RansomStop

2025 Year-End Report

RANSOMWARE IN 2025:

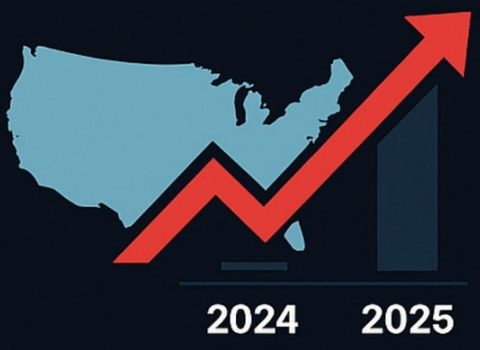
A YEAR OF ESCALATION AND ADAPTATION

Key Findings

Key Findings

34%
YoY increase

126%
Q1 surge



149%
U.S. spike

4,701
confirmed incidents

11,000
daily attempts (projected)

Global ransomware incidents surged 34% in the first three quarters of 2025 compared to the same period in 2024, with approximately 4,701 confirmed cases The data reveals an alarming acceleration of ransomware activity throughout 2025. From January through September, confirmed incidents reached 4,701 globally, a 34% increase over the same period in 2024. The most striking observation is Q1’s 126% year-over-year surge, establishing 2025 as the most aggressive opening quarter on record. In the United States alone, reported attacks jumped 149% in the first five weeks, totaling 378 incidents. This trend continued with monthly average victims in Q3 reaching 535 per month, representing a 25% increase from Q3 2024. Projections suggest approximately 11,000 daily attack attempts globally by year-end, a 3,500% increase over five years.

Ecosystem Fragmentation & Perpetrator Tactics

The RaaS model underwent dramatic fragmentation in 2025. An unprecedented 85 active data leak sites emerged in Q3, with 45 new groups launching attacks throughout the year. This decentralization followed significant law enforcement disruptions to major platforms including RansomHub, 8Base, and BianLian, forcing affiliates to migrate to smaller, independent operators. Despite fragmentation, elite threat actors maintained dominance:

- ***Qilin***: 75 average monthly victims in Q3 (up from 36 in Q1), with an 81-attack peak in June
- ***Akira***: Sustained high double-extortion activity with 9.7% growth
- ***INC Ransom***: 39 monthly victims, intensifying Canadian operations
- ***Play***: 33 monthly victims despite a 31.8% decline from previous periods
- ***LockBit***: Resurgent with version 5.0 launch in September, featuring faster encryption and revised victim disclosure practices

AI emerged as the game-changer. Threat actors increasingly automated attacks from vulnerability scanning through exploitation, enabling encryption in as little as 90 seconds. One documented case involved a Chinese state-sponsored group using advanced AI to automatically attack 30 global organizations. This acceleration dramatically outpaces human security responses, with 76% of organizations struggling to match AI-powered attack speed.

Advanced evasion tactics proliferated, including:

- EDR-killing tools (EDRSilencer, EDRSandblast, EDRKillShifter)
- Living off the Land (LOTL) techniques via legitimate applications
- Double and triple extortion combining encryption with data theft
- Encryption-less extortion focusing purely on data exposure threats
- Compromised credentials initiating 23% of attacks

Major Incidents and Sectors

Ingram Micro

July 2025

Manufacturing

Global operational disruption
3.5 TB stolen

DaVita

Mar–Apr 2025

Healthcare

2.7M patient records affected

PowerSchool

Dec 2024–Jan 2025

Education

62M user accouns compromised

Jaguar Land Rover

Late Summer 2025

Manufacturing / Automotive

Supply-chain disruption,
national economic impact
£1.9B UK economic impact;

In 2025, ransomware attacks increasingly resulted in large-scale operational disruption, data exposure, and cascading economic impact across multiple sectors. Several incidents stood out due to their scope, cost, and downstream consequences, particularly in manufacturing, healthcare, education, and critical infrastructure. These incidents demonstrate a shift from isolated breaches toward events with systemic and national-level implications.

Notable incidents include:

- ***Ingram Micro (July, SafePay)***: Disrupted global operations and logistics, with 3.5 TB of data stolen and estimated daily losses of $136 million
- ***DaVita (March–April, Interlock)***: Impacted 2.7 million patients, resulting in $13.5 million in recovery costs
- ***PowerSchool (Dec 2024/Jan 2025)***: Impacted 62M users; $2.85M paid, followed by district extortion
- ***Jaguar Land Rover (Late Summer)***: The cyberattack cost the UK economy an estimated £1.9 billion ($2.55 billion), making it the costliest single cyber event in UK history. The UK government provided a £1.5 billion ($2 billion) loan guarantee to support JLR and third-party companies affected by the breach

This cluster of incidents highlights the increasing tendency for ransomware events to escalate beyond the initial victim organization, affecting national economies, healthcare delivery, and global supply chains.

Major Incidents Table

Organization	Timeframe	Sector	Impact Summary	Estimated Cost / Impact
Ingram Micro	July 2025	Manufacturing / Distribution	Global operational disruption, 3.5 TB data exfiltrated	~$136M daily losses
DaVita	Mar–Apr 2025	Healthcare	2.7M patient records affected, operational downtime	~$13.5M recovery cost
PowerSchool	Dec 2024–Jan 2025	Education	62M users impacted, ransom paid, secondary extortion	Multi-million USD
Jaguar Land Rover	Summer 2025	Manufacturing / Automotive	Supply-chain disruption, national economic impact	£1.9B ($2.55B); £1.5B loan guarantee

Economic and Human Impact

$1.5M
average recovery cost

$1M
average ransom payment

53%
of victims negotiated

Vulnerability exploitation

Skill shortages

The financial toll of ransomware reached critical levels.

Direct Costs:

- Average recovery costs: $1.5 million per incident (excluding ransoms)
- Average ransom payments: $1 million
- 53% of victims negotiated less than the initial demand
- Global costs projected to exceed $265 billion annually by 2031 Repeat Attack Risk
- 83% of organizations that paid ransoms faced subsequent attacks
- 93% reported that their data was stolen regardless of whether encryption occurred
- Organizations that paid were no more protected than those that refused Organizational Impacts
- Average recovery time: 3+ weeks of operational disruption
- 63% of attacks attributed to skill shortages in security teams
- 39.4% cited insufficient staffing as a root cause
- Significant employee burnout from extended recovery operations
- Loss of customer trust and market confidence

Root Causes Identified

- Exploited vulnerabilities (top factor)
- Skill shortages in cybersecurity
- Insufficient security staff
- Inadequate vendor management
- Unprotected assets (hypervisors, NAS, containers)

Key Takeaways for Organizations

Automation

Supply chain risk

Double-extortion

Ecosystem fragmentation

Tooling evolution

Detection priorities

Sector modeling

Insurance gaps

Why Traditional Defenses Fall Short

Organizations continue to rely solely on endpoint detection and response (EDR), anti-virus, and backup solutions. While necessary, these tools operate at detection boundaries rather than preventing encryption outcomes. Attackers exploit architectural limitations by:

- Modifying ransomware to appear novel to signature-based detection
- Using EDR-killing tools to disable security before execution
- Targeting unprotected assets like hypervisors, containers, and network-attached storage
- Leveraging legitimate applications for malicious purposes
- Focusing attacks on data rather than entry points

The AI Acceleration Challenge 2025 demonstrated that AI fundamentally changes the ransomware threat model. Threat actors now employ AI to:

- Accelerate attacks from weeks to 90 seconds
- Automate vulnerability discovery and exploitation
- Scale attacks to everyday businesses, not just high-profile targets
- Enable less-skilled actors to conduct sophisticated operations
- Outpace traditional human-based security responses 89% of security leaders now view AI-powered defenses as essential to future operations.

Immediate Priorities for 2026

1. Implement real-time encryption detection and halting capabilities
2. Conduct comprehensive asset inventory (especially critical infrastructure)
3. Strengthen vendor management and supply chain security
4. Deploy AI-powered threat detection systems
5. Establish incident response capabilities that operate faster than encryption
6. Invest in security team recruitment and retention
7. Conduct regular backup restoration testing
8. Implement data-centric protection strategies

Outlook for 2026

- Automation
- Leak site growth
- Insurance shifts
- Nation-state expansion
- Law enforcement strategy
- Modular RaaS
- Board-level risk
- Sector laundering
- Threat actor collaboration

2025 established definitively that ransomware has become a critical business continuity threat, not merely a cybersecurity issue. The convergence of AI acceleration, ecosystem fragmentation, and supply chain vulnerabilities signals continued escalation. Expected 2026 Trends:

- Further AI integration enabling attacks at scale
- Continued RaaS ecosystem fragmentation with 100+ active groups
- Supply chain attacks targeting vendors serving critical sectors
- Encryption-less extortion gaining prominence
- Targeting of unprotected cloud environments and serverless architectures
- Geographic diversification of threat actors
- Increased nation-state involvement in ransomware operations

Organizations must fundamentally rethink their defensive posture. Detection-based tools, while necessary, are insufficient. The only effective defense combines:

- Vulnerability management and patching
- Real-time encryption detection and halting
- Data-centric protection strategies
- AI-powered threat intelligence
- Incident response capabilities that operate at machine speed
- Those organizations that implement these comprehensive strategies will dramatically reduce their ransomware risk in 2026 and beyond
- A staggering 126% increase in Q1 2025 marked the most aggressive start to any year on record
- 85 active data leak sites and 45 new groups emerged, fragmenting the RaaS ecosystem
- 76% of organizations report they cannot match the speed of AI-powered attacks
- Critical infrastructure sectors accounted for 50% of all attacks
- Average recovery costs reached $1.5 million per incident
- Average ransom payments hit $1 million, though 83% of payers faced repeat attacks

Attack Volume & Trends

1,984
weekly attacks

23%
ransom pay rate

6,300
leak site cases exposed

76%
involved data theft

50%
targeted critical sectors

Insurance

Global Attack Volume

- 4,701 confirmed ransomware incidents occurred globally between January and September 2025 - a 34% increase over the same period in 2024
- By October 2025, 6,330 cases were exposed on dark web leak sites, up 47% from 4,293 in 2024
- Attack frequency reached 1,984 cyberattacks per week in Q2 2025, with ransomware accounting for a significant share
- By late 2025, global ransomware attempts hit 11,000 per day, marking a 3,500% increase over five years

Monthly Victim Trends

- In Q3 2025, new ransomware victims appeared at a rate of 520-540 per month, nearly double the rate from early 2024
- The average number of ransomware attacks per organization rose sharply, with some sectors experiencing one attack every few seconds globally

Payment Trends & Market Shifts

Payment behavior continues to fluctuate across regions and sectors, but attackers are maintaining leverage through data theft, multi-extortion tactics, and operational disruption.

Tactical Evolution

- 76% of attacks in Q3 2025 involved data theft prior to encryption, with pure data extortion campaigns rising
- Triple extortion tactics - combining encryption, data theft, and harassment - became more common
- Threat actors increasingly targeted cloud infrastructure, operational technology, and critical infrastructure sectors, which accounted for 50% of all attacks

Final Thoughts

Velocity, complexity, and economic impact surged in 2025.

Fragmentation and automation reshaped the ransomware ecosystem.

Detection and resilience are now critical for defenders.

About RansomStop

Stop ransomware.
Protect operations.
Empower defenders.

Next-generation ransomware intelligence and response

RANSOMSTOP

Final Thoughts

2025 marked a turning point in the ransomware landscape, not just in volume, but in velocity, complexity, and economic impact.

The fragmentation of threat actor ecosystems, rise of automation, and collapse of ransom payment rates signal a new era of cyber risk.

Organizations must evolve faster than attackers, with resilience, detection, and recovery capabilities that match the speed and scale of modern ransomware.

About RansomStop

RansomStop is an AI-powered ransomware detection and response platform built for speed, clarity, and control.

By operating at the speed of machine encryption, RansomStop detects and halts active attacks before damage occurs. This enables a fundamentally different approach that prevents rather than responds.

The platform combines real-time threat actor tracking, automated incident response, and strategic risk modeling to help organizations stay ahead of evolving ransomware threats.

For more information on 2025 threats and 2026 mitigation strategies, visit RansomStop.com

Our mission is simple:

Stop ransomware. Protect operations. Empower defenders.