Global Cyber Attacks Rise in January 2026 Amid Increasing Ransomware Activity and Expanding GenAI Risks

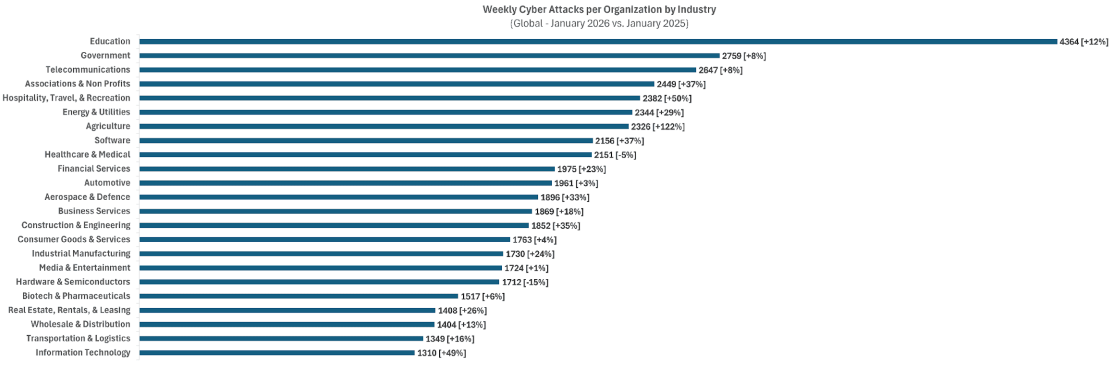
Global Attack Volumes Climb Worldwide

In January 2026, the global volume of cyber attacks continued its steady escalation. Organizations worldwide experienced an average of **2,090 cyber-attacks per organization per week**, marking a **3% increase from December** and a **17% rise compared to January 2025**. This growth reflects a landscape increasingly shaped by the expansion of ransomware activity and mounting data-exposure risks driven by widespread GenAI adoption.

Check Point Research data shows that January's upward trajectory underscores a persistent and evolving cyber threat environment — one defined by fast-moving ransomware operations and intensifying GenAI-related risks.

Critical Sectors Face Intensified Pressure

The **Education** sector remained the most targeted industry in January, facing an average of **4,364 attacks per organization per week**, a **12% increase year-over-year**. Elevated exposure, large user populations, and reliance on aging infrastructure continue to make the sector an attractive target for threat actors.



The **Government** sector followed with **2,759 weekly attacks** (+8% YoY), maintaining its position as one of the most consistently targeted verticals due to its mission-critical systems and high-value data.
A notable shift occurred this month as **Telecommunications** moved into third place, averaging **2,647 weekly attacks** (+8% YoY). This sector replaced Associations & Nonprofits, which occupied the third position in December, reflecting the growing focus on telecom infrastructure as attackers increasingly exploit connectivity dependencies, 5G expansion, and supply-chain ecosystem risks.

Regional Threat Gaps Widen

While this month's headline emphasizes global trends rather than regional specificity, a regional breakdown remains essential to understanding the geographic dynamics behind January's surge. **Latin America** recorded the highest average number of weekly attacks per organization at **3,110**, representing a **33% YoY increase**, the largest regional spike worldwide. It was closely followed by **APAC**, which reported **3,087 attacks** (+7% YoY), and **Africa**, which averaged **2,864 attacks** (-6% YoY). **Europe** and **North America** saw significant increases of **18%** and **19%** respectively compared to January 2025.

REGION	WEEKLY ATTACKS PER ORGANIZATION	YOY CHANGE
Latin America	3,110	+33%
APAC	3,087	+7%
Africa	2,864	-6%
Europe	1,755	+18%
North America	1,465	+19%

This distribution highlights not only the global scale of cyberattack activity but also the intensifying concentration of threats in rapidly digitizing economies.

GenAI Adoption Drives New Data-Exposure Risks

GenAI usage continued to accelerate inside enterprise environments, sharply increasing the risk of accidental data leakage.

January highlights:

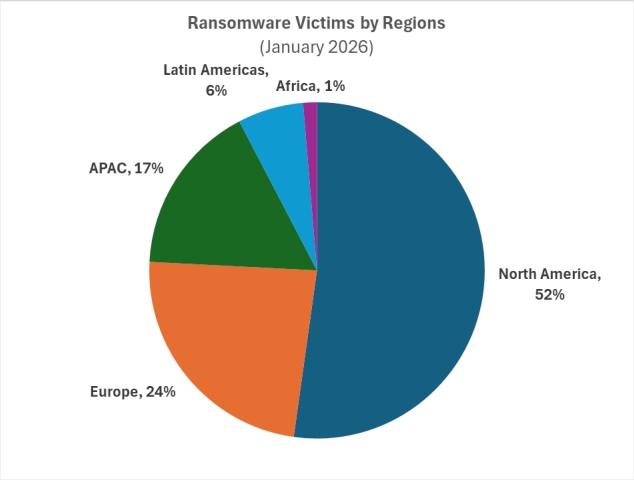
- **1 in every 30 GenAI prompts** submitted by users from enterprise networks posed a **high risk of sensitive data leakage**.
- This data leakage risk impacted **93% of organizations** who regularly use GenAI tools.
- **An additional 16% of prompts** contained potentially sensitive information.
- Organizations used **an average of 10 different GenAI tools**, highlighting fragmented and inconsistent usage patterns.
- The average enterprise user generated **76 GenAI prompts per month**, reflecting deep operational integration of AI-driven workflows

This continued opacity in GenAI usage reinforces the need for robust governance, better visibility into AI tooling, and stringent data-handling controls. Without such safeguards, organizations face heightened exposure to credential leaks, source-code disclosure, internal document mis-sharing, and inadvertent supply-chain vulnerabilities.

Ransomware Gains Momentum

Ransomware activity continued to intensify **in January 2026, with 678 reported attacks, reflecting a 10% increase compared to January 2025.** Despite monthly fluctuations, ransomware remains one of the most persistent and disruptive threats globally, driven by resilient RaaS ecosystems and increasingly data-theft-focused extortion models.

North America accounted for 52% of ransomware victims, followed by **Europe (24%)** — showing attackers continued focus on high value markets with extensive digital infrastructure.

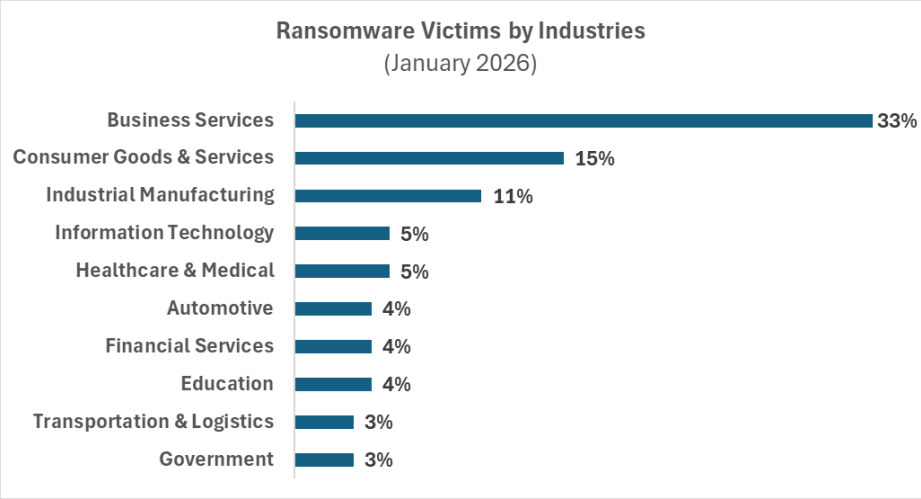


(*) This data draws from ransomware "shame sites" operated by double-extortion ransomware groups, which publicly disclose victim information. While these sources have inherent biases, they provide valuable insights into the ransomware landscape.

The **United States (48%)** remained the most targeted country. Other significantly impacted nations included the **UK (5%)**, **Canada (4%)**, **Germany (4%)**, **Italy (3%)**, and **Spain (3%)**.

COUNTRY	RANSOMWARE VICTIMS
United States	48%
United Kingdom	5%
Canada	4%
Germany	4%
Italy	3%
Spain	3%
France	2%
Turkey	2%
India	2%
Taiwan	2%

Industries with high dependency on continuous operations remained prime targets. **Business Services represented 33% of all ransomware victims, followed by Consumer Goods & Services (15%) and Industrial Manufacturing (11%),** illustrating attackers' focus on sectors where downtime directly translates to financial and reputational damage.



This steady rise in ransomware activity indicates that attackers are becoming more selective, more efficient, and increasingly aggressive in their extortion tactics—reinforcing the need for organizations to strengthen resilience, visibility, and rapid response capabilities.

Leading Ransomware Groups Tighten Their Grip

Qilin (15% of reported attacks) led global ransomware activity, expanding victim disclosures through its Rust-based ecosystem. **LockBit (12%)** continued its widespread double-extortion campaigns. **Akira (9%)** maintained momentum targeting Windows, Linux, and ESXi systems, with particular focus on Business Services and Industrial Manufacturing.

1. **Qilin -** one of the most established RaaS groups, with a consistent track record of victim disclosures dating back to 2022. Originally operating under the name "Agenda," the group rebranded as "Qilin" by September 2022, introducing a Rust-based encryptor and expanding its RaaS infrastructure. It provides affiliates with a full-featured toolkit via a dedicated administrative panel, including an encryptor, negotiation infrastructure, and support services. Following RansomHub's retirement, Qilin intensified its affiliate recruitment efforts and, since March 2025, has significantly increased the volume of victim listings on its data leak site (DLS).
2. **LockBit -** ransomware-as-a-service (RaaS), that was first launched in September 2019 and was updated and improved in June 2021. LockBit targets large enterprises and government entities from various countries and does not target individuals in Russia or the Commonwealth of Independent States. LockBit shares details of their victims on a Tor-hosted leak site along with the countdown to the date and time at which stolen data will be published unless the ransom

payment is received. LockBbit is considered to be the fastest ransomware in terms of encryption speed.

3. **Akira -** RaaS actor first reported in early 2023, with payloads targeting both Windows, Linux and ESXi systems. Its victimology in Q2 2025 shows a notable focus on business services (19%) and industrial manufacturing (18%). In early 2024, Akira introduced a Rust-based encryptor with specific features designed for ESXi servers. The new variant includes selective encryption, VM targeting, and runtime controls. It also implements a unique execution guard using Rust build-IDs to hinder sandboxing and reverse engineering.

What January's Trends Signal

January's findings point to a threat landscape entering 2026 with heightened speed, sophistication, and volatility. Attackers are refining tactics, exploiting systemic weaknesses across industries, and increasingly blending ransomware, data extortion, and GenAI-enabled exposure.

At Check Point Software, our research shows that today's cyber threats demand a **prevention-first, multi-layered security strategy**. Detection alone can't keep pace — adversaries move faster, automate more effectively, and exploit vulnerabilities before defenses activate. Real-time prevention, unified threat intelligence, and end-to-end protection across cloud, network, endpoint, and users are essential to staying ahead.

Only by anticipating adversaries' next moves can organizations meaningfully reduce risk and build lasting cyber resilience.