Cyber Insights on Ransomware 2025

Ransomware threats continue to **rapidly evolve in 2025**, with cybercriminals leveraging AI-driven social engineering, targeted extortion, and large-scale data exfiltration to bypass security defences.

The evidence is clear – network security alone isn't enough to keep businesses secure or compliant. Attackers target data directly, and regulations demand stronger protection.

These cases highlight why protecting the data itself is essential to mitigating risk.

Ticketmaster security breach: Over 560 million users affected.

Reports suggest that ShinyHunters infiltrated the company's network by taking advantage of a security flaw in the customer service portal, demanding a $500,000 ransom.

This follows Ticketmaster's previous fine from the ICO for **£1.25M for failing to prevent a cyberattack** that compromised its customers' personal data.

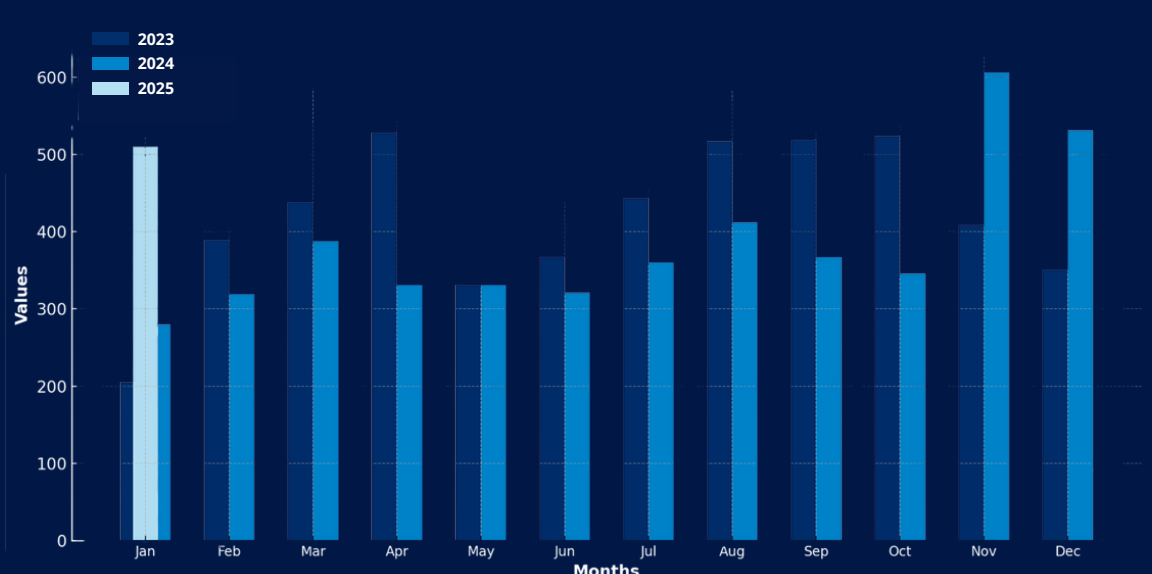
Ministry of Defence data breach: Nation-state interference to blame?

Cybercriminals breached the MOD's payroll system, compromising the personal information of 270,000 current and former military personnel, including names, bank account details, and other sensitive information.

Casio ransomware incident causes system-wide IT outage

Ransomware actors deploying phishing tactics triggered an attack that disrupted multiple systems, stealing personal data of employees, partners, and customers.

Trend Comparison of Ransomware Attacks



January 2025 saw a slight **3.95% drop** in ransomware victims compared to December 2024.

However, the bigger picture tells a different story.

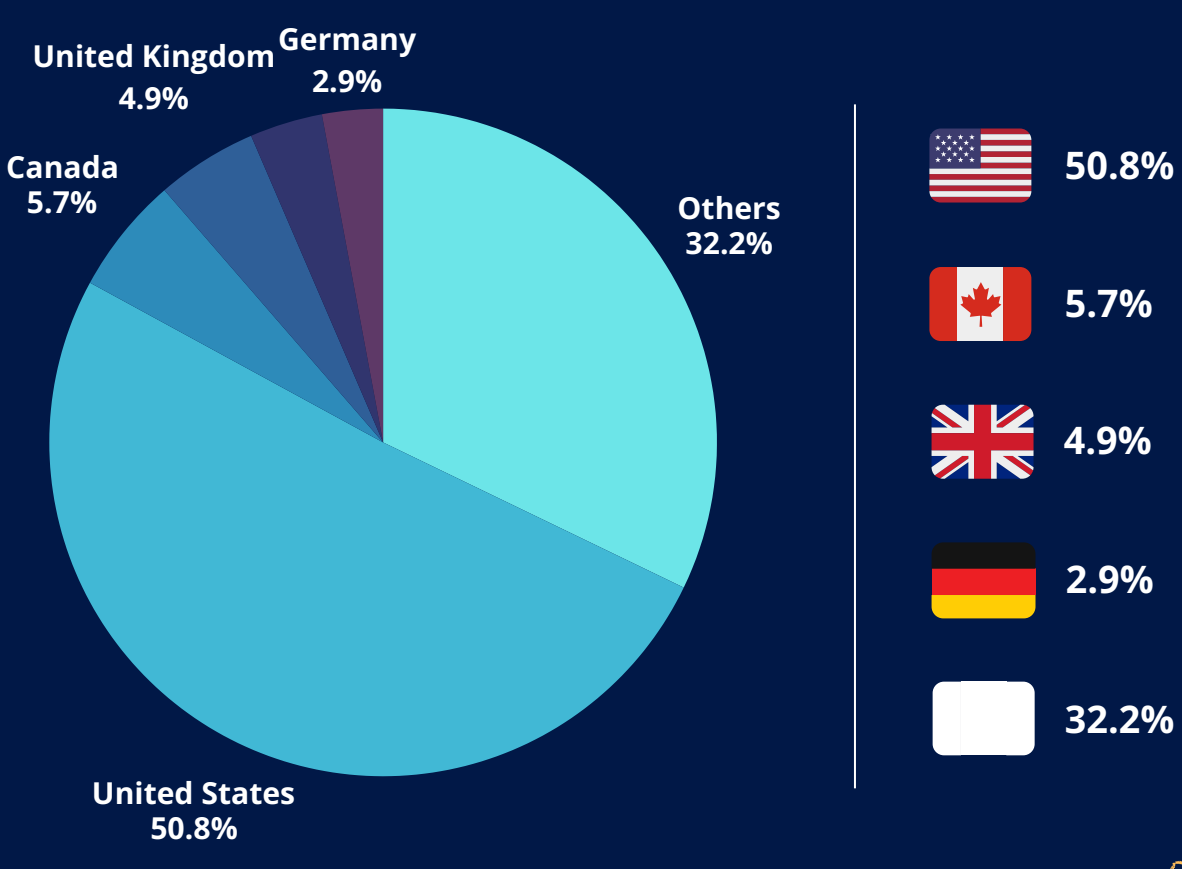
- **Ransomware attacks have escalated significantly over the past two years**
- **Victim numbers grew from 205 in January 2023 to 280 in January 2024**
- **Ransomware attacks soared to 510 in 2025 – an alarming 82.14% increase in just one year**

Source: Cyfirma

Top 5 Locations:

Ransomware Attacks in January 2025

These regions are key targets because of their strong economies, wealth of data-driven businesses, vital infrastructure, and the potential for substantial ransom payments, which make them highly appealing to cybercriminals.



Did you know?

- **Repeat ransomware attacks are common**: 80% of victims who pay a ransom experience another attack soon after.
- **Payment doesn't guarantee data recovery**: Just 46% of victims who pay a ransom receive access to their data — and much of the data they receive is corrupted.
- **The impact of downtime is severe:** On average, businesses hit by ransomware remain offline for 24 days.

Predictions for 2025

Despite takedowns, attacks will continue to grow.

Despite setbacks in 2024, ransomware groups are expected to rebound and escalate attacks in 2025. As barriers to entry lower, attack volumes will rise, forcing organisations to adapt their security strategies – securing your data is key.

Attackers will evolve to bypass defences in place.

As defences improve, ransomware groups are shifting to more disruptive tactics – like halting operations and targeting victims' clients to exert extra pressure – focusing on data theft and business disruption for higher ransoms.

New ransomware groups will emerge, with new tactics.

Ransomware attacks reached all-time highs in Q4 2024, with 13 new groups, such as SafePay and FunkSec, rapidly scaling their operations. Groups will increasingly adopt generative AI and LLMs in their operations to automate and enhance attacks.

Secure tomorrow's data today

Book in a demo with us and find out more about how Certes can help safeguard your business.

www.certis.ai