KELA

National Security Report

Escalating Ransomware Threats to National Infrastructure

Table of Contents

Executive Summary

Ransomware has evolved from an enterprise risk into a strategic national security threat. Once driven primarily by profit, it is now used by organized cybercriminals and state-linked actors to disrupt critical infrastructure, destabilize economies, and erode public trust.

In 2025, half of all ransomware attacks worldwide targeted essential sectors such as manufacturing, healthcare, energy, transportation, and finance — revealing a clear shift from opportunistic crime to systemic disruption.

National Security Implications

The implications for national security are profound and impact many areas. For example,

ECONOMIC STABILITY:

Attacks against manufacturing and financial services can cripple production lines, disrupt trade, and erode market confidence.

PUBLIC HEALTH & SAFETY:

Healthcare systems, already strained, face direct risks to patient care. Transportation disruptions can cascade into broader infrastructure failures.

STRATEGIC RISK:

Repeated successful attacks erode trust in government and the private sector's ability to protect critical infrastructure.

The following report dives into the growing threat and spotlights the ransomware trends impacting the critical infrastructure.

Key Findings

SHARP RISE IN ATTACKS:

KELA observed 4,701 ransomware incidents between January and September 2025, a 34% year-over-year increase (YoY). Of these, 2,332 (50%) targeted critical infrastructure, up from 1,745 (54%) in 2024.

INDUSTRIAL AND ECONOMIC IMPACT:

Manufacturing was hit hardest, with attacks surging 61% (520 → 838 incidents YoY) — the steepest growth among all sectors. High-profile incidents included Jaguar Land Rover's global shutdown and Bridgestone's production disruptions, illustrating how ransomware can paralyze supply chains and economies.

FEW ACTORS, MAJOR DAMAGE:

Out of 103 active ransomware groups, just five (Qilin, Clop, Akira, Play, and SafePay) accounted for nearly 25% of global incidents, reflecting the growing professionalization of cybercrime through Ransomware-as-a-Service ecosystems.

U.S. CONCENTRATION:

The United States remains the epicenter of ransomware activity targeting critical infrastructure, accounting for roughly 1,000 incidents — 21% of all global attacks in 2025. This concentration underscores ransomware's dual motive: to maximize ransom profits in wealthier, digitally mature markets, while testing the resilience of industries central to U.S. national security and global supply chains.

Ransomware: A Strategic Weapon Against National Resilience

Ransomware epitomizes why these efforts are urgent. Once a financially motivated nuisance, ransomware has become a strategic weapon for both cybercriminals and hostile actors to target governments, industries, and even citizen accounts. In 2025, **half of all ransomware attacks struck** critical sectors — from manufacturing and healthcare to finance and transportation — demonstrating how adversaries exploit weaknesses in infrastructure to destabilize societies. This report examines the scope of ransomware activity, the industries and regions most at risk, and the threat actors driving these campaigns, underscoring why national cyber resilience must remain a cornerstone of modern security strategy.

When we look at critical sectors, we're specifically referring to: Manufacturing, Healthcare, Technology, Transportation, Financial Services, Government and Public Sector, Food, Energy, Telecom, Agriculture, Aerospace and Defense, and Utilities.

Scale of the Surge: Sectors Under Attack

Ransomware has evolved from a nuisance for individual organizations to a systemic threat to national resilience. Comparing year-over-year data, the scale of attacks targeting critical sectors is striking. KELA data showed:

2024 (Jan 1 – Sep 1)

3,219

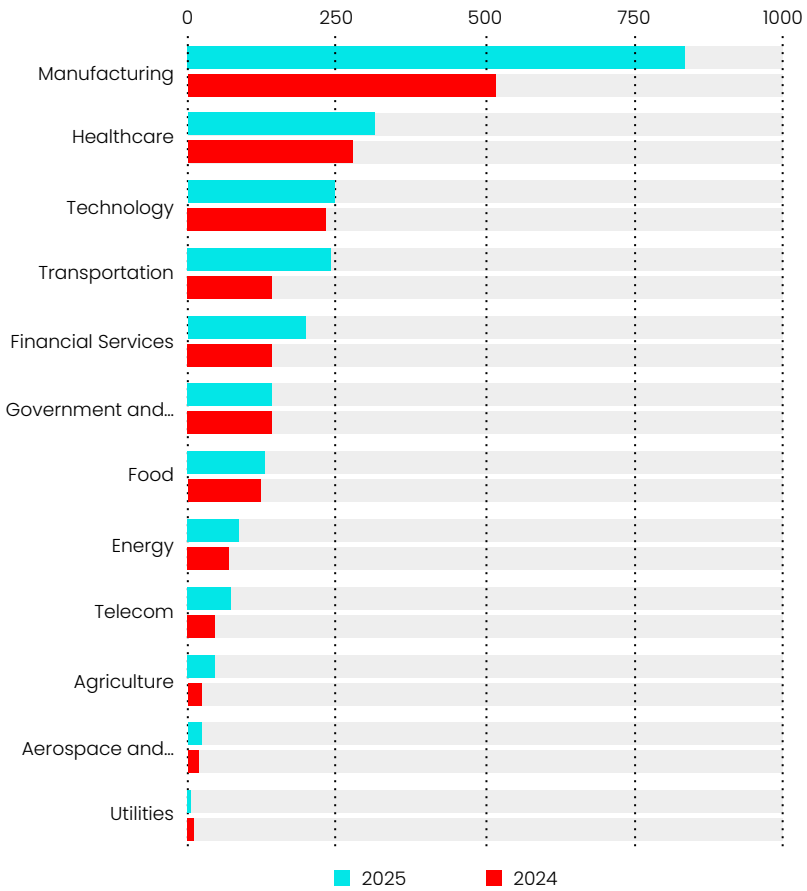
total incidents recorded, with **1,745 (54%)** hitting critical sectors.

2025 (Jan 1 – Sep 1)

4,701

ransomware incidents recorded, with **2,332 (50%)** targeting critical sectors such as manufacturing, healthcare, energy, transportation, and financial services.

Number of ransomware events targeting specific critical sectors in 2025 vs 2024



While the overall percentage of threats targeting the critical sector is just slightly lower, the overall number still shows a **34% increase in ransomware events against critical industries** in just one year. Manufacturing, healthcare, and technology stand out as the most targeted industries, with manufacturing seeing the steepest growth in 2025.

Ransomware attacks against the manufacturing sector surged from 520 incidents to 838, marking a 61% increase. This spike underscores how increasingly digitized and interconnected manufacturing systems have become prime targets. In fact, the IBM X-Force 2025 Threat Intelligence Index showed that manufacturing is the #1-targeted industry, four years in a row. Attackers exploit vulnerabilities in legacy operational technology, supply chain interdependencies, and high-cost downtime, knowing that disrupted production translates into immediate and serious financial consequences.

The most publicized incident came in early September when Jaguar Land Rover (JLR) was forced to shut down production globally—across the UK, Slovakia, China, India, and Brazil—after an attack claimed by the teenage hacker collective "Scattered Lapsus$ Hunters," significantly disrupting manufacturing and retail operations.

Another notable case involved Bridgestone, currently investigating a cyberattack affecting multiple manufacturing facilities in South Carolina and Quebec; although the responsible group hasn't been confirmed, speculation points again to the Scattered Lapsus$ Hunters alliance.

Together, these high-profile breaches underscore how ransomware actors increasingly view manufacturing not just as a means to ransom data, but as a path to critical leverage, knowing that even a short shutdown can ripple through entire industries and economies.

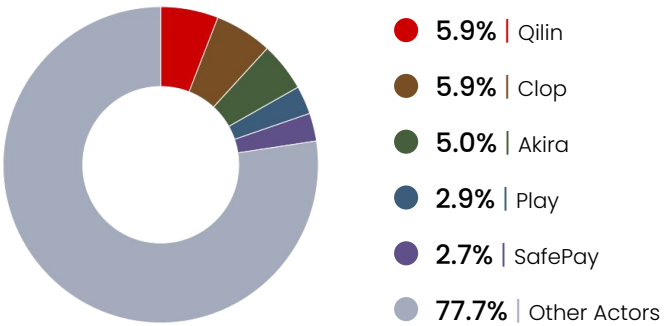
Threat Actors Driving the Surge

The escalation is orchestrated by a wide range of ransomware groups targeting critical infrastructure, with 103 distinct threat actors observed in 2025. However, activity is far from evenly distributed. A handful of groups — Qilin, Clop, Akira, Play, and SafePay — are driving a disproportionate share of incidents:

- **Qilin:** 248 incidents
- **Clop:** 246 incidents
- **Akira:** 209 incidents
- **Play:** 120 incidents
- **SafePay:** 115 incidents

Taken together, these five groups were responsible for 938 incidents — nearly 25% of all ransomware attacks in 2025, while the remaining 98 threat actors carried out the rest. This highlights that while many groups are active, a small cluster of highly aggressive operators is driving a disproportionate share of global ransomware activity.

Share of Ransomware Attacks by Top 5 Groups (2025)



These actors exemplify the professionalization of cybercrime, leveraging Phishing-as-a-Service platforms, double-extortion tactics, and ransomware-as-a-service ecosystems to scale operations globally. Their sustained presence underscores a sobering reality: organized cybercrime groups now operate with the reach, resources, and coordination once attributed primarily to nation-state adversaries.

Geographies in the Crosshairs

Ransomware activity targeting the critical sectors in 2025 was highly concentrated in a handful of regions, underscoring both financial motivations and the strategic impact of disrupting advanced economies. Out of 4,701 total incidents, the following countries' critical infrastructure were hit hardest:

United States:
~1,000 incidents

Canada:
139 incidents

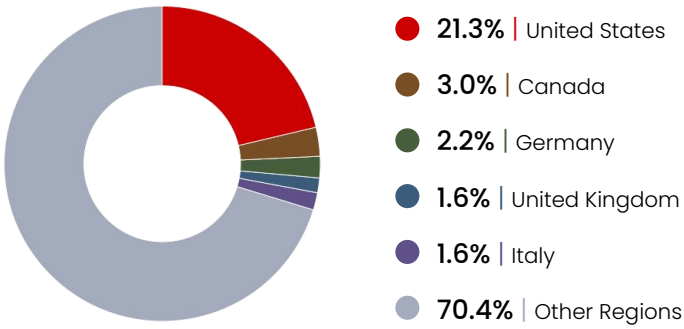
Germany:
102 incidents

United Kingdom:
76 incidents

Italy:
74 incidents

Together, these five countries account for 1,391 ransomware events — nearly 30% of all attacks recorded in 2025.

Share of Ransomware Attacks by Region (2025)



The remaining 3,310 incidents (70%) were distributed across dozens of other geographies, ranging from Latin America to Asia-Pacific. While these countries individually see lower attack volumes, the global spread reflects how ransomware has become a borderless, opportunistic threat — capable of disrupting operations and critical services worldwide.

This concentration against the U.S. and allied economies highlights the dual motive behind ransomware: maximizing ransom payments where digital dependence is highest, while simultaneously testing the resilience of critical industries in nations central to global trade and security.

Building Cyber Resilience Against Ransomware

National security in the digital era depends on cyber resilience — the ability of governments, industries, and societies to anticipate, withstand, and recover from escalating cyber threats. Citizens must have confidence that essential services — from energy and healthcare to finance, defense, and even electoral systems — remain reliable and secure amid relentless digital assaults.

To confront the growing ransomware crisis, cyber resilience must become a core pillar of national security strategy. This requires:

- Public–private intelligence sharing to detect and disrupt ransomware campaigns earlier.
- Sector-specific resilience standards to ensure continuity of operations in healthcare, energy, and transportation.
- Investment in incident response and recovery capabilities to mitigate impact and reduce downtime.
- International cooperation to dismantle the cross-border infrastructure enabling these attacks.

With 50% of all ransomware attacks in 2025 targeting critical infrastructure, the message is clear: cyber resilience is now a matter of national defense. Governments, industries, and global partners must strengthen defenses together to ensure ransomware cannot continue to threaten the safety, stability, and security of modern society.

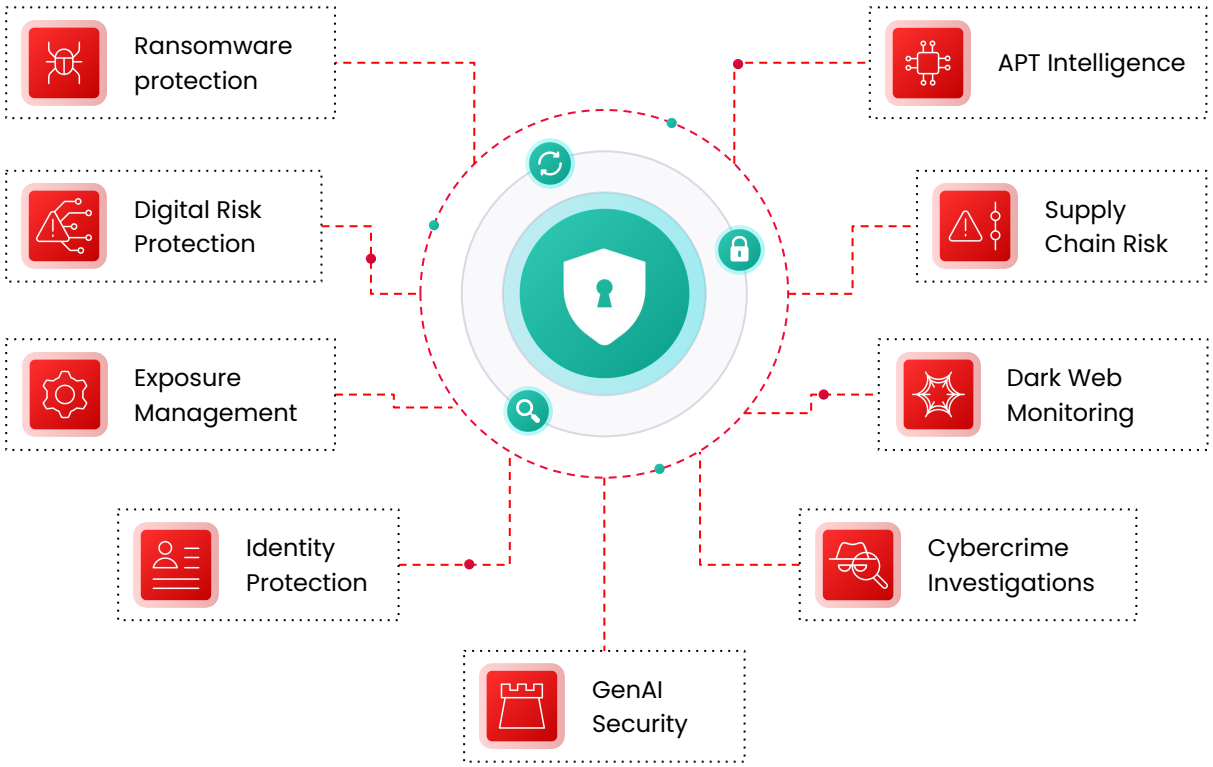
Fight AI with AI

5000+
Ransomware Victims

4.3 Million+
Infected Machines

4 Billion
Compromised Credentials

Proactive Threat Exposure Reduction



Who Are Our Clients?

- Businesses
- Enterprises
- Law Enforcement
- Government
- GenAI Developers

What Makes Our Customers Happy

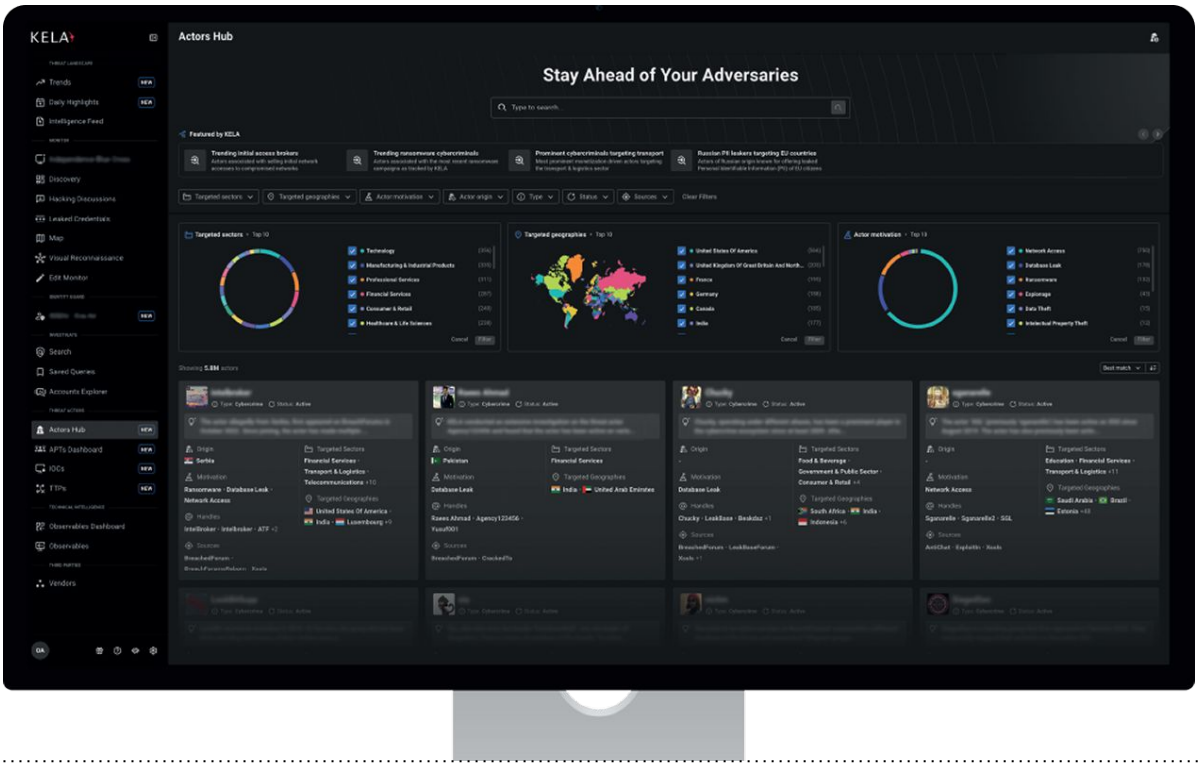
KELA holds a strong rating of 4.8 on Gartner Peer Reviews, exceeding Recorded Future. This high rating underscores KELA's dedication to quality, relevance, and the delivery of high-impact intelligence that integrates seamlessly into your security strategy.

4.9 ★★★★★

53 Ratings on Gartner Peer Insights

As of July, 30 2025

- Stop Real Attacks Before They Happen
- Exposure-Centric with Actionable Intelligence
- Automated and Easy to Use



Empowering Diverse Industries:

From retail to finance, healthcare to government, KELA's platform ensures that every sector can safeguard against financial loss, compliance violations, operational disruptions, and more.

Book a demo

Choose KELA for 100% real, actionable intelligence!