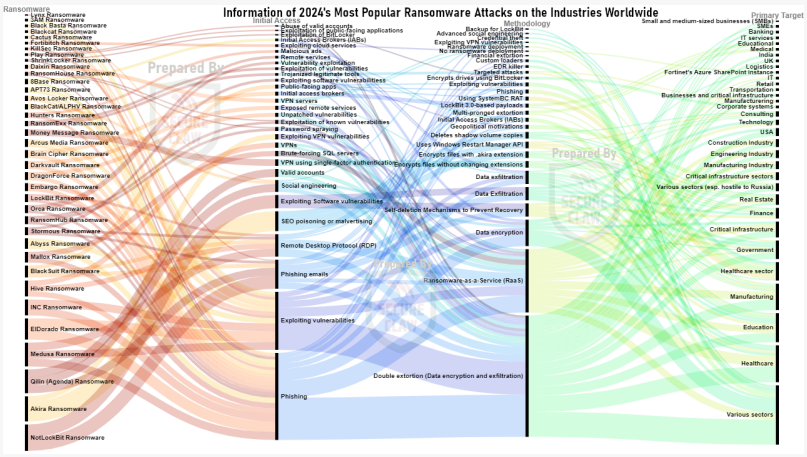
Takeaways from 2024's Worldwide Industry Targeted Cyberattack Statistics for Cybersecured New Year 2025 by SecureClaw

In 2024, the year was proclaimed as the "Year of AI" due to advancements in AI technologies, 6G services, and even AI-powered, more sophisticated cyberattacks.

DOVER, DE, UNITED STATES, January 1, 2025 /EINPresswire.com/ -- Historical data from 2024 reveals cyber-attack patterns, as threat actors frequently reuse infrastructure across campaigns, aiding security teams in identifying and predicting future attacks.



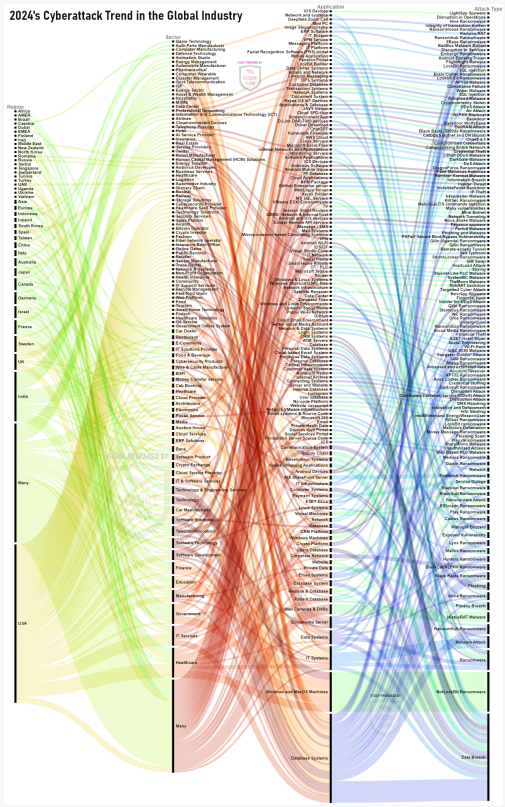
2024's Worldwide Industry Targeted Ransomware Cyber Threats Statistics by SecureClaw

In 2024, cybersecurity has improved significantly due to advancements in AI and ML technologies, enabling real-time threat identification and mitigation. Global collaboration has reduced large-scale cyberattacks, and public awareness and education about cybersecurity have increased. New laws and regulations have been enacted to protect critical infrastructure, and quantum cryptography is expected to revolutionize data security in the future. Even though the technological advancements and collaboration are improving the cybersecurity of industries in many countries, it is also evident that the effective uses of AI technologies are being used by cybercriminals for more sophisticated cyberattacks.

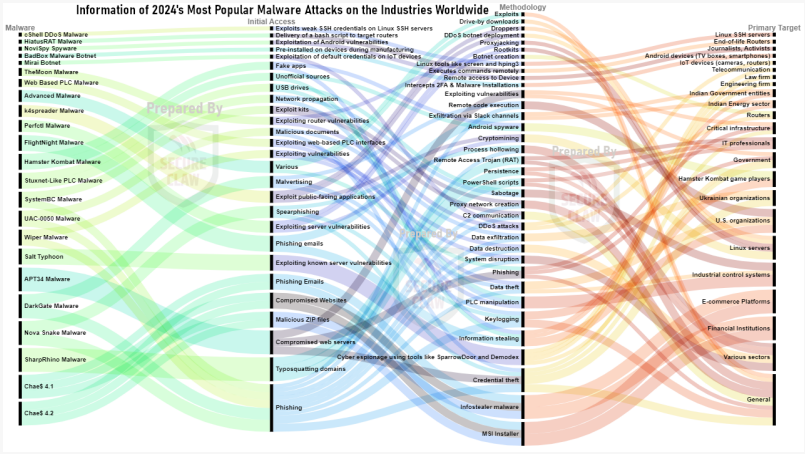
> Cybersecurity is a right of every business, regardless of its size, location or revenue. SecureClaw is providing a cost-effective, easy-to-adopt, and tailored BDSLCCI framework 3.0 for SMEs worldwide!"
>
> *Dr. Shekhar Pawar, Founder & CEO, SecureClaw*

The SecureClaw Cyber Threat Advisory team studied more than 5000 international cyber-attack news stories in various industries and created a most visible cyber threats trend considering sampling basis summary report, which will be discussed in this article. It is worth noting down that many organizations never report the cyber incident to media or government; hence, no one is able to identify exact statistics of the

cyber-attack trends. Organizations have fear disclosing cyberattacks could damage their reputation and erode customer trust, especially for sensitive customer data. This article examines cyber-attack trends in countries with limited data privacy enforcement, focusing on organizations forced to report incidents to the government or media, using various sources of cyber-attack news.



2024's Worldwide Industry Targeted Cyber Threats Statistics by SecureClaw



2024's Worldwide Industry Targeted Malware Cyber Threats Statistics by SecureClaw

SecureClaw reports that healthcare, IT services, manufacturing, and software industries are among the most targeted by cybercriminals globally, with the top industries being healthcare (7.84%), government (4.71%), IT services (3.92%), education (2.35%), finance (2.35%), and manufacturing (2.35%). Year 2024 started with the Mercedes-Benz source code and Subway's data leaked by hackers. While reaching the year-end, Japan Airlines experienced a denial-of-service (DoS) cyberattack on December 26, 2024, overwhelming the airline's network with massive data transmissions, causing delays and system disruptions. Fortunately, the airline managed to restore its systems within a few hours, and flight operations returned to normal by December 27. In the last three days of December 2024 in the USA, a ninth US telecommunications company, AT&T Inc. and Verizon Communications Inc., were targeted by the 'Salt Typhoon' campaign, a sophisticated cyberattack attributed to Chinese hackers. Also, the Volkswagen Data Breach caused 800,000 electric car owners' data to leak.

Malware is malicious software designed to harm the confidentiality, integrity, or availability of a computer, server, client, OT, IoT, or network. Common types include viruses, worms, trojans, ransomware, spyware, adware, and rootkits. Malware can infiltrate systems through phishing emails, infected files, malicious websites, or exploiting software vulnerabilities. Once installed, it

can steal, encrypt, or delete data; hijack core functions; spy on user activity; and lock users out until a ransom is paid. Cybercriminals use malware for financial gain, data theft, espionage, or disruption in operations.

The cShell DDoS malware, discovered in December 2024, targets poorly managed Linux SSH servers by exploiting weak SSH credentials. The Mirai botnet, first discovered in August 2016, targets IoT devices like routers, IP cameras, and home devices, turning them into remote-controlled bots for large-scale network attacks. The BadBox malware botnet, first discovered in early 2023, is insidious due to its pre-installation on devices before they reach consumers. The HiatusRAT malware, a Remote Access Trojan, has been in operation since July 2022, targeting outdated network edge devices and expanding to Taiwan and reconnaissance against a U.S. government server. APT34 malware, originating from Iran, first appeared in 2014, while K4spreader malware was identified in 2024. FlightNight Malware and Hamster Kombat Malware are new cyber threats, while SharpRhino malware has been active since 2023. Other malware threats include DarkGate malware since 2018, Nova Snake malware since 2020, Perfctl malware since 2021, SystemBC malware since 2019, and TheMoon malware since 2014.

Ransomware attacks have evolved from encrypting victim systems or data to using double and triple extortion techniques. Double extortion involves encrypting data and taking a backup before encryption, threatening to leak it online. Triple extortion uses stolen data to target customers or business partners through DDoS attacks. Ransomware attacks can be costly, with average costs reaching millions of dollars. Nation-state-sponsored cybercriminals are increasingly targeting critical infrastructure, including energy, healthcare, and manufacturing sectors. Conflicts between nations like Ukraine, Israel, and the South China Sea fuel this trend. In 2024, APT73 Ransomware and Arcus Media Ransomware were visible, followed by 3AM Ransomware, Abyss Ransomware, Akira Ransomware, BlackSuit Ransomware, and Cactus Ransomware. In 2022, 8Base Ransomware, Black Basta Ransomware, Bl00dy Ransomware, Daixin Ransomware, Lockbit 3.0 Ransomware, Play Ransomware, RansomHouse Ransomware, and Stormous Ransomware were first observed. RansomExx Ransomware has been active since 2020, and LockBit Ransomware has been active since 2019. NotLockBit, a new ransomware variant, emerged in 2023 and is part of the LockBit ransomware family. It encrypts files and demands a ransom for decryption. In September 2024, cybercriminals created "Fortibitch" to target cybersecurity company Fortinet, resulting in unauthorized access and a 440GB leak of customer data from their Azure SharePoint repository. Fortinet confirmed the breach did not involve ransomware deployment or network access appearing as a new methodology of ransomware.

Cybersecurity is crucial in today's increasingly sophisticated world, and organizations must identify their mission-critical assets and adopt defense-in-depth mechanisms. Especially for small and medium enterprises (SMEs), the BDSLCCI 3.0 cybersecurity framework can be cost-effective and better for specific cybersecurity needs of businesses. Employee awareness is crucial, and training should cover phishing precautions, policies, and insider threats. Monitoring third-party users and access to vendors is essential. Vulnerability assessment and penetration

testing (VAPT) are essential for IT assets, and compliance should be improved. Organizations should have a working plan for unseen cyber incidents, track incidents, and prepare a business continuity plan for any unseen circumstances. It's essential to check operating locations and reporting requirements to the government. SecureClaw provides various cybersecurity services, including the BDSLCCI Cybersecurity Framework for SMEs, Vulnerability Assessment and Penetration Testing (VAPT), Virtual CISO, and Source Code Security Review (SAST) services. Till now, SecureClaw has worked for clients in many countries, including various domains.

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