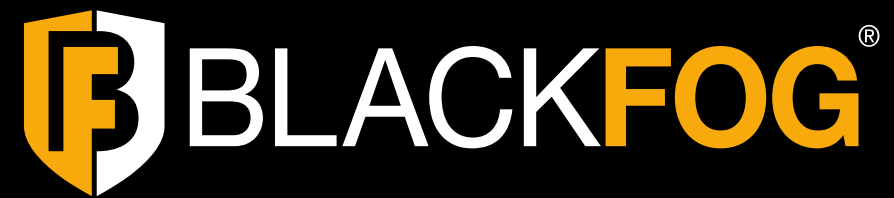


BLACKFOG.COM



The State of Ransomware

Q3 | 2025

FIGURES UP TO THE END OF Q3, 2025

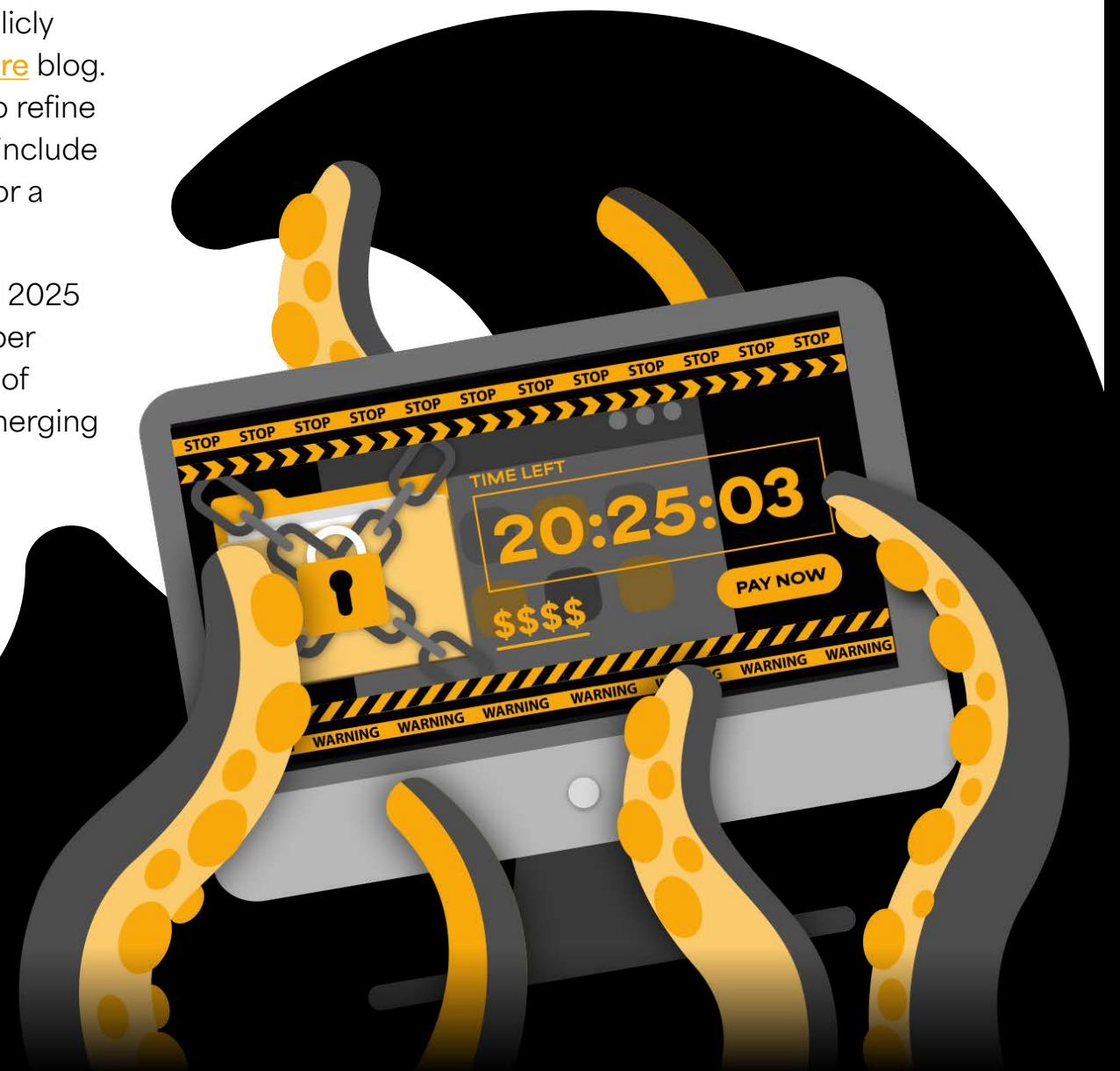


Introduction

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

Since 2020, BlackFog has been tracking and documenting publicly disclosed ransomware attacks through our [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.



Q3 | 2025

The Unstoppable Trend: Ransomware Sets Fresh Records in Q3

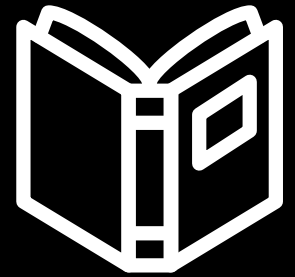
Publicly disclosed ransomware attacks continued their record-setting pace in Q3 2025, with 270 reported cases. This figure marks a 36% increase compared to the same quarter in 2024.

Each month of the quarter set a new benchmark. July led with a sharp 50% year-on-year surge, followed by August with a 37% increase, and September with a 27% rise in reported attacks.

The healthcare sector once again bore the brunt, experiencing 86 attacks, which accounted for 32% of all incidents. Government and technology sectors ranked next, each reporting 28 attacks. Together, these three industries represented more than half (53%) of all publicly disclosed ransomware activity during the quarter.

In total, 54 ransomware groups were linked to attacks in Q3. For the second consecutive quarter, **Qilin** emerged as the most active group, responsible for 20 incidents. Notably, approximately 40% of reported attacks have not yet been attributed to any known ransomware group.

Data theft remained the dominant tactic, with 96% of all disclosed cases involving data exfiltration, marking the highest rate recorded to date.

**“**

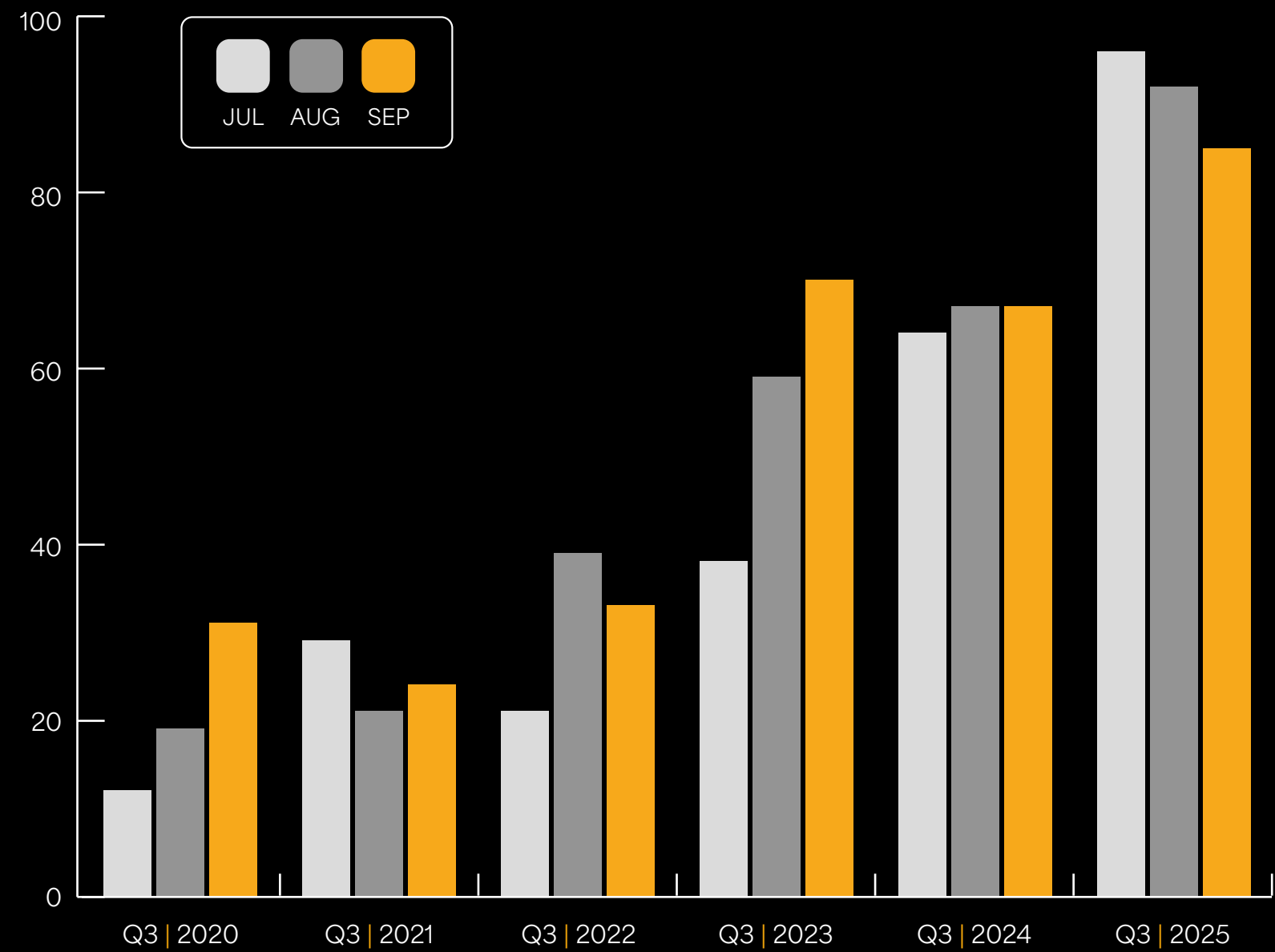
The **healthcare sector** once again bore the brunt, experiencing **86 attacks**, which accounted for 32% of all incidents.”





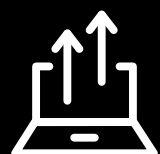
Q3 | 2025 YOY

Disclosed Ransomware Attacks By Month



	TOTAL	INCREASE YOY
Q3 2020	62	
Q3 2021	74	↑ 19%
Q3 2022	93	↑ 26%
Q3 2023	167	↑ 80%
Q3 2024	198	↑ 19%
Q3 2025	270	↑ 36%

DID YOU KNOW?



A new record for **data exfiltration** with

96%

of all attacks now involving **data theft**



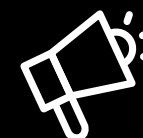
Q3 attacks have surged

335%

SINCE 2020



Between July and September, **publicly disclosed attacks** were attributed to **54 ransomware groups**.



107 attacks were left unclaimed, making up 40% of all incidents.



Companies in **35 countries** reported ransomware attacks this quarter, showing its true global reach.



For the second straight quarter, **education** dropped out of the top three targeted industries.

Q3 | 2025

The Hidden Majority: 85% Of Ransomware Attacks Stay In The Shadows

In Q3 2025, an estimated 1,510 ransomware attacks went unreported, representing a 21% increase compared with the same period in 2024.

The lack of transparency remains a critical challenge, with nearly 85% of all ransomware incidents not disclosed publicly. To put this into perspective, for every 100 attacks, only 15 are publicly reported, underscoring a persistent and troubling reporting gap.

Qilin was the most active ransomware group within this segment, responsible for 16% of cases. **Akira** and **Inc** followed, with 139 and 111 victims respectively. The quarter also saw the emergence of 18 new ransomware groups, several of which were linked to high-profile incidents targeting large organizations.

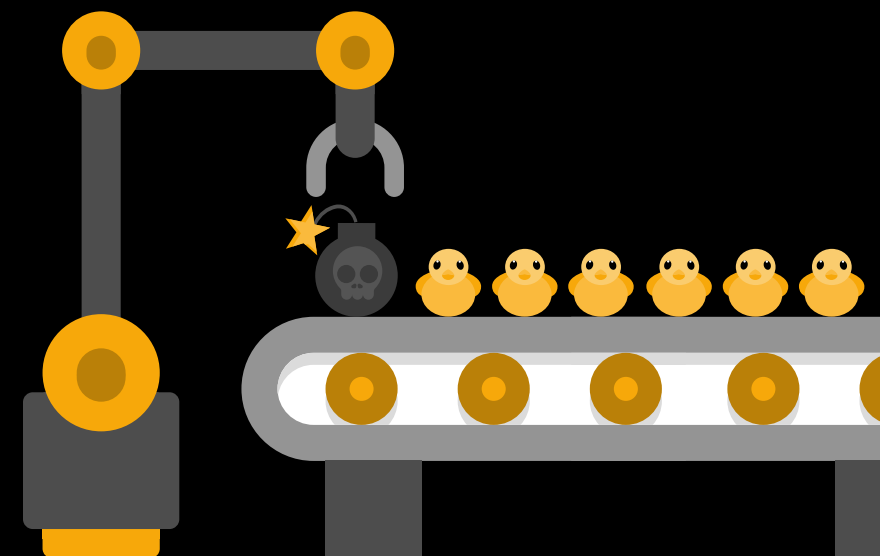
By industry, manufacturing was hit hardest, accounting for 22% of all undisclosed attacks. The services sector followed closely with 333 incidents, while construction entered the top three for the first time, suffering 143 attacks between July and September.

Data theft remained a hallmark of these attacks. Across 449 dark web victim listings where details were available, the average data volume exfiltrated was 527.65GB. Notably, only 3% of undisclosed cases included an upfront ransom demand, as gangs increasingly prefer to negotiate directly with victims.



“

By industry,
manufacturing
was hit hardest,
accounting for
22% of all
undisclosed attacks.”

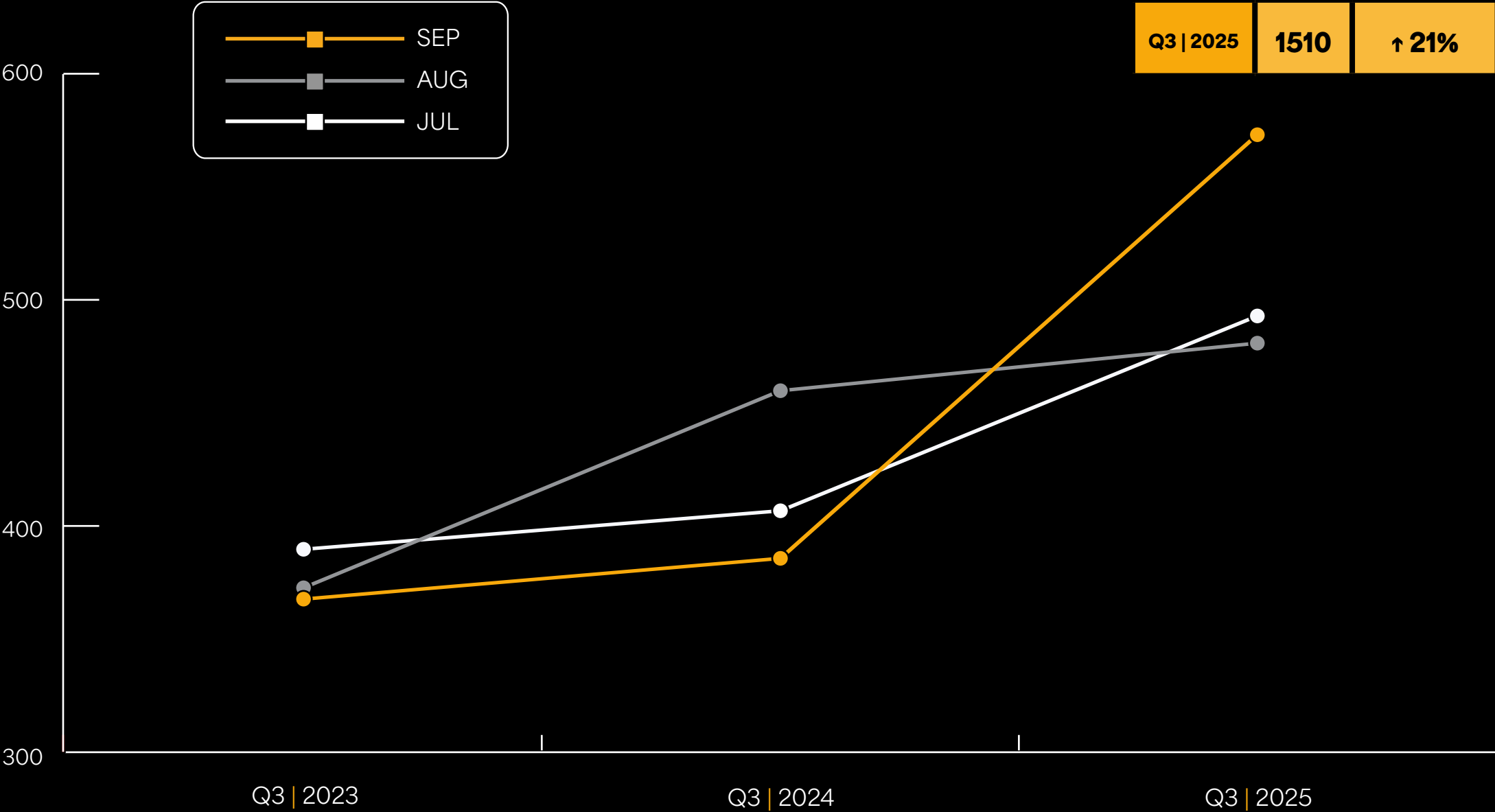




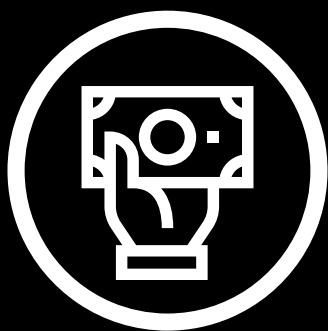
Q3 | 2025 YOY

Undisclosed Ransomware Attacks By Month

	TOTAL	INCREASE YOY
Q3 2023	1131	
Q3 2024	1252	↑ 11%
Q3 2025	1510	↑ 21%



DID YOU KNOW?



DEVMAN
demanded
\$91 million
from
Shimao Group,
the largest
ransom in Q3.



The **legal sector**
recorded **79 attacks**, its highest
level yet.



80 groups published
victims on dark
web leak sites.



Ransomware groups
targeted organizations
in **93 countries**
worldwide.

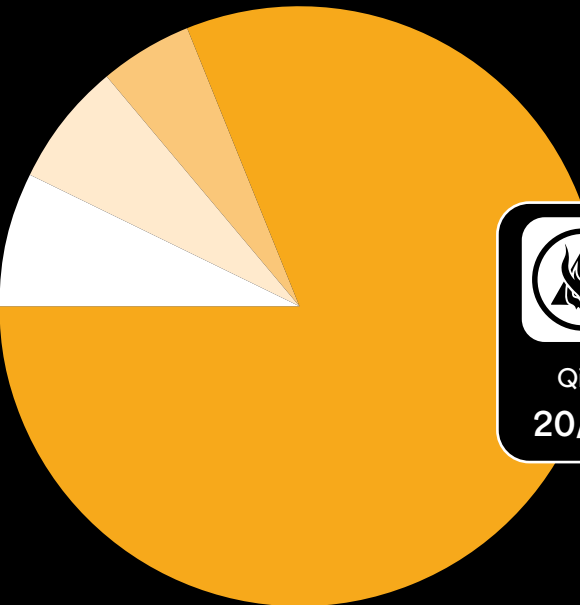






18 new ransomware groups appeared
during Q3.



Q3 | 2025

Disclosed Ransomware Attacks By Group



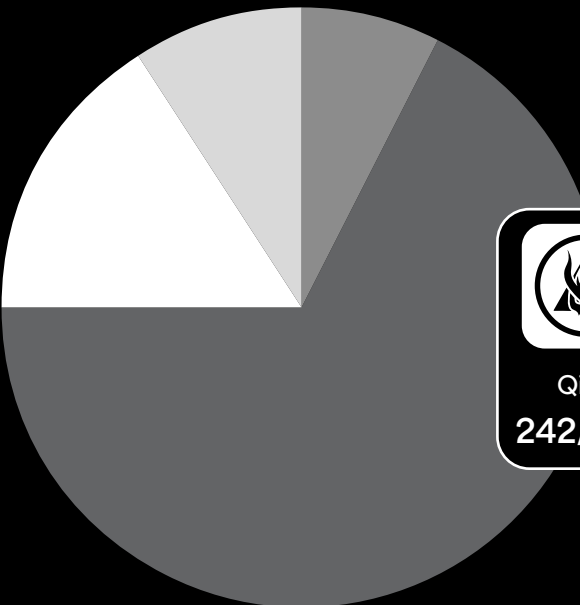
			
Qilin	INC	Everest	Other
20/7%	18/7%	13/5%	219/81%





270
DISCLOSED
ATTACKS



Q3 | 2025

Undisclosed Ransomware Attacks By Group



			
Qilin	Akira	INC	Other
242/16%	139/9%	111/7%	1018/67%

1510
UNDISCLOSED
ATTACKS

FEATURED GANG



DEVMAN: A New Ransomware Offshoot Making Global Headlines

DEVMAN is a newcomer to the ransomware landscape, derived from the **DragonForce/Conti** lineage, but it has already made headlines with bold extortion attempts. While the malware shows rough edges, sometimes encrypting its own ransom note and failing to display warnings on newer Windows systems, it remains highly disruptive. Victims see their files renamed with the .DEVMAN extension, and the group pressures them via its leak site, Devman’s Place.

In just months, **DEVMAN** has claimed 19 attacks across Asia, Africa, Europe, and Latin America. Standout cases include a July 2025 attack on PT.El.COM with a \$4 million ransom, an earlier strike on a French transport company, and most dramatically, a \$91 million demand against the Chinese real estate giant Shimao Group, one of the largest ransomware demands seen this year.

These incidents underline how even “immature” ransomware strains can quickly scale into global threats. **DEVMAN**’s trajectory shows how rebranded or derivative groups can leverage aggressive extortion tactics to target both mid-sized firms and multinational enterprises, forcing defenders to treat emerging names with the same seriousness as established gangs.

Q3 | 2025 Top 5 Reported Attacks

Q3 saw ransomware and data breaches disrupt airlines, governments, and critical industries worldwide, underscoring the widening scale, cost, and human impact of cyber incidents across sectors.



1

In July 2025, [Qantas](#) disclosed that attackers had gained access to a third-party customer service platform used by one of its call centers, compromising service records of about six million customers. The exposed data reportedly included names, email addresses, phone numbers, dates of birth, and frequent flyer numbers. Importantly, no credit card, passport, or login credential data were held in the breached system. Qantas said it immediately contained the system, notified regulatory and law enforcement bodies (such as the Australian Cyber Security Centre and AFP), and is investigating the scope of exfiltration. The airline also revealed it has been contacted by a potential cybercriminal demanding ransom or extortion, although it has not publicly confirmed any demand or attribution. In response, the Qantas board [imposed a 15% reduction in short-term bonuses](#) for the CEO and senior executives to reflect accountability for the breach; for CEO Vanessa Hudson, that penalty amounted to about A\$250,000.

2

In August 2025, the [Pennsylvania Office of Attorney General \(OAG\)](#) was hit by a ransomware cyberattack beginning on Aug 11, 2025, which encrypted files and took down systems including its website, email, and phone lines across 17 offices statewide. **INC** ransomware group claimed responsibility, stating it exfiltrated 5.7 TB of data and posting sample documents to support its claim. The OAG refused to make any ransom payments. The operational fallout included forced workarounds for approximately 1,200 staff, delays in civil and criminal litigation (some courts issued case extensions), and continued uncertainty over what kinds of files or sensitive data may have been exposed.

Q3 | 2025 Top 5 Reported Attacks

3

[Jaguar Land Rover \(JLR\)](#) was hit by a cyberattack that shut down global IT systems and halted UK factory production, crippling dealer and parts operations. The disruption is expected to cost the company tens of millions of pounds per week, with reports suggesting losses could reach £1 billion if outages extend into November, compounded by the lack of confirmed cyber insurance coverage. JLR initially said no customer data was stolen but later admitted “some data” was affected. A group calling itself [Scattered Lapsus\\$ Hunters](#) claimed responsibility, citing ransomware, though attribution remains unconfirmed. The attack underscores the severe financial and operational risks ransomware poses to manufacturing supply chains.

4

In September 2025, the preschool chain [Kido International](#) was breached by ransomware group **Radiant**, which claimed to have exfiltrated data on over 8,000 children across its UK sites. To prove their access, **Radiant** published profiles of ten children, complete with names, photos, home addresses, and family contact details, and threatened to release full profiles of 30 children plus data for 100 employees (including billing, safeguarding and staff records). Kido acknowledged a cyber incident, engaged forensic experts, and informed regulators and affected families. Law enforcement (Metropolitan Police) and the UK’s Information Commissioner’s Office are investigating, and the attack has drawn sharp criticism for its targeting of highly sensitive children’s data.

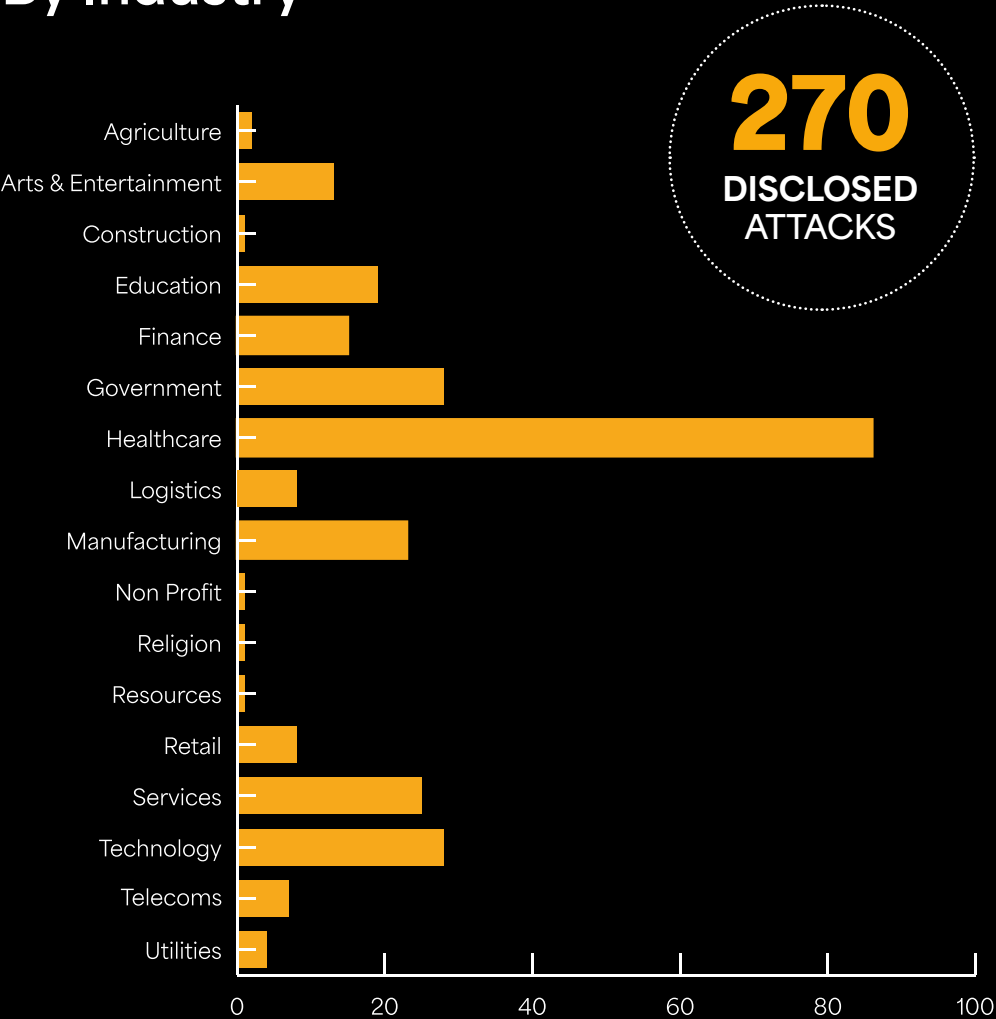
5

In mid-September 2025, [Collins Aerospace](#), a subsidiary of RTX providing the MUSE / vMUSE shared check-in, boarding, and baggage software to European airports, was hit by a ransomware attack that knocked out electronic check-in at major hubs like Heathrow, Brussels, Berlin, and Dublin. With kiosks, bag drops, and boarding systems disabled, affected airports switched to manual processes, triggering long queues, widespread delays, and flight cancellations. Brussels Airport even asked airlines to cancel roughly half of its departures on one day to manage congestion. Authorities later arrested a suspect in the UK under the Computer Misuse Act in connection with the incident. Collins and RTX have characterized the event as a “cyber related disruption” of their MUSE systems and are working to restore functionality, while regulators and cybersecurity agencies across Europe continue investigating causation and attribution.



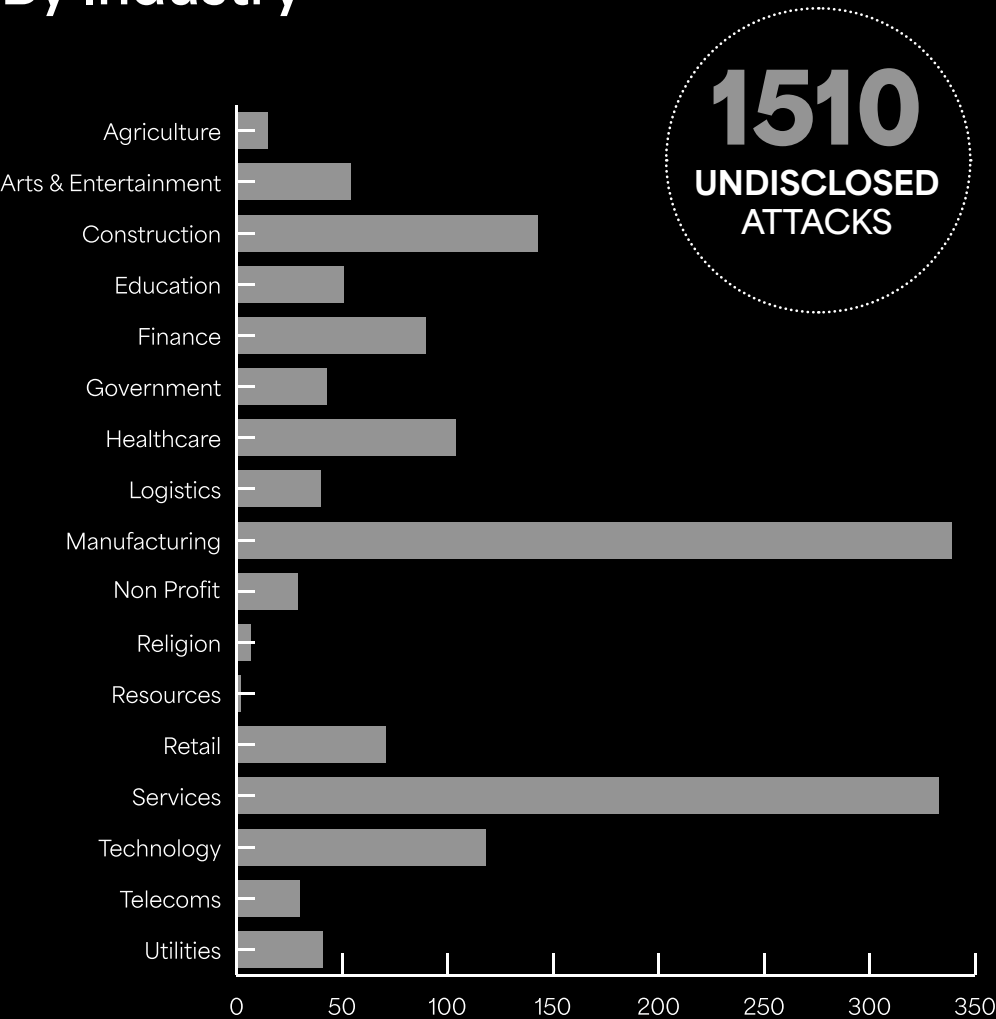
Q3 | 2025

Disclosed Ransomware Attacks
By Industry



Q3 | 2025

Undisclosed Ransomware Attacks
By Industry



How Ransomware Gangs Exploit Geography For Maximum Impact

Ransomware campaigns are increasingly shaped by geography. Attackers no longer cast wide nets but focus on regions where the rewards are higher and the risks lower. Economic conditions, language familiarity, and legal protections all influence where they strike, turning specific countries and industries into repeat targets.

Targeting By Region

Ransomware actors don't strike randomly. They focus on geographies where the payoff is higher because victims hold valuable data, disruption creates pressure to pay, or operational factors like language and legal risk work in their favor. In Q3 2025, gangs reported victims in 93 countries.

Focusing on one sector in a single country lets attackers scale quickly. Once they identify entry points and common vendors, the same playbook can be reused across many organizations. **Qilin**, for example, launched a coordinated campaign against multiple South Korean asset-management firms, leaking stolen data under a "Korean Leak" label.

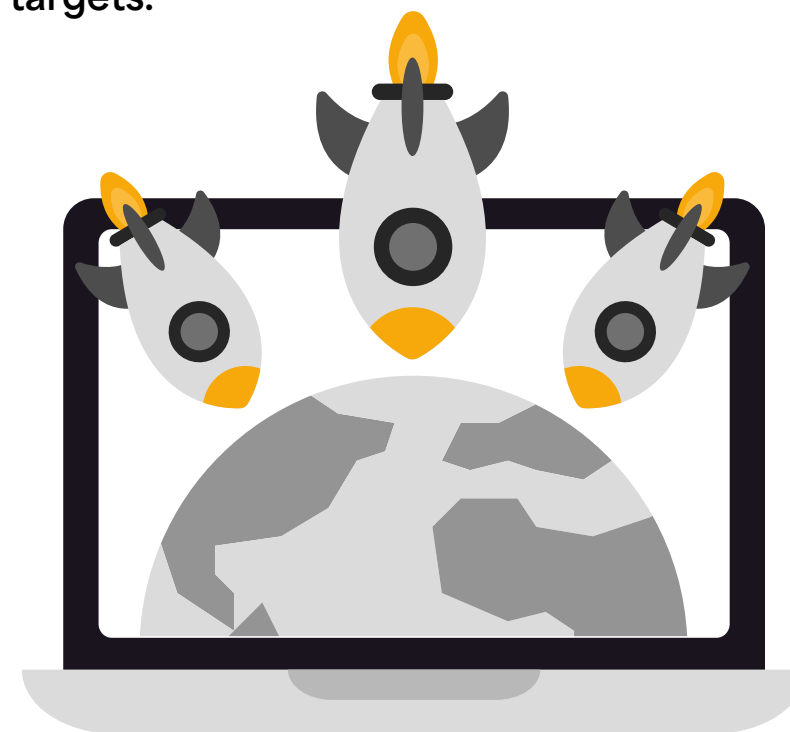
Geographic targeting offers three main advantages. First, economic leverage: financial organizations hold sensitive client data, increasing ransom pressure. Second, efficiency: attackers can reuse local phishing

lures, exploit regional software weaknesses, and use language familiarity for better social engineering. Third, supply-chain compromises: breaching one cloud provider or vendor serving many local firms multiplies impact, as seen in South Korea.

Regional Risk And Geopolitical Influence

Some groups have concentrated on Latin American governments and infrastructure. Agencies and utilities hold sensitive records and operational data, and weaker regional defenses make intrusions easier. For affiliates in permissive jurisdictions, legal risks are minimal, while striking government entities carries both financial and geopolitical impact.

This example highlights how geopolitics and safe-harbor protections influence targeting. Limited cross-border enforcement lowers risks, while some actors blend profit with political or symbolic aims.



A Business Model Built On Geography

Finally, ransomware business models reinforce geographic focus. Ransomware-as-a-service, affiliate networks, and leak markets allow groups to scale targeted campaigns. These geographically targeted attacks show how ransomware groups maximize returns by concentrating where leverage, disruption, and efficiency align.

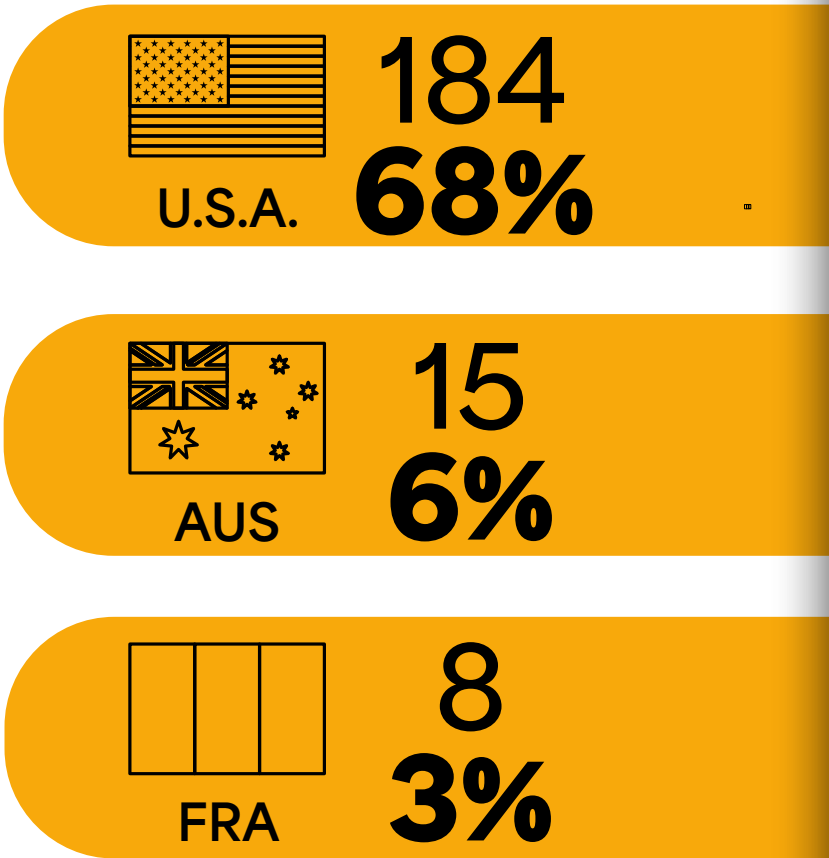


Q3 | 2025

Top 3 Targeted Countries



DISCLOSED



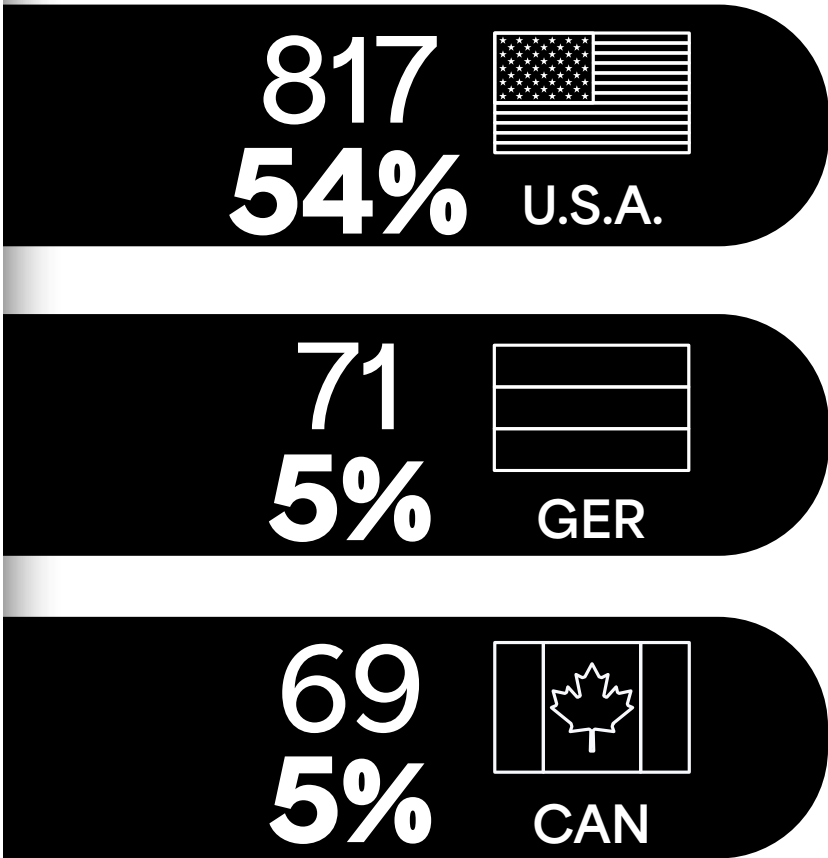
01

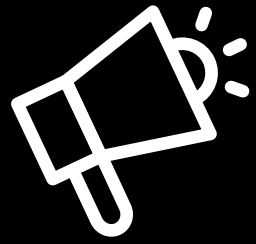
02

03



UNDISCLOSED





In the News

In Q3, two key stories highlight ransomware's changing landscape: its growing psychological toll on defenders and the rise of data exfiltration as the attacker's weapon of choice.

The Internal Blast Radius Of Ransomware Attacks: Why Cyber Resilience Must Start With People

Ransomware incidents do not only disrupt systems and compromise data, they also have a cascading effect on the internal health of an organization. When attackers penetrate defenses, the consequences extend beyond financial costs and downtime; employees face immense pressure, morale suffers, and security teams often experience burnout. This "internal blast radius" highlights the hidden costs of an attack, where the psychological and operational strain on staff can weaken resilience long after systems have been restored. Building cyber resilience, therefore, requires more than backups and detection tools and must include measures to support the human side of defense.

Our CEO Darren Williams points out that organizations often underestimate the human toll of these attacks. He stresses that attrition among security professionals, the erosion of institutional knowledge, and the mental stress placed on defenders can leave businesses vulnerable even after the technical aspects are addressed. The view is that resilience should be holistic, balancing the restoration of systems with the care and retention of the people who protect them. In doing so, companies can strengthen their ability not only to recover from ransomware, but to withstand its long-term impacts.

Post-Modern Ransomware: When Exfiltration Replaces Encryption

Ransomware has evolved: whereas earlier attacks often focused on encrypting data and systems, today's most potent threats begin with exfiltration. Attackers steal critical data first, whether customer records, financials, intellectual property, and then use that as leverage, threatening to leak, sell, or publicly expose it if demands aren't met. In this "post-modern" phase, encryption becomes a supporting act rather than the main weapon, as theft offers faster, irrevocable damage. Adding fuel to this shift is the integration of AI, which accelerates operations, automates deception, and magnifies the psychological pressure on defenders to concede.

Darren Williams, our CEO, highlights that organizations must get far more proactive in detecting signs of exfiltration, patterns like unusual outbound traffic, anomalous MFA behaviors, or sudden file movement, because by the time systems are encrypted, the damage is often irreversible. He also warns that cyber resilience needs to incorporate psychological and operational safeguards: defenders already under strain can be pushed over the edge by the stress, blame, and fatigue that these nuanced attacks inflict. In short, true defense now demands equal focus on protecting data and preserving the people who defend it.



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 96% of all attacks now 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

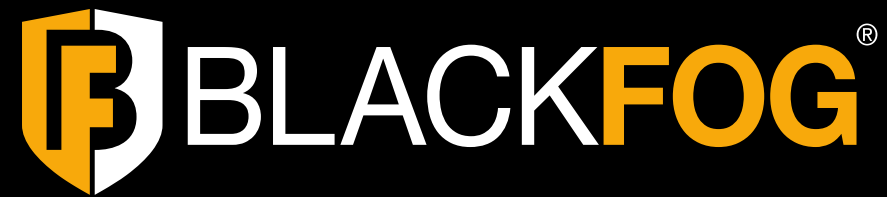
Methodology

This report was generated in part from data collected by BlackFog Enterprise over the specific report period July–September 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.



Follow Us



Award-winning Technology



Contact us for a demo

Start your free trial

Visit blackfog.com

All contents copyright © 2025 BlackFog, Inc. All rights reserved. The BlackFog logo and name are trademarks of BlackFog, Inc. All other trademarks are the property of their respective owners.

Except as specifically stated herein, none of the material may be copied, reproduced, distributed, republished, downloaded, displayed, posted, or transmitted in any form without authorized, prior written permission from BlackFog, Inc. Permission is granted for you to make a single copy of this document solely for informational uses within your organization, provided that you keep intact all copyright and other proprietary notices. No other use of the information provided is authorized.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners. The information contained in this document represents the current view of BlackFog, Inc. on the issues discussed as of the date of publication.