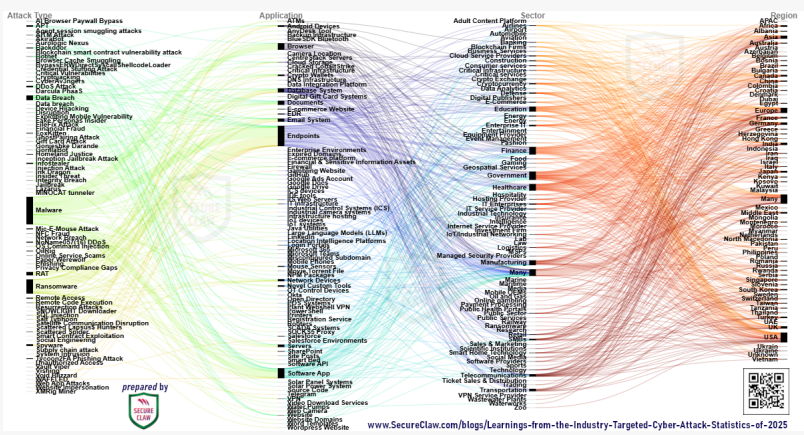
2025 Cyber Threat Landscape and 2026 Resilience Roadmap: SecureClaw's Global Perspective for Organizational Leaders

The rise in cyberattacks on government entities and global business supply chains signifies heightened geopolitical tensions and a lack of attention to SMBs.



2025 Annual Cyber Threat Report Summary by SecureClaw

SAN FRANCISCO, CA, UNITED STATES, January 1, 2026 /EINPresswire.com/ -- SecureClaw has recently released its annual Cyber Threat Analysis Report, based on data from 2025, which highlights recurring attack patterns affecting organizations of all sizes. The findings reveal that threat actors frequently reuse infrastructure - such as IP addresses, domains, and malware variants - across multiple campaigns. By examining these overlaps, security teams and organizational leadership can enhance attribution, strengthen defenses, and proactively anticipate future attacks before they escalate.

> Cybersecurity is essential for every business, regardless of its size, location, or revenue. The BDSLCCI Cybersecurity Framework supports SMBs worldwide with a tailored set of controls."
>
> *Dr. Shekhar A Pawar, Founder & CEO, SecureClaw*

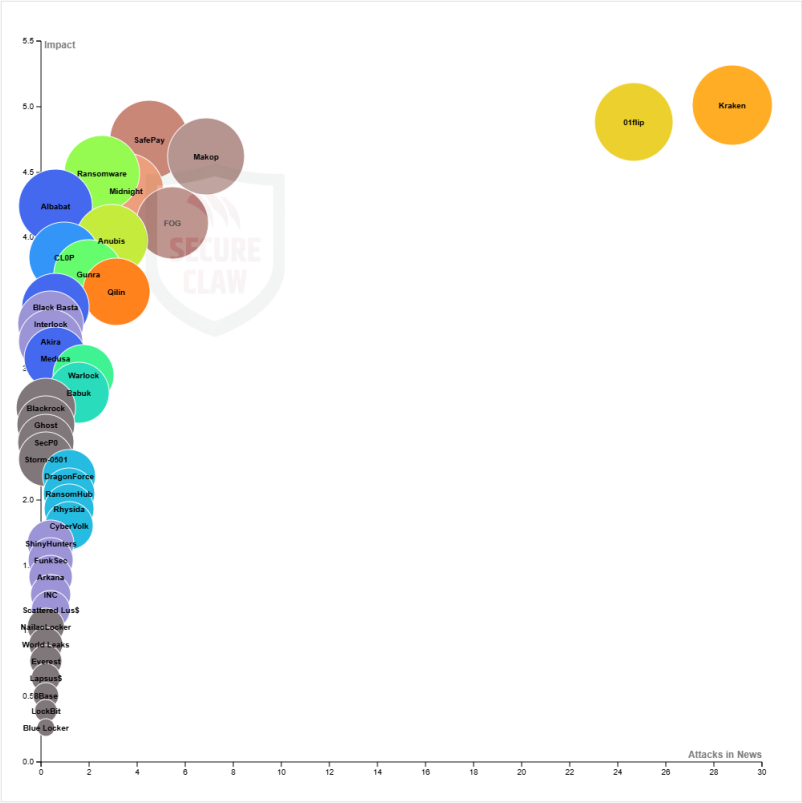
In 2025, reports on cyberattacks reveal that government organizations remain the most heavily targeted sector, accounting for 24% of incidents. Healthcare follows closely at approximately 21%, while financial services represent 15%. Manufacturing industries face 11% of attacks, education 5%, and hosting providers, small and medium businesses (SMBs), and cloud service providers each account for about 2%. Beyond these primary targets, a wide range of other industries are also under persistent threat. These include telecommunications, transportation, enterprise IT, cryptocurrency, e-commerce, critical services, retail, the public sector, data analytics, construction, location intelligence, financial institutions, geospatial services, consumer productivity, fintech, critical infrastructure, smart home technology, IoT and industrial networking, blockchain firms,

crypto foundations, energy, military, internet service providers, managed security providers, technology and IT services, defense, airlines, and electric utilities. Collectively, this broad spectrum of vulnerable domains underscores the pervasive and far-reaching nature of cyber threats across both public and private sectors.

Increased cyberattacks on government entities signify growing vulnerabilities in national infrastructure, heightened geopolitical tensions, and the urgent need for stronger cybersecurity frameworks. Also, since there are industry-specific cyberattack trends, the BDSLCCI framework can play an important role in securing the supply chain.

Countries where industries face the highest levels of cyber threats include the United States (approximately 16%), Europe (6%), India (around 5.32%), the United Kingdom (5.00%), Germany (5.00%), Canada (4.41%), Japan (4.22%), France (3.96%), Asia (3.76%), South Korea (3.63%), Africa (1.69%), the Middle East (1.62%), and Turkey (1.43%). In addition to these, numerous other nations report significant cyberattacks across their industries. These include China, Brazil, Egypt, Australia, Kenya, Serbia, Tanzania, Slovenia, Greece, Bosnia and Herzegovina, Singapore, Montenegro, Albania, North Macedonia, Croatia, Romania, Bulgaria, Rwanda, Kosovo, Taiwan, Iran, Italy, Switzerland, Belgium, Vietnam, Russia, Pakistan, the Philippines, Morocco, Iraq, Hong Kong, Ukraine, Mexico, Peru, Thailand,

Cyber Attacks Trend showing Industrywide Report of Year 2025 Report by SecureClaw



Reported Ransomware Attacks Compared to Average Impact, 2025

Colombia, Sweden, Denmark, Myanmar, Malaysia, Israel, Azerbaijan, the United Arab Emirates, Kuwait, Dubai, Poland, Mongolia, Austria, the Netherlands, and Indonesia, among others.

Many industries fail to report cyber threats, either despite existing compliance requirements or due to the absence of strict regulatory obligations in their countries. Consequently, only a limited number of cases are reflected in media reports.

In 2025, the ransomware variants identified - including Kraken, Makop, Babuk, CL0P, Black Basta, LockBit, Rhysida, Medusa, Akira, and many others - represent a broad spectrum of malicious campaigns targeting global organizations. These groups employ tactics such as data encryption, double extortion, and data leaks to pressure victims into paying ransoms. Some, such as LockBit, CL0P, and Black Basta, are among the most notorious for large-scale attacks on enterprises and critical infrastructure, while emerging strains like Qilin, 8Base, and RansomHub highlight the constant evolution of the ransomware ecosystem. Collectively, these operations demonstrate how ransomware has become one of the most disruptive cyber threats, combining financial extortion with reputational damage and operational paralysis across industries worldwide.

As illustrated in the figure, the known malware families represent a diverse spectrum of cyber threats targeting global organizations and individuals. These include infostealers such as LeakyStealer, JSCEAL, and ACRStealer, which exfiltrate sensitive data like credentials and financial information; remote access trojans (RATs) such as MysterySnail, Silver RAT, RokRat, and KimJongRAT, which enable persistent unauthorized control of infected systems; and keyloggers like Snake Keylogger and Agent Tesla, designed to capture keystrokes and compromise accounts. Other strains, including Raspberry Robin, ModiLoader, and Gootloader, act as malware loaders, distributing additional payloads across networks, while botnets such as MikroTik and XorDDoS orchestrate large-scale distributed denial-of-service (DDoS) attacks. Specialized threats like DroidLock, Gorilla Android, and Deepfake Mac Malware highlight the growing risks to mobile and macOS platforms, while advanced persistent threats (APT37, HollowQuill, and MuddyWater) demonstrate state-sponsored or highly organized campaigns. Collectively, these malware variants showcase the evolving tactics of cybercriminals - from credential theft and financial fraud to espionage and infrastructure disruption - underscoring the urgent need for robust, adaptive cybersecurity defenses across all sectors.

Below are quick preventive measures that any organization can implement:
(1) Regular Data Backups:
(a) Backups should be stored offline or in immutable cloud storage.
(b) Test restoration processes frequently to ensure business continuity.
(c) This prevents attackers from holding data hostage.
(2) Patch and Update Systems:
(a) Many ransomware campaigns exploit outdated software.
(b) Automating patch management reduces human error and delays.
(3) Zero Trust & Access Controls:
(a) Adopt the principle of “never trust, always verify.”

(b) Restrict administrative rights and segment networks to contain breaches.
(c) Multi-factor authentication (MFA) is critical to stop credential theft.
(4) Employee Awareness & Training:
(a) Human error is often the weakest link.
(b) Training employees to spot phishing emails, malicious attachments, and suspicious links reduces risk significantly.
(5) Endpoint Protection & Monitoring:
(a) Use EDR solutions, intrusion detection systems, and AI-driven monitoring.
(b) Proactively hunt for indicators of compromise (IoCs) to stop attacks before escalation.

If your organization is a small or medium-sized business (SMB), the BDSLCCI framework can help implement comprehensive cybersecurity. Below are five key benefits of BDSLCCI:
(1) Provides tailored cybersecurity controls designed specifically for SMBs, helping reduce overall implementation costs. It also offers consulting assistance, tools via BDSLCCI's web platform, and certification, transcripts, and reports that demonstrate coverage and effectiveness of controls achieved after audit and assessment.
(2) Strengthens supply chain security against industry-specific attack trends.
(3) Ensures compliance readiness without overwhelming limited resources.
(4) Builds resilience and trust with customers and partners.
(5) Empowers SMB leaders to adopt scalable, practical defenses for a safer digital future.
SecureClaw provides end□to□end cybersecurity services including VAPT, SAST, V□CISO, compliance support, threat intelligence, and training solutions for SMBs and enterprises. It can help organizations build cyber resilience.

Dr. Shekhar A Pawar
SecureClaw Inc.
+1 218-718-2121
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X
Other