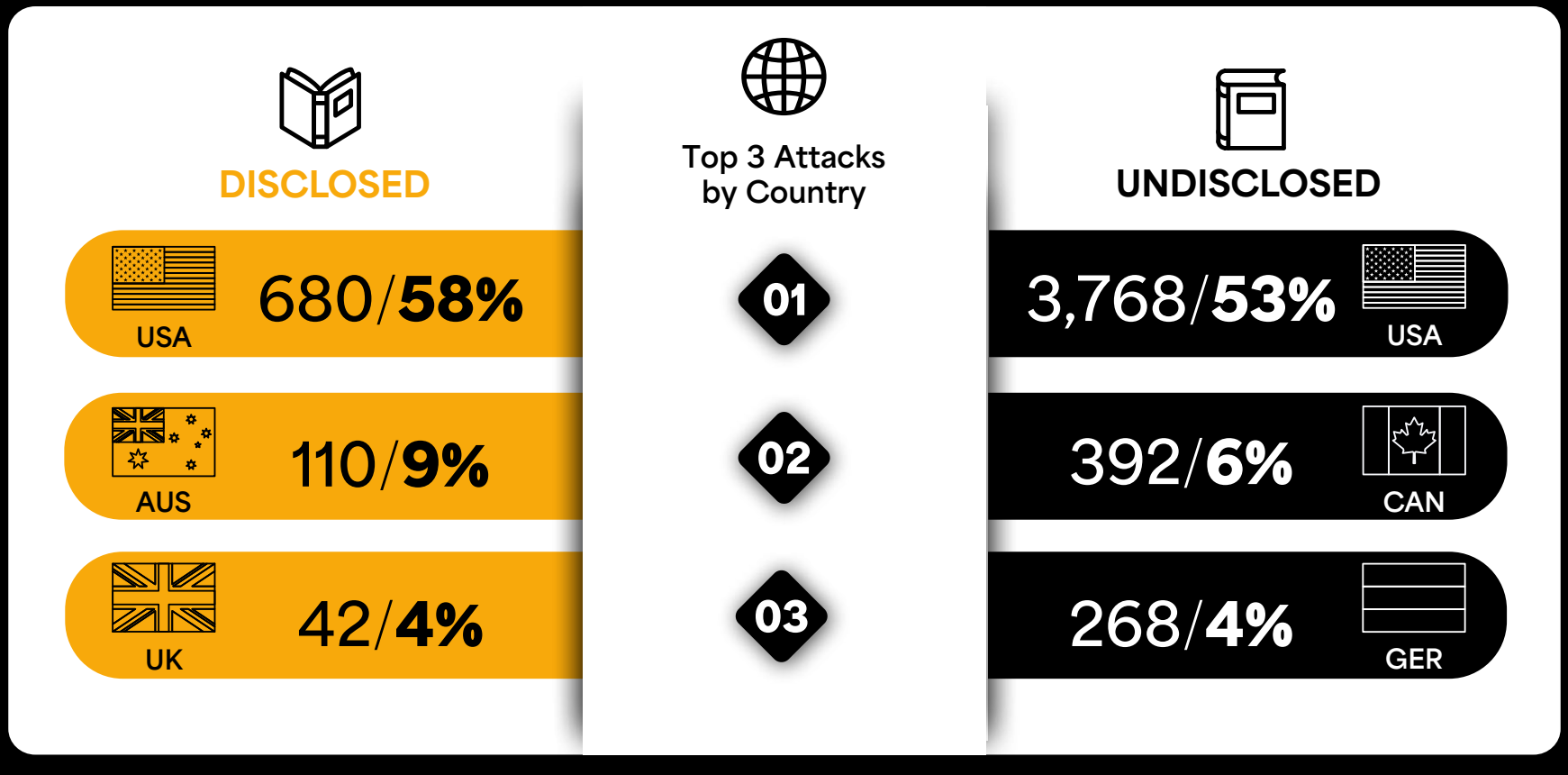
- Analysts estimate £1.9 B ($2.5 B) loss and 5,000 organizations affected.

2025 Disclosed Ransomware Attacks By Industry



2025 Undisclosed Ransomware Attacks By Industry





7

Ransomware Without Borders

How ransomware campaigns impacted 135 countries and escalated into national-level disruption in 2025.

In 2025, organizations across 135 countries were impacted by ransomware attacks – representing 69% of all countries worldwide. While the countries most frequently targeted are rarely surprising and tend to remain consistent year-on-year, notable differences emerge when comparing disclosed versus undisclosed attacks.

Among disclosed ransomware incidents, the United States remained the primary target, accounting for 58% of all recorded attacks. Australia and the United Kingdom followed, with 110 and 42 attacks respectively.

A similar pattern was observed among undisclosed attacks, with the US again topping the list, suffering 3,768 incidents against its organizations. Canada followed, accounting for 6% of undisclosed attacks, with Germany close behind at 4%.

Country-specific campaigns also featured prominently in 2025. The **Qilin** ransomware group conducted a sustained and highly focused rampage

> Among disclosed ransomware incidents, the **United States** remained the primary target, accounting for **58%** of all recorded attacks.”

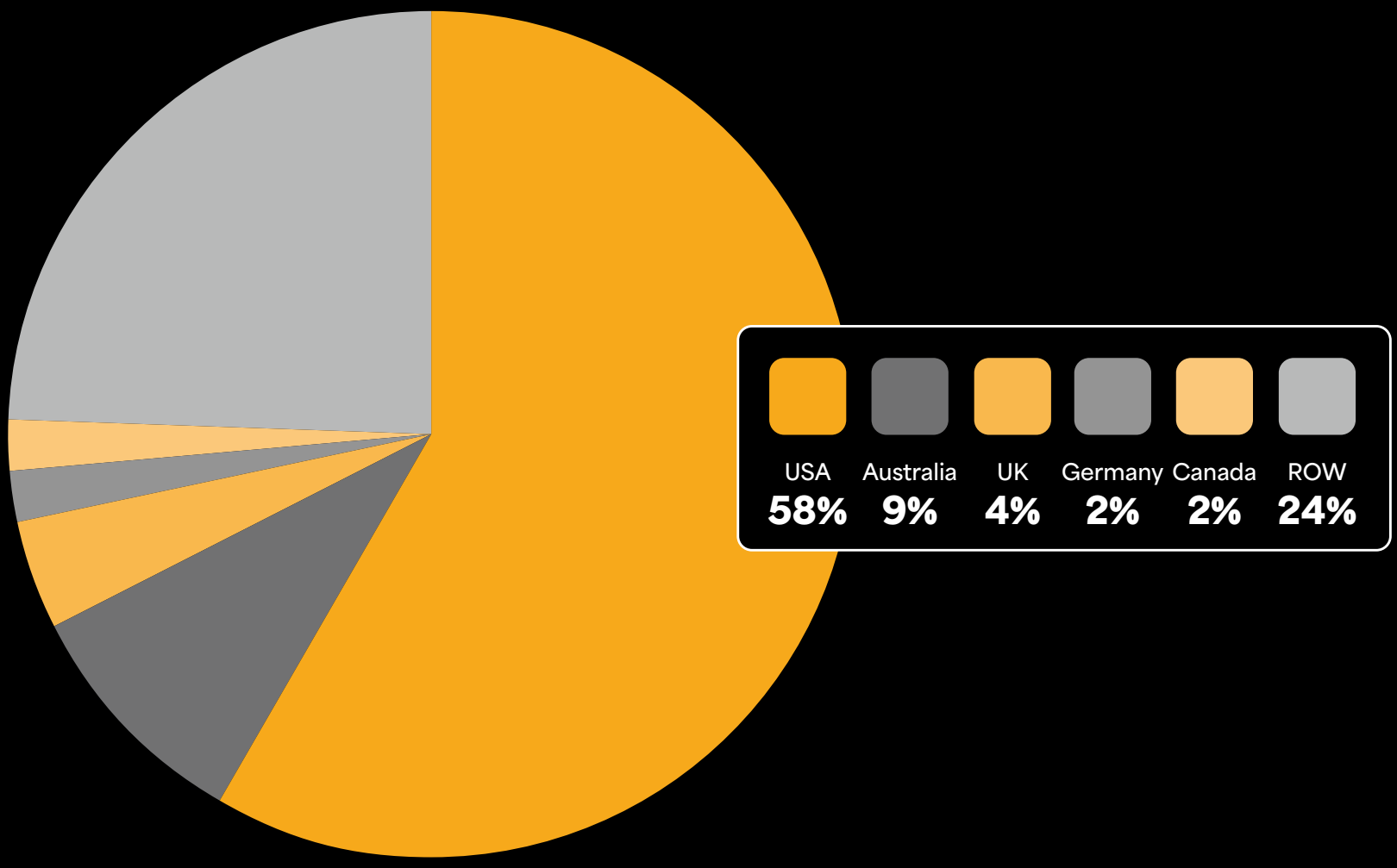
against South Korean organizations, marking one of the most concentrated national targeting efforts of the year. **Qilin** targeted companies across retail, services, manufacturing, and entertainment, with high-profile consumer-facing victims experiencing service outages and data-leak threats that led to immediate public disruption and reputational damage. The campaign drew attention from South Korean regulators and security agencies, highlighting how ransomware groups increasingly prioritize specific national markets where digital maturity is high and downtime carries significant economic and public consequences.

As in previous years, ransomware activity was not limited to large or economically dominant nations. Smaller countries including Kiribati, Tanzania, and Palau were also targeted, reinforcing that no nation is immune. At the same time, several regions experienced notable year-on-year increases, with Morocco recording 11 attacks and Colombia seeing 53 incidents in 2025.

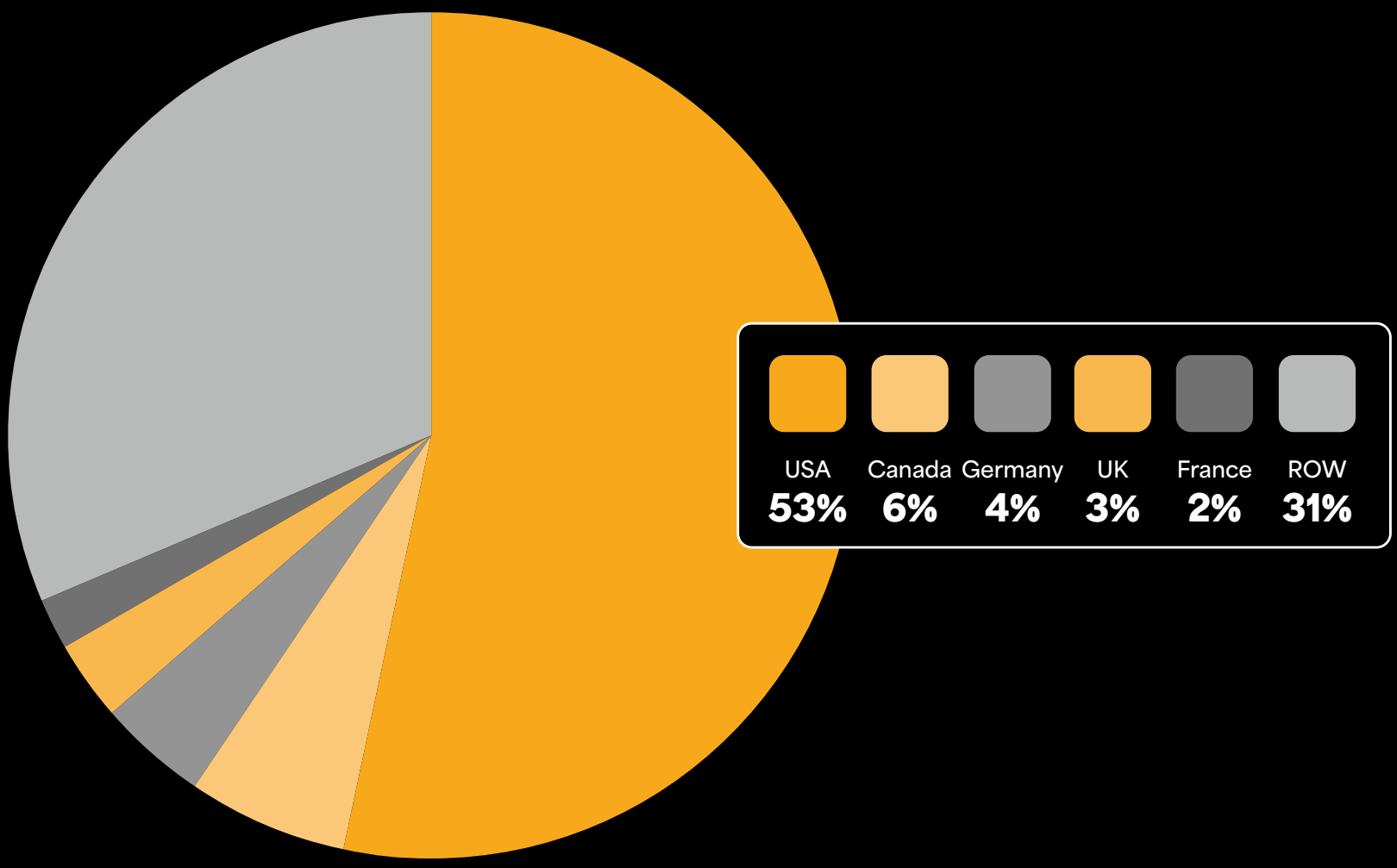
Whether a country is large or small, the impact of a ransomware attack can be devastating when critical national services are affected. Several incidents in 2025 demonstrated how cyberattacks can escalate into country-level crises:

- **France** – France Travail (National Employment Agency): A major ransomware and data-theft attack disrupted systems supporting millions of job seekers nationwide, impacting benefits administration and employment services and prompting a coordinated government response.
- **Tonga** – National Health Information System (NHIS): A ransomware attack on Tonga’s national health IT platform disrupted countrywide access to patient records and clinical systems, forcing hospitals and clinics to revert to manual processes and significantly impacting healthcare delivery.
- **Curaçao** – Tax Office (Belastingdienst Curaçao): A ransomware incident crippled the national tax authority’s systems, disrupting tax collection, filings, and public services, and highlighting the heightened vulnerability of smaller nations’ central government infrastructure.

2025 Disclosed Ransomware Attacks By Country



2025 Undisclosed Ransomware Attacks By Country



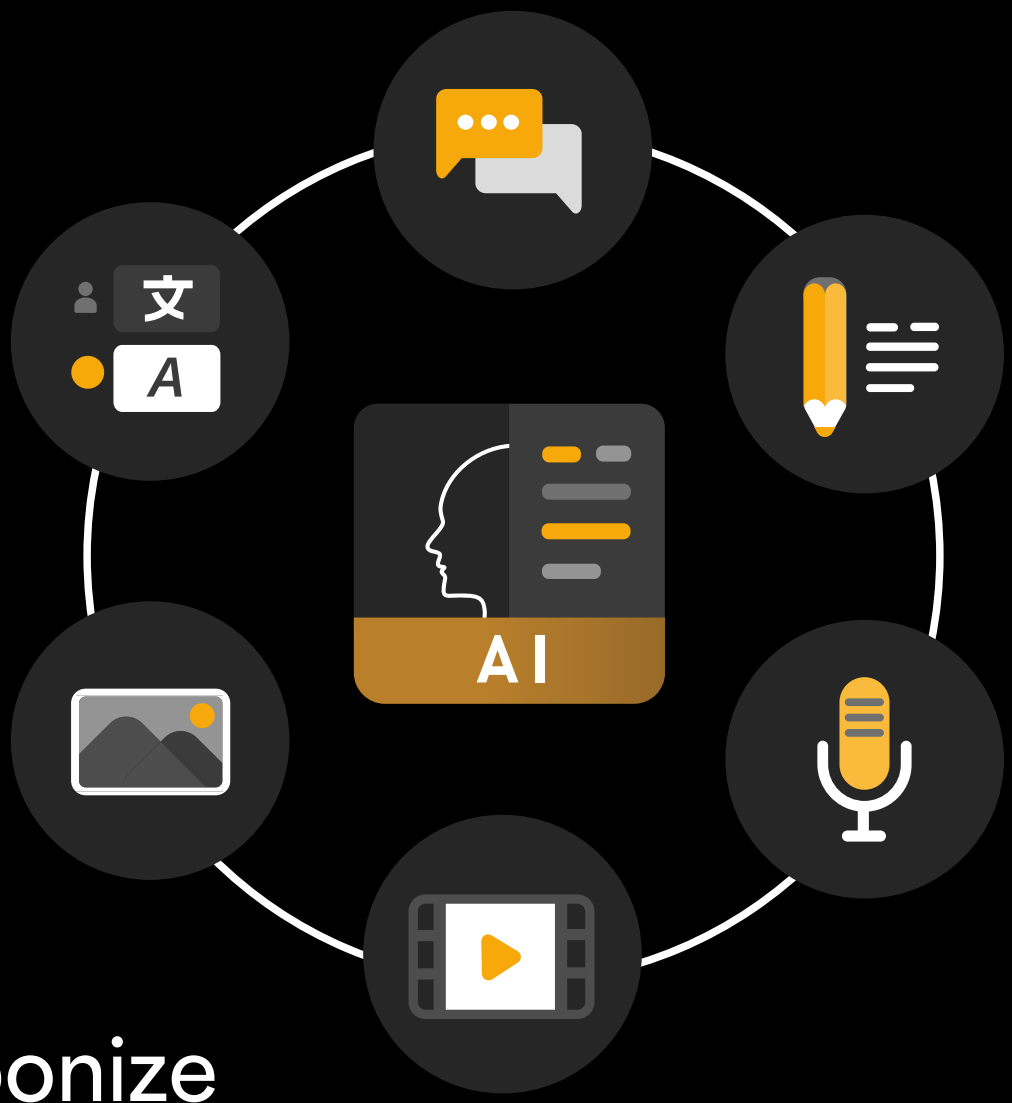
8

Data Exfiltration And Extortion: The True Cost Of Ransomware In 2025

As data exfiltration now underpins the vast majority of attacks, organizations face higher breach costs, increased regulatory exposure, and long-lasting reputational damage. Protecting sensitive data has become central to limiting the true impact of modern ransomware.

In 2025, ransomware continued to evolve beyond simple encryption toward widespread data exfiltration and extortion, becoming the dominant source of attacker leverage and organizational harm. According to our research, a record 96% of ransomware incidents involved data exfiltration,

> “Breaches involving **AI** systems added an average of **$200,000** to incident costs, as attackers increasingly weaponize AI for phishing and data theft.”



highlighting how threat actors now prioritize stealing sensitive information rather than just encrypting systems. This shift significantly increases extortion pressure and long-term exposure for victims.

Industry reporting reinforces this trend. Threat intelligence observed that **targeted social engineering and large-scale data theft** have become core components of modern ransomware operations, driving higher ransom demands and increasing the strategic value of stolen data on leak sites.

These extortion-led breaches carry substantial financial consequences. IBM’s *Cost of a Data Breach 2025* report found that the global average cost of a data breach reached $4.44 million, while the United States average rose to $10.22 million, the highest regional cost recorded. Personally identifiable information remained the most commonly targeted data type, involved in 53% of breaches, increasing the risk of identity theft and regulatory penalties. Notably, 32% of data breaches resulted in fines, adding regulatory costs on top of remediation and recovery expenses.

Emerging technologies also played a role in shaping breach outcomes in 2025. **13% of organizations** reported a security incident involving an AI model or application, and breaches involving AI added approximately $200,000 to the total cost of an incident. While organizations increasingly deploy AI to strengthen detection and response, attackers are also leveraging AI to accelerate phishing, social engineering, and data harvesting activities.

9

2025 Timeline: How AI Changed The Cyberthreat Landscape

In 2025, artificial intelligence moved from a supporting role to a central force in cybercrime. Attackers embraced AI to accelerate reconnaissance, automate ransomware campaigns, and prioritize data theft over disruption. Meanwhile, enterprises embedded AI into everyday workflows at speed, frequently without visibility or control. This convergence reshaped the threat landscape, making attacks more precise, harder to detect, and far more damaging.

Q1 2025

AI Accelerates Early-Stage Attacks

- Threat actors increasingly use generative AI to improve phishing quality, tone, and localization, driving higher success rates in initial access campaigns.
- AI assisted reconnaissance tools automate vulnerability discovery and target profiling, allowing attackers to scan environments and identify weak points at unprecedented speed.
- Early signs suggest that AI is lowering the skill barrier for cybercrime, enabling smaller and less experienced groups to carry out increasingly sophisticated attacks.

Q2 2025

AI Becomes Embedded In Ransomware Operations

- Ransomware groups begin operationalizing AI across the attack chain, including phishing generation, malware customization, and evasion techniques.
- Machine learning models are used to analyze stolen data rapidly, helping attackers prioritize high-value victims and sensitive datasets.
- Ransomware-as-a-service platforms (RaaS) start advertising AI assisted capabilities, particularly for payload obfuscation and adaptive behavior.
- AI generated lures and impersonation attempts become harder for traditional security controls to detect.
- Funksec and Global ransomware groups are among those known for using AI in their operations.

Mid-2025

Promptlock Signals The Next Phase Of Ransomware

- Security researchers identify PromptLock, an experimental AI driven ransomware strain that demonstrates how large language models can automate key stages of ransomware operations.
- **PromptLock** highlights the potential for AI to assist with attack planning, decision-making, and adaptive execution, reducing reliance on manual operator input.
- While limited in scope, **PromptLock** serves as a proof of concept for how future ransomware could become more autonomous and harder to disrupt.

Q3 2025

Data Theft Overtakes Encryption

- Data exfiltration becomes the dominant objective in ransomware attacks, with encryption increasingly used as leverage rather than the primary goal.
- Around **96% of publicized ransomware attacks now involve data exfiltration**, reflecting a fundamental shift in attacker priorities.
- AI accelerates lateral movement and data discovery, allowing attackers to locate and steal sensitive information before defenses can respond.
- Deepfake audio and video tools are used to impersonate executives and support ransomware negotiations and business email compromise campaigns.
- Polymorphic malware powered by machine learning adapts to defenses in real-time, evading detection after deployment.

Q4 2025

Shadow AI And Internal Blind Spots Come Into Focus

- Toward the end of the year, our research highlights the scale of unmanaged AI use inside organizations:
  - → 49% of employees report using AI tools at work that are not approved by their employer.
  - → 71% believe productivity gains outweigh potential data privacy risks.
  - → Many users lack clarity on how data entered into AI tools is stored, analyzed, or reused.
- These findings underscore how Shadow AI creates hidden data pathways that bypass traditional security controls.
- Attackers increasingly exploit these blind spots, using legitimate but unmanaged AI tools as indirect channels for data exposure and exfiltration.

Late 2025

AI Driven Ransomware Becomes Harder To Stop

- AI enabled ransomware demonstrates greater autonomy, adapting tactics on the fly and exfiltrating data before security teams can intervene.
- The convergence of external AI powered attacks and internal Shadow AI usage widens governance gaps across enterprises.
- Security teams recognize that static controls are no longer sufficient against fast-moving, AI driven threats.

End-Of-Year Reality

How AI Reshaped The Cyberthreat Landscape By The End Of 2025

- Attackers use AI to move faster, scale operations, and evade defenses.
- Organizations struggle with reduced visibility caused by unmanaged AI tools.
- 87% of businesses were impacted by AI driven cyberattacks.
- Effective defense increasingly depends on real-time visibility, continuous monitoring, and enforced AI governance, particularly around where AI tools interact with sensitive data.
- Organizations that fail to close these gaps face a higher risk of severe, data-driven ransomware incidents.

2025 Synopsis:

In 2025, AI transformed cybercrime, enabling faster, more autonomous ransomware and making data theft the primary objective. As enterprises adopted AI without governance, attackers exploited blind spots, increasing breach frequency, extortion pressure, and overall organizational impact.

AI Predictions For 2026

The Rise Of Shadow AI And Data Risk

Artificial intelligence is redefining the cybersecurity landscape, acting both as a driver of innovation and an emerging source of risk. While enterprises are rapidly adopting AI tools for efficiency and scale, this acceleration has introduced a new security gap: Shadow AI. In 2026, this duality will reach a breaking point, and organizations must find a way to harness AI's power without losing control of their data.

1 Shadow AI Is Creeping In As A Top Enterprise Threat

While organizations often look outward for cyberthreats, some of the most serious risks are emerging internally. Shadow AI, defined as unauthorized and unmonitored AI tools used by employees, is becoming an escalating security concern. Generative AI is now embedded in everyday work, yet many tools operate beyond the visibility of IT and security teams, quietly processing sensitive data through extensions and plug-ins.

Our research shows that nearly half of employees, 49%, use AI tools at work without employer approval, often with little understanding of how their data is stored or reused. Despite these risks, 71% believe the productivity benefits outweigh potential data privacy concerns.

The result is a growing governance gap where intellectual property, customer data, and trade secrets may be exposed indefinitely. In the year ahead, organizations will need to enforce stronger AI governance, backed by continuous oversight and monitoring, or risk severe security consequences.

Shadow AI Will Be A Risk Multiplier

In addition to increasing cyber risk, Shadow AI also drives up the cost of security failures. When sensitive data leaks through unsanctioned tools, tracing the path of exposure becomes extremely difficult. This leaves organizations unsure where their information is stored and who can access it.

IBM research shows that breaches involving unmanaged AI tools add an average of $670,000 to the total cost of an incident. This figure is likely to rise in 2026 as Shadow AI spreads deeper into enterprise systems. Preventing these silent leaks requires visibility. Organizations must understand where AI tools interact with data, define clear boundaries for approved tools and data sharing, and apply continuous monitoring to detect data exfiltration early.

AI Turns Data Exfiltration Into A Precision Weapon

Ransomware has continued to evolve, with data theft overtaking encryption as the primary objective. Our research shows that approximately **96% of publicized ransomware attacks now involve data exfiltration**.

Artificial intelligence is driving the next phase of this evolution, enabling faster and more targeted attacks. Machine learning models can analyze stolen data to identify high-value targets, while commercially available AI video tools can produce convincing deepfakes and large language models can generate highly tailored phishing emails. As a result, even small or inexperienced groups can now operate at a level once limited to sophisticated crime syndicates.

AI is also accelerating the rise of polymorphic malware that adapts to defenses in real-time. This will lead to more ransomware attacks that evade detection and exfiltrate data before they can be stopped. The most effective defense will be real-time visibility, allowing organizations to identify malicious activity and attempted data theft before damage occurs.

SIEM Gives Way To Prevention And AI Driven Defense

Security Information and Event Management (SIEM) systems have been the backbone of enterprise defense for years, but they are reaching their limits as the speed and scope of incoming threats increase.

SIEMs are costly, complex, and reactive, and their focus on collecting alerts long after the damage is done will be less relevant in 2026 as the focus shifts from post-incident forensics to prevention.

AI will drive this change, enabling systems that recognize abnormal behavior and stopping attacks as they happen. By blocking unauthorized data transfers and automating response, prevention-first models will replace endless alert triage and win back valuable time for security teams.

10

Conclusion

The data in this report underscores a fundamental shift in the ransomware threat landscape. In 2025, ransomware evolved into a highly efficient, AI enabled data theft and extortion model, with attackers prioritizing speed, scale, and stealth over disruption. At the same time, unmanaged AI adoption inside organizations has introduced new and largely invisible data exposure pathways, turning Shadow AI into a significant risk multiplier. Together, these forces are reshaping cyber risk in ways that traditional, reactive security models can no longer address.

As organizations look toward 2026, incremental improvements to detection and response are not enough. Security leaders must take decisive action to prevent data exfiltration at every stage of an attack. This means shifting from perimeter-centric and alert-driven defenses to prevention-first architectures that provide real-time visibility and control over outbound data flows, across endpoints, networks, cloud services, SaaS platforms, and AI tools. It also requires enforcing clear AI governance, closing blind spots created by Shadow AI, and ensuring that sensitive data cannot leave the organization without authorization.

Ransomware, insider threats, supply-chain compromise, and AI driven attacks are no longer separate challenges. They are different expressions of the same underlying risk: loss of control over data. Organizations that act now to implement continuous, automated data exfiltration prevention will be better positioned to reduce extortion leverage, limit regulatory and reputational damage, and maintain operational resilience in an increasingly hostile threat environment. Those that delay risk facing faster, more autonomous attacks that leave little time to respond, and even less margin for error.

About BlackFog

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 on 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 the BlackFog Console over the specific report period January - December 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®

AIDX

AI Security For AI Threats

Experience the next generation of cybersecurity with **BlackFog's ADX Product Suite**. With ADX at the core of unified security, advanced AI delivers real-time protection against data exfiltration, ransomware, and Shadow AI. Safeguard your data with proactive defense, intuitive intelligence, and adaptive security.

AIDX Protect | AIDX Vision | AIDX Instinct | AIDX Agility | AIDX Defend

blackfog.com

BLACKFOG®

Follow Us

Award-winning Technology

Contact us for a demo

Start your free trial

Visit blackfog.com