Healthcare Heartbeat

2024: Q4

Cybersecurity Trends and Threats in the Healthcare Sector

Health-ISAC™
Collaborating for Resilience in Healthcare

TABLE OF CONTENTS

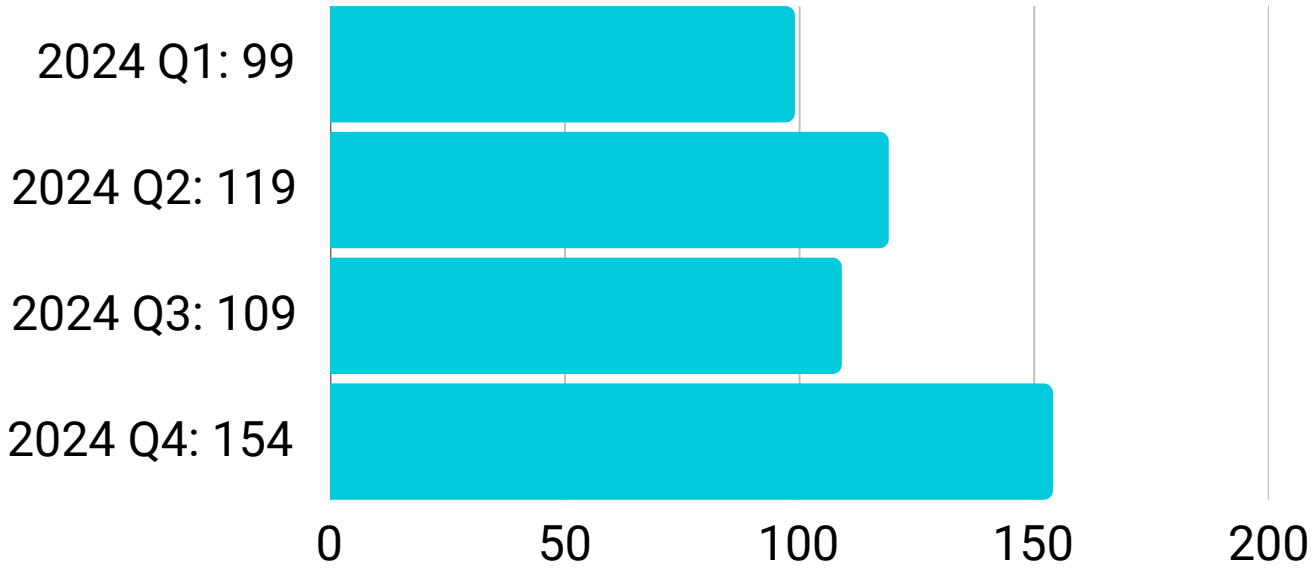
Summary

Health-ISAC's 2024 Q4 Healthcare Heartbeat provides observations of ransomware, cybercrime trends, and malicious actor forum postings that could potentially impact healthcare sector organizations. This product is for your situational awareness, and Health-ISAC recommends that members affiliated with the victim companies or those potentially affected take appropriate measures to secure critical infrastructure.

If Health-ISAC becomes aware of an imminent threat to members of the healthcare sector, it will communicate the information directly with the impacted organization.

Comments: Health-ISAC will continue to monitor this activity and provide relevant updates when necessary. If you have any questions or comments, please contact us at toc@h-isac.org.

Ransomware Attacks Against Healthcare



Health-ISAC observed a continuous trend of cyber security incidents and data breaches impacting healthcare over the past year. While ransomware events saw a slight decrease in Q3 of 2024, ransomware events continued to trend upward for 2024. VPN provider vulnerabilities and compromised credentials remained a consistent theme that caused risk for organizations.

Health-ISAC provided 229 Targeted Alerts to specific Health-ISAC member organizations with potentially vulnerable infrastructure to help teams mitigate common vulnerabilities and exploits (CVEs) and actively exploited vulnerabilities. The most common themes included open and exposed databases, remote access tools, and a PAN-OS weakness.

Open and Exposed Databases

Health-ISAC cooperates with intelligence partners to identify open and exposed databases within health sector organizations. These databases include CouchDB, Elastic, MongoDB, MSSQL, MySQL, and Postgres solutions.

An open and exposed database is accessible to anyone on the internet without authentication or authorization. Threat actors can view, modify, or delete the data in the database, leading to data breaches, data theft, and other security risks.

Healthcare products exposed to the internet can divulge sensitive patient information if they are vulnerable. Health-ISAC has no insight into whether the exposed database contains protected health information (PHI) or personally identifiable data (PII). Targeted Alerts are delivered out of an abundance of caution when open and exposed databases are discovered.

Health-ISAC delivered 26 alerts related to open and exposed databases during Q4 of 2024. The most common exposures are MySQL databases.

PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect (CVE-2024-3400)

On April 12, 2024, Palo Alto Networks announced a critical vulnerability found in PAN-OS software. The command injection vulnerability allows an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. This means an attacker could completely take over the firewall and potentially an entire network.

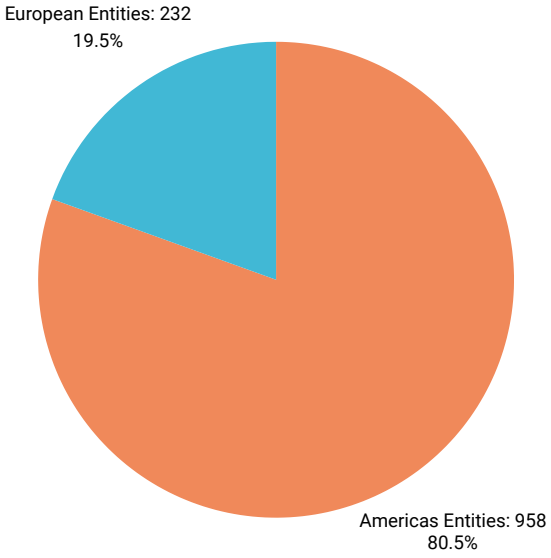
Although this vulnerability was announced in April 2024, Health-ISAC continues to deliver related targeted alerts as this exposure has remained unpatched within multiple environments.

More information is available in the Palo Alto advisory available here.

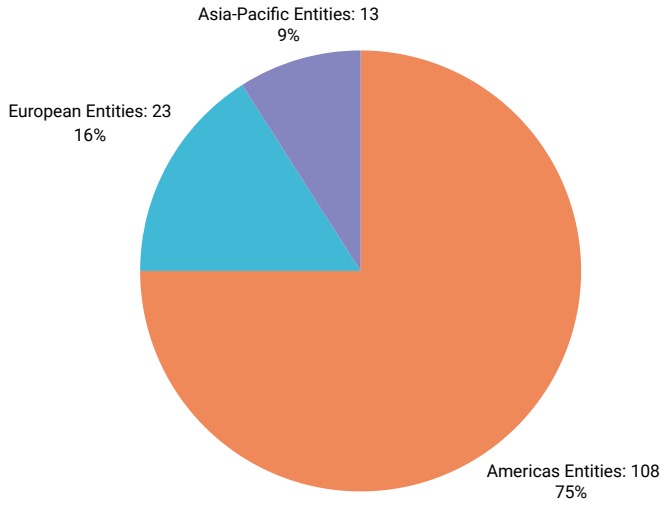
Healthcare Sector Statistics

Global Events Analysis

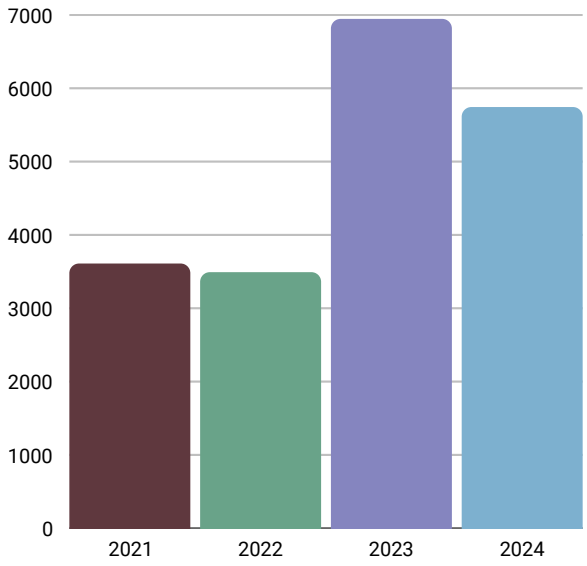
All Sectors: 1,807 Events



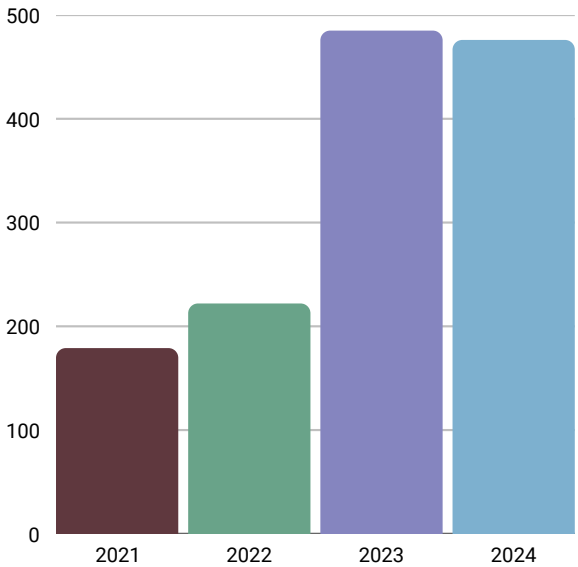
Healthcare Sector: 154 Events (6.2% of All Ransomware Attacks in 2024 Q4)



Total Breaches Tracked: 21,556



Healthcare Sector Breaches: 1,367 (6.3% of Total Breaches Tracked)



Threat Actor Profile: BianLian

BianLian, a Russian-based threat actor, emerged in 2022 as a new ransomware group. Over the following years, the group became one of the most prolific threat actors currently operating in the cybersecurity threat landscape. The healthcare sector is one of the group's main targets, presumably due to valuable data, with several dozens of victims from the sector being listed on their leak website since its operations began. The group employs various tactics, techniques, and procedures (TTPs) to execute sophisticated operations that result in data exfiltration and ultimately extort the victim.

The threat actors collaborate as a cohesive unit, separating themselves from the more common ransomware-as-a-service (RaaS) model used in ransomware operations.

While the name BianLian is connected to Chinese mythology, the group is thought to be operating from Russia. The group uses Russian for internal communications and does not attack Russian-speaking countries, which is common among threat actors of Russian origin.

The group employs a sophisticated attack chain involving a multi-step strategy. It often gains initial access via spear-phishing emails with malicious attachments or compromised Remote Desktop Protocol (RDP) credentials. The group has also targeted exposed VPNs and exploited the ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) to gain a foothold in its victims' systems in previous operations.
Once inside a victim's system, BianLian establishes persistence by implanting custom backdoors and utilizing remote access tools like TeamViewer. This custom backdoor is written in Go and acts as a loader, with its primary function being downloading and executing additional payloads.

The group employs various methods to evade detection, such as disabling antivirus tools using PowerShell and querying the victim's network environment through compiled tools. Their backdoor uses different names and paths, challenging naming-based behavior detection in each incident. Additionally, BianLian utilizes valid accounts for lateral movement within the network, making it more difficult to spot intrusions.

Once the threat actor has successfully accessed sensitive data, they then exfiltrate the files using exfiltration tools like File Transfer Protocol (FTP), Rclone, or Mega. The group then requests ransomware from the victims and threatens to release their data if no payment is made. While they used to operate on a double-extortion model, exfiltrating data and then encrypting the systems, the group moved to exclusively exfiltration at the beginning of 2024.

The group's diverse tactics, techniques, and procedures (TTPs) and evolution over time demonstrate its adaptability and sophistication, making it a formidable enemy. The group is expected to continue posing a significant threat to the healthcare industry. Therefore, healthcare organizations are advised to closely monitor the group's evolving TTPs to protect themselves from potential attacks

Underground Forums Activity

Threat actors frequently advertise stolen data or access to organizations' systems for sale on various underground forums. In some cases, these posts reveal the names of organizations allegedly breached. At the same time, in other instances, the threat actors conceal the victims' identities and provide details such as the company's revenue or sector to indicate the value of the data being auctioned.

Payment is typically demanded in a selected cryptocurrency, and sometimes, these transactions are facilitated by middlemen like forum administrators. Often, threat actors share a sample of the stolen data to demonstrate its legitimacy; however, there are rarely any details regarding the origin of the data.

In Q4 of 2024, there were multiple cases where threat actors tried to sell alleged stolen data which could have potentially impacted the healthcare industry:

Miyako/miyako

On November 14, 2024, a cybercrime forum user, posting under the alias Miyako, advertised root access to the server to an unnamed healthcare organization for $1,500 of undocumented cryptocurrency. The user claimed the organization has an annual revenue of $4 billion USD and that the advertised access would permit entry to the organization’s server hosting firewall.

On November 22, 2024, a cybercrime forum user posting under the alias miyako advertised root access to the server of two unnamed healthcare organizations in two forum advertisements. In the first post, Miyako advertised root access to the server hosting firewall to a healthcare software-as-a-service (SaaS) organization for $300 of unspecified cryptocurrency.

On December 6, 2024, a cybercrime forum user, posting under the alias miyako, advertised root access to a server hosting firewall to an unnamed Medical Practice Management for $300 of unspecified cryptocurrency.

m0riarty

On December 10, a cybercrime forum user, posting under the alias “m0riarty” claimed to publish data allegedly from the software company ProcessMaker—the company services to various industries, including US healthcare and government.

Recommendations

- Patch all of the vulnerable devices in a timely manner.
- Ensure there are up-to-date data backups.
- Continuously work on raising security awareness among employees.
- Segment corporate networks.
- Implement stringent internet access and network controls
- Deploy endpoint protection tools.
- Implement phishing-resistant multi-factor authentication (MFA) across the organization.
- Conduct regular security audits, backup testing, and verification.
- Continuously monitor for any sign of suspicious activity.
- Develop detailed incident response plans to ensure business continuity in the case of a cyberattack.
- Review Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources for additional guidance on how to keep organizations safe from cyberattacks.

References

- BianLian: The Face-Changing Ransomware Menace
- #StopRansomware: BianLian Ransomware Group
- BianLian - SentinelOne
- Threat Assessment: BianLian
- Threat Actor Profile: BianLian