Healthcare Heartbeat

2023: Q4

Cybersecurity Trends and Threats in the Healthcare Sector

Health-ISAC™
Collaborating for Resilience in Healthcare

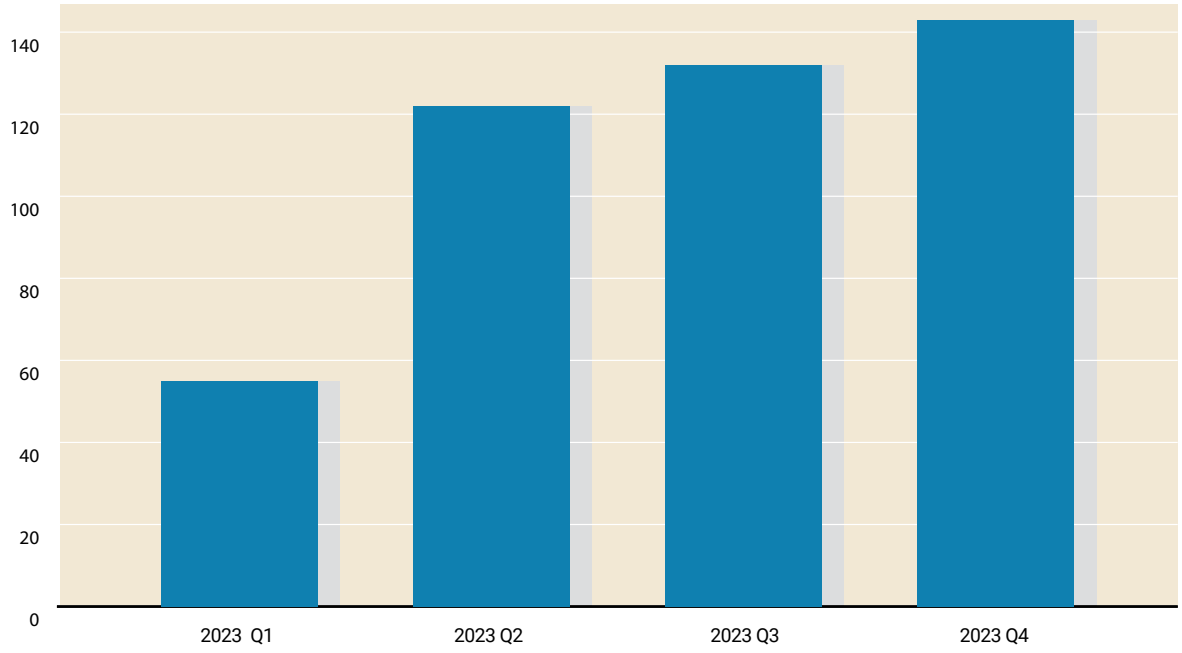
Summary

Health-ISAC's Q4 2023 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 members affiliated with the victim companies or those potentially impacted take appropriate measures to secure critical infrastructure.

If Health-ISAC becomes aware of an imminent threat to members of the healthcare sector, the information will be communicated 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



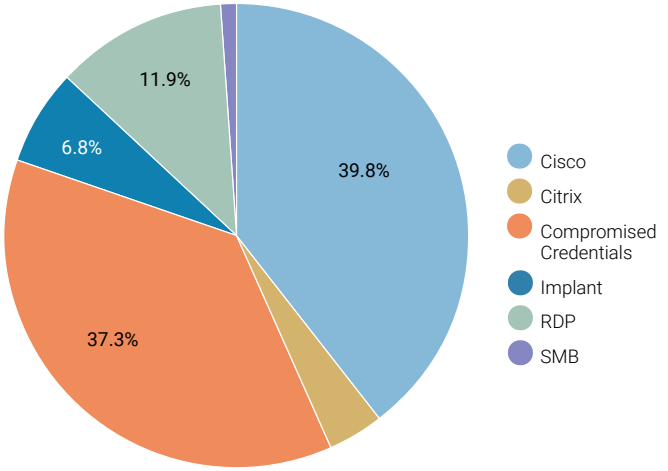
Health-ISAC observed a continuous trend of cyber security incidents and data breaches impacting healthcare over 2023. While RDP exposures and Compromised Credentials remained a consistent theme, the actively exploited Cisco IOS XE bug was of note for many security teams.

Cisco IOS XE

On October 16, 2023, Cisco reported that they were aware of threat actors actively exploiting a privilege escalation vulnerability in Cisco IOS XE software, CVE-2023-20198. The issue affects physical and virtual devices running Cisco IOS XE software with the HTTP or HTTPS Server feature enabled. The flaw has been assigned a critical CVSS score of 10.0.

Health-ISAC provided 39 Targeted Alerts to specific Health-ISAC member organizations with potentially vulnerable interfaces to help teams mitigate the actively exploited vulnerability. In addition to 39 Targeted Alerts related to potentially vulnerable interfaces, Health-ISAC delivered 8 Targeted Alerts to member organizations where threat actors had already installed an implant using the Cisco IOS XE vulnerability.

The Cisco IOS XE bug potential exposure notifications accounted for 39.8% of Targeted Alerts sent to members in Q4 of 2023, and the presence of implants detected alerts accounted for 6.8%.



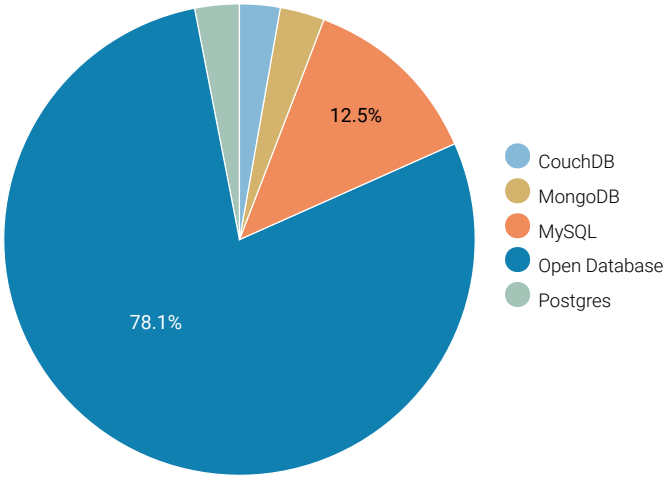
Open Databases

In Q4 of 2023, Health-ISAC began alerting members of open databases that may expose personal health information (PHI) or personally identifiable information (PII). An open database is directly accessible over the internet and requires no authentication.

Exposed Database Alerts include the following technologies:

- CouchDB
- Microsoft SQL
- MongoDB
- MySQL
- Postgres

MySQL instances were the most likely to be exposed for Health-ISAC members. Health-ISAC provides alerts related to open/exposed databases to mitigate the risk of PHI/PII data exposure.



Healthcare Sector Statistics

Global Events Analysis

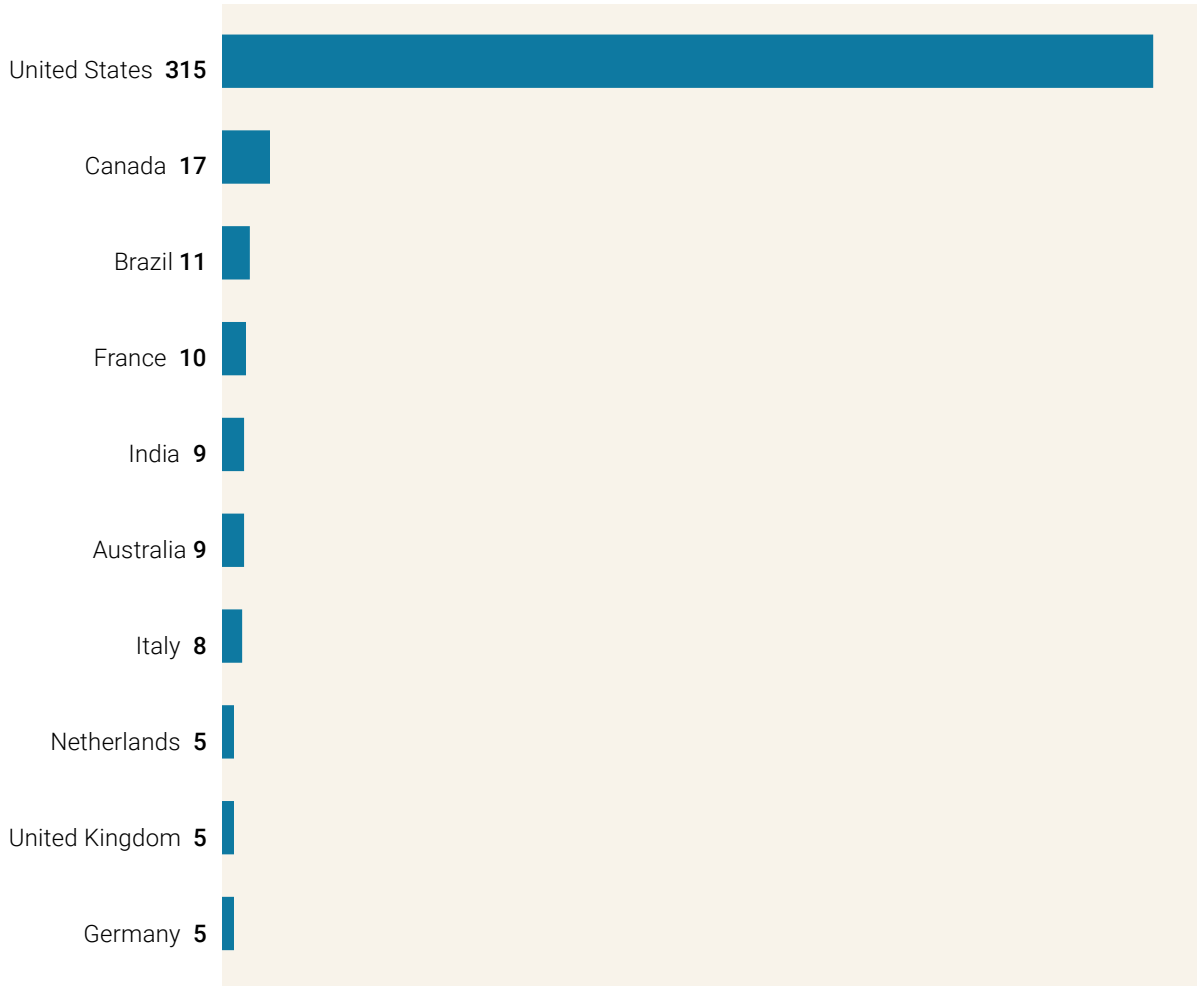
All Sectors: 5,559 Ransomware Events Globally during 2023

- 2,549 Events Impacting Americas Entities
- 884 Events Impacting European Entities

Healthcare Sector: 459 Ransomware Events Globally during 2023

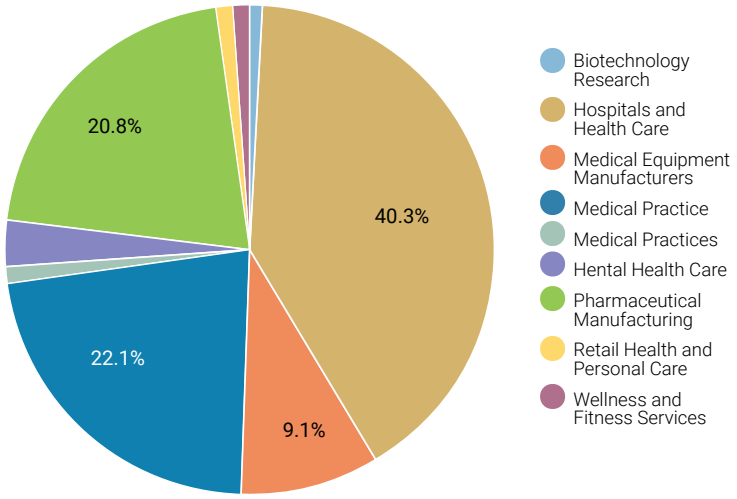
- 379 Events Impacting Americas Healthcare Sector Entities
- 61 Events Impacting European Healthcare Sector Entities
- 19 Events Impacting APAC Healthcare Sector Entities

Top 10 Most Breached Countries



Threat Actor Profile: Hunters International Attacks on Healthcare

Hunters International, a new threat group that presumably began operations in October 2023, drew attention using an aggressive extortion technique exposing private images of patients. While there is limited intelligence regarding the group's operations, Health-ISAC observed targeted attacks against seven healthcare delivery organizations (HDOs), including in Europe and the United States. Considering the threat group's opportunistic targeting, recently observed activity, and disdain for patient privacy, the healthcare sector will likely remain a target of operations.



Analysis

The ransomware used in the attacks orchestrated by Hunters International, though modified, bears similarities to code and infrastructure associated with Hive threat actors. The code is still written in Rust, but modifications include switching to a more standard mode of encryption, simplifying the code, and adding debugging functionality. The new group has reduced the number of command line parameters, streamlined the encryption key storage process, and made the malware less verbose compared to earlier versions.

In the new operation, compromised files have the .locked extension appended once they are encrypted. The threat actor does not immediately specify the ransom amount or payment method but rather provides credentials for victims to access a chat portal to negotiate payment.

The ransomware attempts to disable backup and restore capability by performing a sequence of commands to terminate services and processes used to recover and backup data. Additionally, following the trend of other Ransomware-as-a-Service (RaaS) groups, the actors appear to favor data exfiltration over data encryption.

Hunters International was initially suspected to be a rebrand of the Hive ransomware group, which was dismantled earlier this year in January in a joint international police operation. The correlation between the two groups came after multiple security researchers noticed code overlaps that linked Hive and Hunters International operations. However, in a unique statement published on their leak website, Hunters International refuted the Hive rebranding claims and stated they bought the code and existing infrastructure from Hive, but they had since made changes to the original code for their own operation.

The new threat actor has shown to be particularly aggressive in their extortion techniques. In their first recorded breach of a healthcare organization, a plastic surgery practice, they allegedly leaked private images of patients. With the latest developments in the cyber threat landscape and the increased use of sophisticated tactics, techniques, and procedures by threat actors, it is critical for healthcare organizations to implement rigorous security protocols to ensure the confidentiality of patient data.

Recommendations

- Review the 2023 Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients.
- Conduct employee training to create a cyber awareness culture for non-IT staff in the organization.
- Implement multi-factor authentication and strong password policies or, where possible, switch to passwordless environments to enhance access control.
- Conduct regular security audits and penetration testing to know your organization's weaknesses before the threat actors.
- Establish a patching management policy to ensure your software and systems are patched promptly, and no vulnerabilities expose your organization to an attack.
- Segment your network to limit the attack's impact in case of a compromise.
- In the event of an attack, immediately disconnect and isolate the compromised device from the network to prevent the malware from spreading further.
- In the aftermath of the attack, conduct a thorough investigation, including detailed digital forensics, to establish the full impact of the attack and determine the infection chain.
- Ensure all relevant data is stored as a backup in case of encryption of primary systems.
- Establish good vendor management to avoid falling victim to a compromise through a supply chain.

If you have any questions, please reach out. We hope you find the insights valuable.

References

405(d) Health Industry Cybersecurity Practices
https://405d.hhs.gov/Documents/HICP-Main-508.pdf

Software Fix Availability for Cisco IOS XE Software Web UI Privilege Escalation Vulnerability - CVE-2023-20198
https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-dublin-17121/221128-software-fix-availability-for-cisco-ios.html

Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021
https://jamanetwork.com/journals/jama-health-forum/fullarticle/2799961