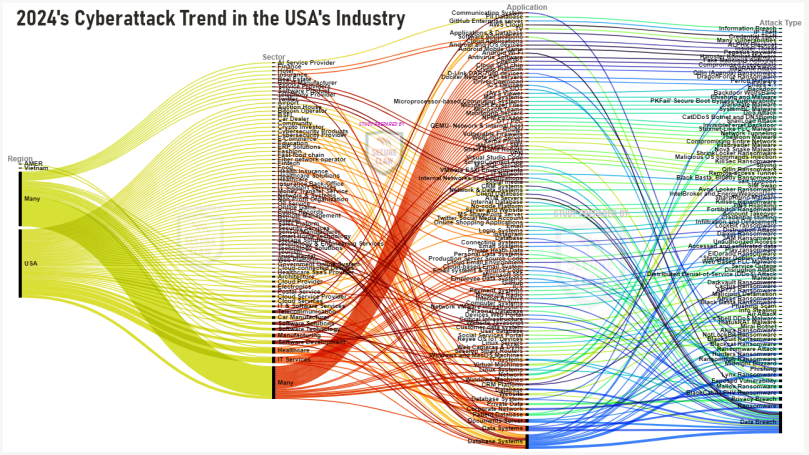
Analyzing 2024 USA Industry Cyberattack Trends: SecureClaw's Blueprint for Cybersecurity in the New Year

In 2024, the USA's industry cybersecurity posture improved with proactive strategies, but threats remain complex and evolving, requiring continuous vigilance.



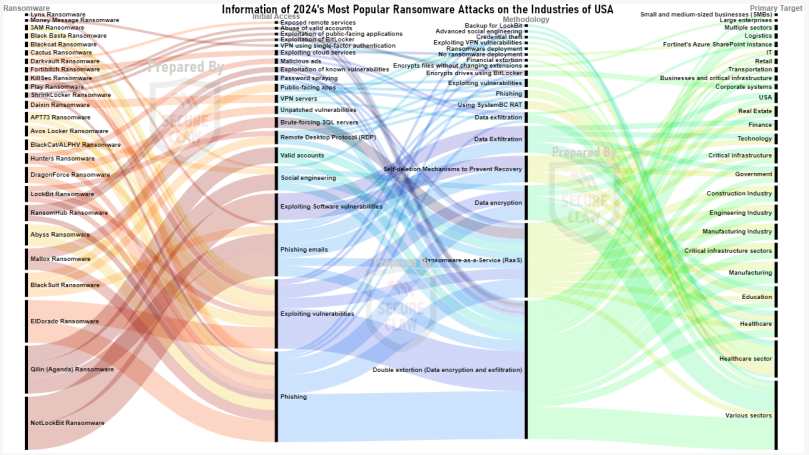
2024's USA Industry Targeted Cyber Threats Statistics by SecureClaw

LOS ANGELES, CA, UNITED STATES, January 3, 2025 /EINPresswire.com/ -- SecureClaw's Cyber Threat Advisory team has studied more than 5000 cyber-attack news stories worldwide in the year 2024, and here is a snapshot of its annual report. These diagrams showing analysis of USA's industry-targeted cyberattack trends were observed through various media sources and research articles. Few were directly from USA, whereas few sources were generic about entire world, not specific to a particular region. In the United States, under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), covered entities must report cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours. Additionally, ransom payments must be reported within 24 hours. For healthcare organizations in the USA, under the Health Insurance Portability and Accountability Act (HIPAA), healthcare entities must report breaches involving personal health information within 60 days. For the banking sector of the USA, the Federal Deposit Insurance Corporation (FDIC) requires banking organizations to report significant cyber incidents within 36 hours. Hence, it is assumed that maximum cyberattack incidents are reported by USA-based organizations to respective entities.

> 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*

There are two cyber threat terms mostly visible in many cyber-attack news, one is “Malware” and another one is “Ransomware”.
Malware is malicious software designed to harm computer, server, client, OT, IoT, or network confidentiality. Common types include viruses, worms, trojans, ransomware, spyware, adware, and rootkits. As evident in diagram, DarkGate Malware, Hamster Kombat Malware, k4spreader Malware, Nova Snake Malware, Perfctl Malware, SharpRhino Malware, Stuxnet-Like PLC Malware, SystemBC Malware, TheMoon Malware, Web-Based PLC Malware, and Mirai Botnet are various types of malwares that can compromise systems, steal credentials, and evade detection. These malwares use sophisticated techniques to steal credentials and log keystrokes, exploit misconfigurations to install rootkits and mine cryptocurrency, and can be used in ransomware campaigns. They also target routers, IoT devices, web applications, and IoT devices for large-scale DDoS attacks. cShell DDoS Malware targets poorly managed Linux SSH servers, exploiting weak credentials and using Linux tools for DDoS attacks. HiatusRAT Malware targets IoT devices, targeting vulnerabilities in Chinese-branded devices like Hikvision and Xiongmai.

2024's Malware Threats of USA by SecureClaw



2024's Ransomware Threats of USA by SecureClaw

Ransomware attacks initially focused on encrypting victim systems or data and demanding ransom for the decryption key. However, gangs have since evolved to include double and triple extortion techniques. Double extortion involves encrypting data and taking a backup before encryption, threatening to leak it online. Hence, only having a backup ready to restore doesn't help the victim. In triple extortion, attackers use stolen data to target customers or business partners through DDoS attacks. Ransomware attacks can be costly, with average costs reaching millions of dollars, and pose a significant threat due to their speed and difficulty in tracing attackers.

As shown in diagram, the list of ransomware groups found or suspected to be active in the USA includes 3AM, Abyss, APT73, Avos Locker, Black Basta, Blackcat, ALPHV, BlackSuit, Cactus, Daixin, Darkvault, DragonForce, ElDorado, Fortibitch, Hunters, KillSec, LockBit, Lynx, Mallox, PlayCrypt, Qilin (Agenda), RansomHub, ShrinkLocker, Money Message, and NotLockBit. Each group uses

different tactics, such as encrypting files, renaming them, and wiping Volume Shadow Copies. Abyss uses double extortion tactics, targeting VMware ESXi instances and threatening to leak stolen data if the ransom isn't paid. AvosLocker operates as a Ransomware-as-a-Service (RaaS) and targets various sectors, including financial services and critical infrastructure. Black Basta is known for its double extortion attacks, targeting healthcare and critical infrastructure. Blackcat uses double and triple extortion tactics, targeting multiple devices and operating systems. ALPHV targets Windows and Linux devices, employing advanced evasion techniques. BlackSuit conducts data exfiltration and extortion before encryption, targeting various critical infrastructure sectors. Cactus targets large commercial organizations by exploiting VPN vulnerabilities. Daixin targets healthcare and encrypts critical servers, threatening to release sensitive data if the ransom isn't paid. Darkvault uses leaked LockBit and Conti ransomware builders, while ElDorado targets Windows and Linux systems. KillSec uses a RaaS model and exploits publicly leaked data for extortion.

According to Dr. Shekhar Ashok Pawar, founder of SecureClaw, there are below key areas which needs attention towards cybersecurity adoption.
(1) Cyber-attacks can cause significant damage to an organization's reputation, trust, and share market price.
(2) Organizations can lose their productive time while undergoing cyber-attacks.
(3) Cybercriminals may sell an organization’s intellectual property (IP), such as source code, or technical designs on the dark web.
(4) The American Data Privacy and Protection Act (ADPPA) is a proposed federal bill in the United States aimed at regulating how organizations handle consumer data. The Federal Trade Commission (FTC) would enforce the ADPPA and could impose civil penalties for non-compliance. These penalties can be substantial, potentially reaching millions of dollars depending on the severity and nature of the violation. There is also the California Privacy Rights Act (CPRA), which applies to businesses with annual gross revenues over $25 million, those that buy, receive, or sell the personal information of 100,000 or more consumers, or derive 50% or more of their annual revenues from selling consumers' personal information. Cybersecurity controls implementation can help protect sensitive data.
(5) Big organizations outsource their operations or a few areas to other small and medium enterprises (SMEs), but it is important to check those are cyber-secured.

Generally, SMEs are facing several challenges while adopting existing cybersecurity standards or frameworks. It includes less funding, a lack of cybersecurity knowledge, and available cybersecurity standards that are not specific to their business's domain requirements, making it less attractive for return on investment. In that case, SecureClaw is providing the Business Domain Specific Least Cybersecurity Controls Implementation (BDSLCCI) cybersecurity framework, providing tailored cybersecurity controls depending on the organization's domain's specific needs. BDSLCCI is very helpful for SMEs, startups, or any such kind of organizations, as it is very cost-effective, less time consuming while implementation, and provides cybersecurity for your business’s mission critical assets. It provides good return on investment (RoI) justifying cybersecurity for sustaining and growing business success.

Apart from BDSLCCI Cybersecurity Framework for SME kind of organizations, SecureClaw provides various services, including Vulnerability Assessment and Penetration Testing (VAPT), Virtual Chief Information Security Officer (Virtual-CISO), and Source Code Security Review (SAST) services.

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