Health Sector Heartbeat

2025: Q2

Cybersecurity Trends and Threats to the Health Sector

Health-ISAC®
Collaborating for Resilience in Health

TABLE OF CONTENTS

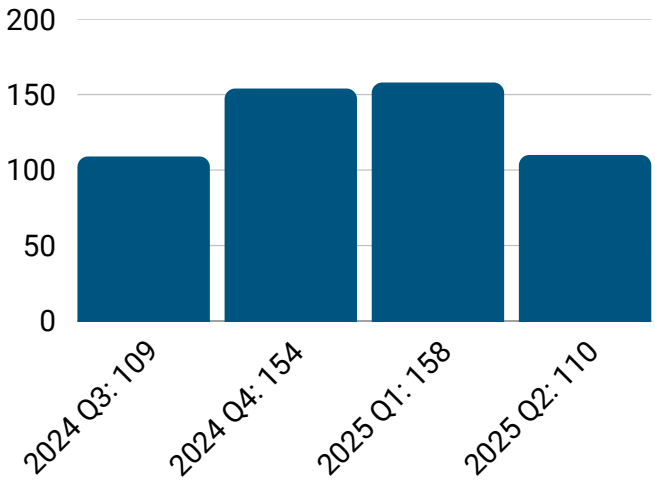
Summary

Health-ISAC's 2025 Q2 Health-ISAC Heartbeat provides observations of ransomware, cybercrime trends, and malicious actor forum postings that could potentially impact health 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 health sector members, 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 in the Health Sector



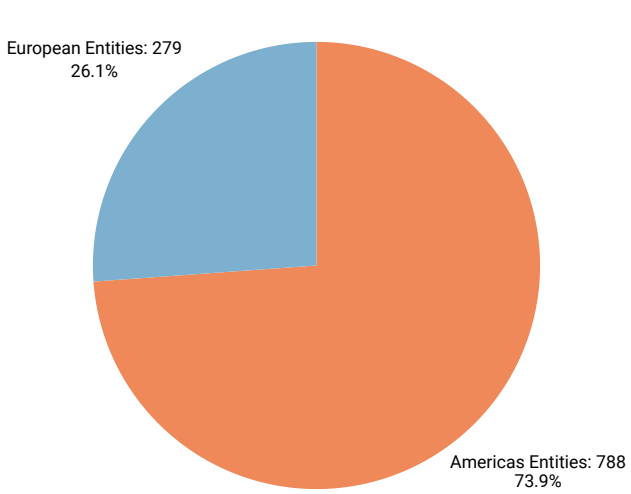
Health-ISAC observed a continuous trend of cybersecurity incidents and data breaches impacting health sector organizations over the past year. While ransomware events saw a continued trend upward for Q4 of 2024 and Q1 of 2025, Q2 appears to show a decrease in overall ransomware incidents. Health-ISAC identified 4,159 incidents across all sectors in Q1 of 2025. 281 of those incidents were health sector incidents. At this rate, 2025 will surpass 2024 in both total incidents and incidents impacting the health sector specifically in comparison to other critical infrastructure sectors.

Health-ISAC provided 466 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, exposed remote access tools, and potentially vulnerable Dangling DNS records.

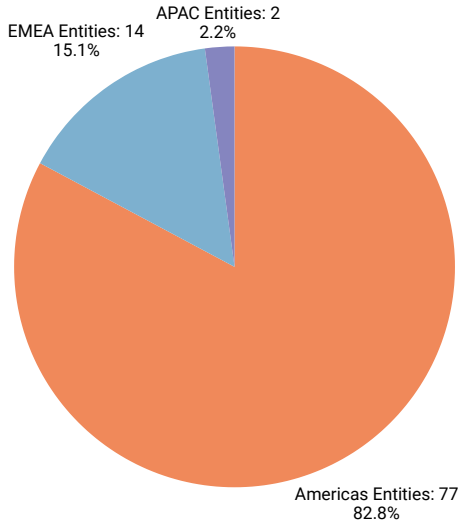
Health Sector Statistics

Global Events Analysis

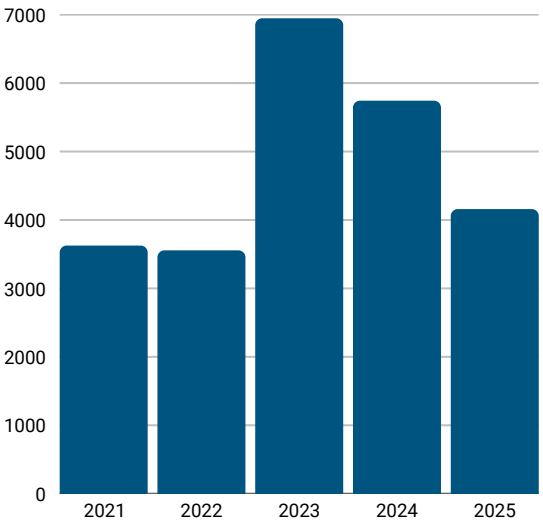
All Sectors: 1,609 Events



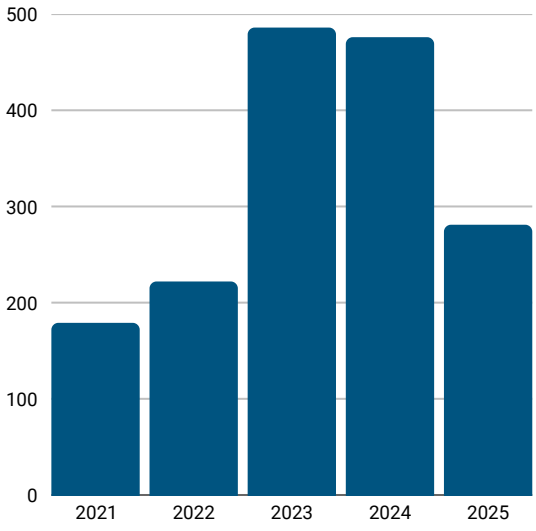
Health Sector: 93 Events (5.8% of All Ransomware Attacks in 2025 Q2)



Total Breaches Tracked: 25,183



Health Sector Breaches: 1,651 (6.6% of Total Breaches Tracked)



Targeted Alert Trends

The most common themes included open and exposed databases, remote access tools, potentially vulnerable Dangling DNS records, and CEO Doxxing.

Surge in Dangling DNS Records in the Health Sector

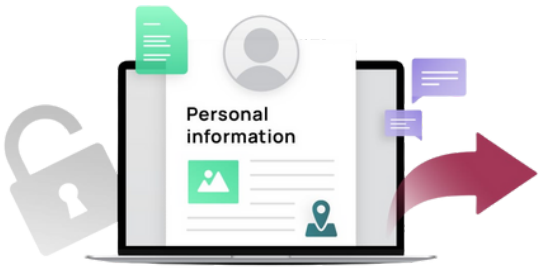
The health sector has witnessed a concerning spike in Dangling DNS findings, a vulnerability that arises when DNS records point to decommissioned or unclaimed resources.

This issue poses significant risks to healthcare organizations, as threat actors can exploit these misconfigurations to hijack domains, redirect traffic to malicious sites, and impersonate trusted entities. Such attacks disrupt critical operations, erode patient trust, and inflict lasting brand damage.

Health-ISAC will continue to deliver Targeted Alerts and Bulletins related to the Dangling DNS Record issue.

Approximately 50% of the Dangling DNS records alerted to members have been remediated and are no longer at risk of being hijacked by threat actors.

Health-ISAC sends follow-up Targeted Alerts to organizations that have not remediated the DNS records 30 days after the initial Targeted Alert.



CEO Doxxing

On May 28, 2025, Health-ISAC reviewed a list of organizations named in a database that contained several member organizations' names. Targeted Alerts were distributed to impacted teams to increase awareness.

On May 28, 2025, a Health-ISAC member shared the URL of a website created in April 2025, and the name is a reference to Luigi Mangione, the individual accused of shooting the UnitedHealthcare CEO. The website, hxxps://play[.]luigiwasright[.]com, was a database hosting details related to the CEOs of many large organizations.

The website lists over 1,000 company CEOs and executives, publicly available business information, possible personal or work mobile numbers, and LinkedIn accounts.

The webpage had an About section that stated the provided information was intended to give individuals the power to contact those in power at the organizations, rather than talking to a customer service agent. Although the intent may have been to provide individuals with the ability to hold corporate leadership accountable, there may be tertiary threats from the data having been located in one location.

This list does not likely pose a significant physical threat to the listed executives; however, a potential threat actor could use the LinkedIn accounts and other sensitive information to target executives.

Reverse phone number searches could lead to a threat actor gaining additional personally identifiable information (PII) on executives, such as residential addresses and family members.

The post was shared in the Health-ISAC Secure Chat #threats-to-c_suite channel, where members can discuss executive protection and threats to executives.

The luigiwasright[.]com website now responds with a 502 bad gateway error, indicating a successful takedown may have occurred. Health-ISAC will continue to monitor the directory's health status for changes.

Health-ISAC released a TLP:AMBER bulletin for the wider community attached to the Targeted Alerts for context.

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 Q2 of 2025, there were multiple cases where threat actors tried to sell alleged stolen data which could have potentially impacted the health sector industry:

Croco Siffredi

On April 25, 2025, a Russian-speaking threat actor operating under the alias Croco Siffredi on XSS cybercriminal forum offering a database of highly sensitive medical and personal information leaked from a well-established health sector company providing MRI services and other high-precision diagnostic services. The threat actor posted an asking price of $20,000.

Croco Siffredi has been active on XSS since at least February 3, 2025, and has previously advertised similar products.

ReyXS

On May 1, 2025, a cybercrime forum posting under the alias ReyXS claimed to advertise shell access to an unnamed healthcare company for $1,200 USD. While not identifying the company's name, ReyXS claimed the company’s annual revenue is roughly $600KK, an abbreviation for $600 million USD.

The threat actor directed interested users to contact them through a provided Tox account. The entry also included the sale of access to two other victim organizations.

Threat Actor Profile: BERT Ransomware

BERT Ransomware is a relatively new threat actor that emerged in April 2025. The group could become a significant threat globally, with its current victims spanning multiple continents, including Asia, Europe, and North America. This financially motivated and opportunistic threat actor has targeted the health, technology, and event services sectors.

BERT is a ransomware strain that, despite using relatively simple code, achieves effective execution through several tactics, including PowerShell-based loaders, privilege escalation, and concurrent file encryption. This ransomware operates on both Windows and Linux operating systems.

On Windows, the infection chain involves utilizing PowerShell scripts as loaders for the ransomware payload. This method enables the attackers to escalate privileges, disable critical security features such as Windows Defender, the firewall, and User Account Control (UAC), and subsequently download and execute the ransomware from a remote IP address. In a recent observed attack, the threat actor was linked to Russian infrastructure, specifically a Russian IP address. However, this connection was not sufficient to establish clear attribution.

The Linux variant of BERT Ransomware uses 50 threads to streamline the encryption process, allowing operators to work quickly and reduce the chances of detection. This version incorporates a JSON-formatted configuration embedded within the binary, making it easier to customize and adapt. Once the encryption is complete, the malware adds the extension encrypted_by_bert to the affected files and displays a Base64-encoded ransom note indicating which files have been encrypted. Researchers from TrendMicro have determined that the group likely reused code from the REvil Linux variant, which was known for targeting ESXi and Linux systems before it was dismantled.

Older variants of BERT ransomware would first enumerate drives, drop ransom notes in every directory, collect valid file paths for encryption, and then proceed with multi-threaded encryption. Newer variants streamline this process by using ConcurrentQueue and creating a DiskWorker on each drive, which allows them to encrypt files as soon as they are discovered. These improvements demonstrate the ability of the operators behind BERT ransomware to evolve and refine their methods.

Impact on the Health Sector

Health sector organizations are prime targets for BERT Ransomware due to the critical nature of their operations and the high value of medical data. The group exploits the sector's reliance on legacy systems, limited cybersecurity budgets, and the critical need for operational continuity. Key impacts include:

- Operational Disruption: Encryption of critical systems leads to downtime, delaying patient care and medical procedures.
- Data Breaches: Theft of sensitive patient data, including medical records, which are highly valuable in the cybercriminal market.
- Financial Losses: Ransom payments, legal fees, regulatory fines, and reputational damage.

The group's tactics, techniques, and procedures (TTPs), as mapped by Broadcom and Cyfirma according to the MITRE ATT&CK Framework:

MITRE ATT&CK: Tactics, Techniques, and Procedures (TTPs)

Execution

- **T1106:** Native API
- **T1059:** Command and Scripting Interpreter
  - **T1059.001:** PowerShell
- **T1204:** User Execution
- **T1053.005:** Scheduled Task

Persistence

- **T1547.001:** Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
- **T1137:** Office Application Startup
- **T1574:** Hijack Execution Flow
  - **T1574.002:** DLL Side-Loading
- **T1543.003:** Create or Modify System Process: Windows Service

Privilege Escalation

- **T1055:** Process Injection
- **T1547.001:** Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (also in Persistence)
- **T1574:** Hijack Execution Flow (also in Persistence)
- **T1548.002:** Bypass User Account Control

Defense Evasion

- **T1027:** Obfuscated Files or Information
- **T1036:** Masquerading
- **T1055:** Process Injection (also in Privilege Escalation)
- **T1070.006:** Indicator Removal: Timestomp
- **T1497:** Virtualization/Sandbox Evasion
- **T1562.001:** Impair Defenses: Disable or Modify Tools
- **T1564.001:** Hide Artifacts: Hidden Files and Directories
- **T1574:** Hijack Execution Flow (also in Persistence/Privilege Escalation)
- **T1140:** Deobfuscate/Decode Files or Information (Implicit in Obfuscation/Deobfuscation)

Credential Access

- **T1056:** Input Capture
- **T1539:** Steal Web Session Cookie.

Lateral Movement

- **T1080:** Taint Shared Content

Collection
- **T1074:** Data Staged

Command and Control
- **T1071:** Application Layer Protocol

Impact
- **T1486:** Data Encrypted for Impact
- **T1490:** Inhibit System Recovery
- **T1489:** Service Stop

Mitigation Strategies

Patch Management
- Regularly update and patch all systems, especially public-facing applications like Citrix NetScaler, to address known vulnerabilities (e.g., CVE-2023-3519).

Email Security
- Implement advanced email filtering solutions to detect and block phishing attempts.
- Train employees to recognize phishing emails and report suspicious activity.

Endpoint Protection
- Deploy endpoint detection and response (EDR) solutions to identify and block malicious activities.
- Enable application whitelisting to prevent unauthorized software execution.

Access Controls
- Enforce the principle of least privilege (PoLP) to limit user access to only what is necessary.
- Implement multi-factor authentication (MFA) for all accounts, especially remote access.

Network Segmentation
- Isolate critical systems within segmented networks to prevent lateral movement.
- Restrict RDP access to only trusted IPs and monitor for unusual activity.

Backup and Recovery
- Maintain regular, offline backups of critical data and test recovery procedures.
- Ensure backups are encrypted and stored in a secure location.

Detection and Response

- Monitor for Indicators of Compromise (IOCs)
  - Look for suspicious activities such as the use of tools like PsExec, WMIC, and Megasync.
  - Monitor for unusual file renaming or deletion patterns.

Incident Response Plan

- Develop and regularly update an incident response plan tailored to ransomware attacks.
- Conduct tabletop exercises to test the plan and improve readiness.

Threat Intelligence

- Leverage threat intelligence feeds to stay informed about emerging threats and IOCs related to INC Ransomware.
- Share threat information with industry peers through organizations like Health-ISAC.

Red Team Exercises

- Conduct regular penetration testing and red team exercises to identify and address vulnerabilities.

Recovery and Resilience

- Use offline backups to restore systems and data without paying the ransom.
- Verify the integrity of restored data to ensure it is free of malware.

Post-Incident Analysis

- Perform a thorough root cause analysis to understand how the attack occurred.
- Implement lessons learned to strengthen defenses and prevent future incidents.

By implementing these measures, health sector organizations can significantly reduce their risk of falling victim to INC Ransomware and other similar threats. The key is to adopt a proactive, layered defense strategy that combines prevention, detection, and response capabilities.

Additional Recommendations:

- Conduct regular scanning for vulnerabilities and subsequent patching of vulnerable devices.
- Maintain regular backups of critical data, including immutable and offline backups.
- Enforce network segmentation and strict network access control policies.
- Implement multi-factor authentication for accounts across the organization.
- Implement anti-phishing tools and regularly raise awareness among staff on relevant social engineering campaigns targeting the sector.
- Continuously monitor for suspicious activities.
- Have an incident response plan ready to limit operational disruptions in the event of a successful attack.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients resources.

References

TrendMicro
SocPrime
Broadcom
Cyfirma
Linux Security