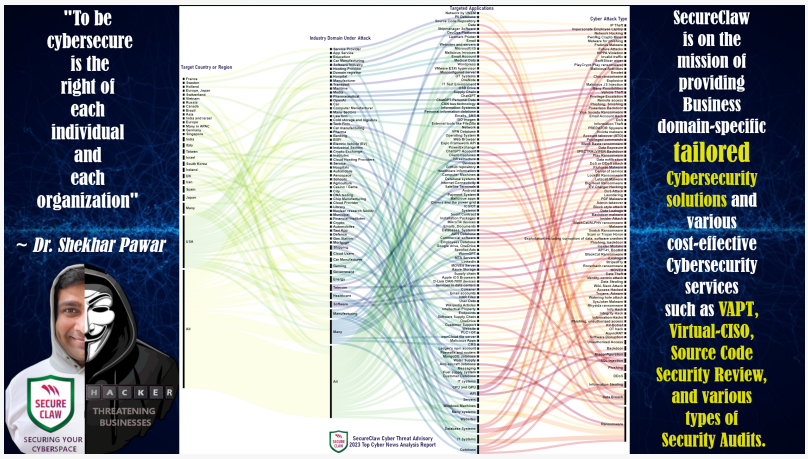
Learnings from the Cyber Attack Statistics of 2023 can help improve cybersecurity strategies, according to SecureClaw

SecureClaw Cyber Threat Advisory has published an analysis of cyber-attacks that happened in 2023, helping to understand the latest trends and gaps in security.



2023 Top Cyber News Analysis by SecureClaw Cyber Threat Advisory

DOVER, DELAWARE, UNITED STATES, January 1, 2024 /EINPresswire.com/ -- Happy Cybersecure New Year 2024! As world approach 2024, it is time to reflect. The year 2023 has been an exciting one, with many twists and turns in cyberworld. SecureClaw Inc., headquartered in Delaware, USA, offers a variety of cybersecurity services around the world, with a future focus on cybersecurity for small and medium-sized businesses (SMB or SME). SecureClaw Cyber Threat Advisory has reviewed over 4,500 cyber articles from various sources and nations to provide global solutions to businesses facing cyber threats. As indicated in the graphic, a few crucial statistics are the result of those. The data may differ geographically from actual cyber-attack figures in some countries due to the fact that many firms in these countries do not report cyber incidents.

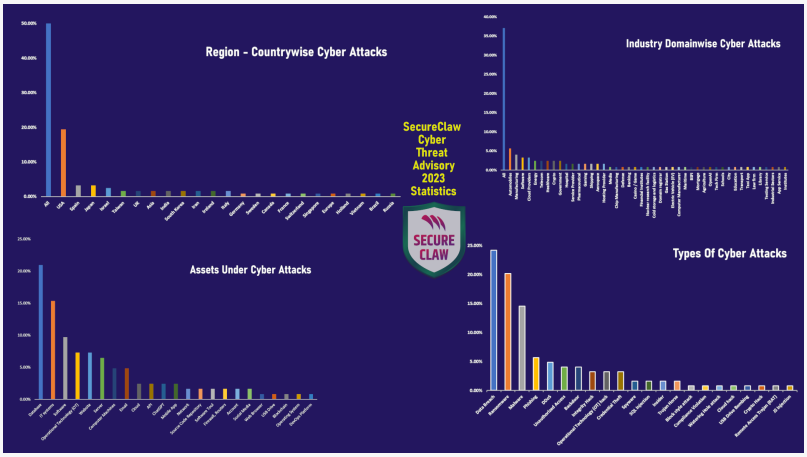
> Every organization, like institutes, manufacturing, maritime, chemical, pharma, IT, and e-commerce, should adopt cybersecurity best practices. The BDSLCCI framework provides tailored cybersecurity."
>
> *Dr. Shekhar Pawar, CEO, SecureClaw Inc., Inventor of BDSLCCI*

 Key Observations by SecureClaw:

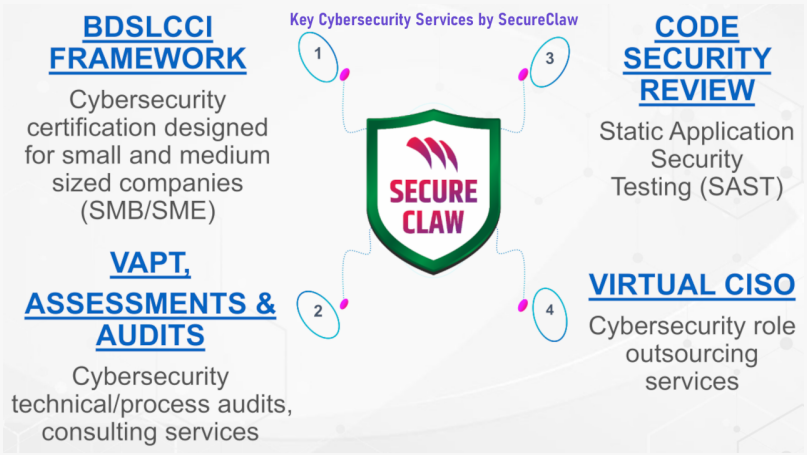
Apart from various industry domains, a few domains, such as automobiles, manufacturing, software providers, cloud providers, energy, telecom, healthcare, crypto, government, hospitals, pharmaceuticals, gaming, shipping, aerospace, and a few service providers, were mostly on the radar of cybercriminals throughout entire 2023. Most cyber threats were targeted at database systems, IT infrastructures, software systems,

operational technology (OT), websites, servers, computer machines, emails, the cloud, APIs, ChatGPT, and mobile apps.

Different techniques and sophisticated cyber-attacks were used via various types of data breach methods, including ransomware, malware, phishing, DDoS, unauthorized access, backdoors, integrity hacks, operational technology (OT) hacks, credential theft, spyware, SQL injection, insiders, and Trojan horses. The purpose of these cyber-attacks can be summarized as damaging reputations, disrupting business activities, hurting the competition's business, extortion (financial demands), or illegal or unauthorized access to data. Also, few cyberattacks seem to be state sponsored, as there are wars and conflicts going on across the borders of the few countries.



Cyber Attack Statistics of Year 2023 by SecureClaw Inc.



Key Cybersecurity Services Offered by SecureClaw Inc.

The Israel-Hamas war has significantly impacted the cyber domain, with potential targeted attacks from state-sponsored threat actors, despite social media abuse and opportunistic-hacktivism. Iran attempted to infiltrate Israel's water system in April 2023, causing water poisoning by increasing chlorine levels in residential water, according to media reports. Such cybercrime is a serious threat to human life. State-backed cyberattacks on US water systems have prompted federal attention to the digital challenges in 2023.

 SecureClaw observed innovative cyber-attack techniques:

2023's ransomware attacks had negatively impacted a few large enterprises, including Volvo Car, Maritime Firm Royal Dirkzwager, Ferrari, Hitachi Energy, Taiwanese PC Company MSI, Tesla, Suzuki motorcycle plant, multinational tech firm ABB, Japanese pharma giant Eisai Group, Spanish bank Globalcaja, TSMC, Japanese watchmaker Seiko, Johnson Controls, MGM casino, Chilean telecom giant GTD, British Library, and South Korean Anti-Aircraft. During these months, PlayCrypt (Play ransomware), Clop ransomware, Vice Society ransomware, Black Basta ransomware, LockBit ransomware, BlackCat/ALPHV ransomware, Snatch ransomware, Rorschach ransomware, and Rhysida ransomware were among hundreds of ransomware gangs

that were more active in sophisticated cyber-attacks.

Ransomware gangs have developed unique patterns for cybercrimes. Play ransomware, named after its encrypting process, has been a popular target since June 2022. Russian group Clop demands millions of dollars before disclosing compromised information. Russian-based Vice Society targets education and extortion, stealing data before encryption. Black Basta, active since April 2022, targets manufacturing, construction, real estate, food and beverage, chemicals, insurance, healthcare, mining, metals, and business services. LockBit ransomware encrypts files and demands payment for decryption keys, targeting businesses and organizations. BlackCat, also known as ALPHV and Noberus, uses a ransomware as a service (RaaS) business model, charging affiliates for ransomware payloads and using double extortion to gain access to victims' private information. Snatch, formerly known as Team Truniger, charges other threat actors for ransomware payloads and threatens public exposure if not paid. BabLock, also known as Rorschach, uses an unusual method of attaching extensions, allowing multiple extension versions to arise from a single execution. Rhysida targets Windows systems and gained notoriety in May 2023, possibly connected to the infamous Vice Society ransomware group.

Few malwares were very active in this period, such as Frebniis Malware, SwiftSlicer Widget, Emotet, Invicta Malware, Fluhorse Malware, Letscall Malware, Big Head, PDF-related malware, Backdoor-related malware, StripedFly, SysJoker Malware, and KV-Botnet. Researchers have uncovered a new, sneaky malware called "Backdoor.Frebniis", or simply "Frebniis". It uses an IIS weakness to create a backdoor into Windows web servers. Targets in Taiwan have been actively targeted by anonymous cybercriminals. Hackers must first gain access to an Internet Information Services (IIS) server in order to infect a system. The malware's internal mechanisms, however, are distinct. Failed Request Event Buffering (FREB) is a feature that IIS employs to gather information about requests, such as the originating IP address and port, HTTP headers containing cookies, etc. Frebniis abuses this feature. Similarly, each identified malware has its unique technique to perform malicious activities till actual cybercrime.

 How to be more secured and good cyber resilience?:

Here are a few important points on which businesses should focus.

 Adopt Cybersecurity Standard:
Every organization, starting from schools, colleges, manufacturing, maritime, chemical, pharma, information technology (IT), e-commerce, and even government organizations, should adopt cybersecurity best practices. 90% of the business population, which are SMBs, globally contributes to employment and GDP. To reduce cyberattack surface, they should adopt the Business Domain Specific Least Cybersecurity Controls Implementation (BDSLCCI) framework, which is cost-effective, easy, and tailored to their business domain.

 Cybersecurity Awareness Training for Employees:
Cyberattacks often stem from inadequate employee cybersecurity awareness. Effective training

should cover phishing precautions, policies, and insider threats, with employee testing for effectiveness.

 Backup important data:
Maintain secure and encrypted backups of crucial files, ensuring they are operational and can be restored as needed.

 Third-party users, access to vendors and external applications should be monitored.

 Monitor Your Network:
Regularly monitoring network logs and business transaction notifications is crucial for detecting malicious activities and taking necessary action to prevent them.

 Regular security audits, including vulnerability assessment and penetration testing (VAPT), should be part of the governance process, with processes enhanced as needed and compliances improved.

 Track Incidents as a report Until Permanent Closure.

 Prepare a business continuity plan (BCP) for any unseen circumstances, including natural disasters and cybercrimes.

Dr. Shekhar Pawar
SecureClaw Inc.
+1 218-718-2121
customercare@secureclaw.com
Visit us on social media:
Facebook
Twitter
LinkedIn
YouTube
Other
