Healthcare Heartbeat

2023: Q3

Cybersecurity Trends and Threats in the Healthcare Sector

Health-ISAC™
Collaborating for Resilience in Healthcare

health-isac.org

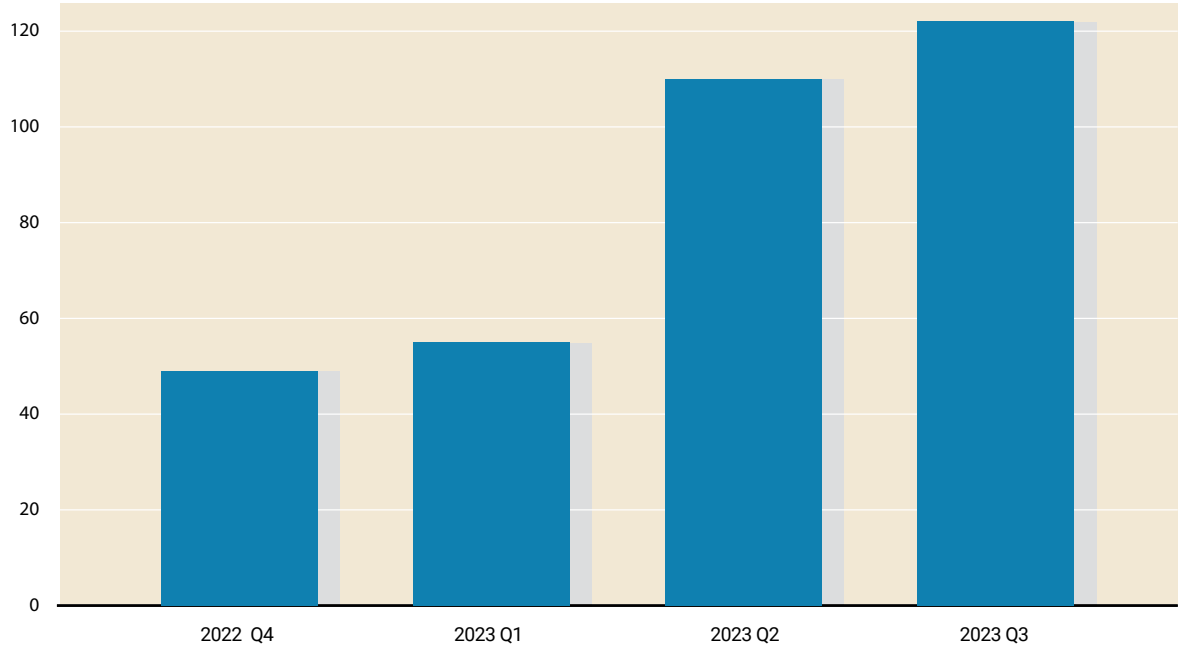
Summary

Health-ISAC's Q3 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.

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 contact@h-isac.org. The TLP:GREEN version of the Healthcare Heartbeat is available for members within the portal.

Ransomware Attacks Against Healthcare



Health-ISAC observed a continuous trend of cyber security incidents and data breaches impacting healthcare over 2021, 2022, and 2023. In 2021, according to Health-ISAC tracking, the average number of healthcare sector ransomware incidents per quarter was 30. In 2022, that number rose slightly to over 32 per quarter. In contrast, the number of ransomware incidents in the healthcare sector in 2023 has increased dramatically, largely due to the Progress MOVEit file transfer vulnerability.

Healthcare Sector Analysis

DICOM Exposure Statistics

Health-ISAC tracks DICOM systems that are available via the internet and require no authentication, ultimately exposing sensitive patient information, including PHI, image files, medical records, and more. DICOM, an international standard for medical images, stands for Digital Imaging and Communication of Medicine. When exposed, DICOM systems provide an attractive attack vector for cybercriminals targeting the healthcare sector.

DICOM systems may also be exposed after phishing attacks and exploitation of known exploited vulnerabilities (KEVs). A lesser-known attack involves threat actors posing as legitimate patients seeking medical services. Threat actors complete all of the necessary paperwork for telemedicine care, then upon request for medical images, deliver trojanized DICOM files. Upon delivery and execution by the recipient, the threat actor gains initial network access.

Additional details on threat actors targeting healthcare are included in the Health-ISAC Alert titled Ransomware Actors Target Healthcare, detailing intercepted CLOP communications that show the group bragged about twice having success infiltrating new victims in the healthcare industry by sending infected files disguised as ultrasound images or other medical documents for a patient seeking a remote consultation.

Health-ISAC has delivered 27 DICOM Targeted Alerts to health sector organizations from October 2021 through September 2023.

RDP Exposure Statistics

Health-ISAC tracks RDP exposures and the remediation status of those exposures. RDP, a native remote desktop protocol within Windows operating systems, is one of the Top 10 most common attack vectors leveraged by actors targeting healthcare. When enabled and exposed to the internet, RDP systems provide an attractive attack vector for cybercriminals targeting the healthcare sector.

Health-ISAC has delivered 79 alerts related to exposed RDP instances since 2020.

Healthcare Sector Statistics

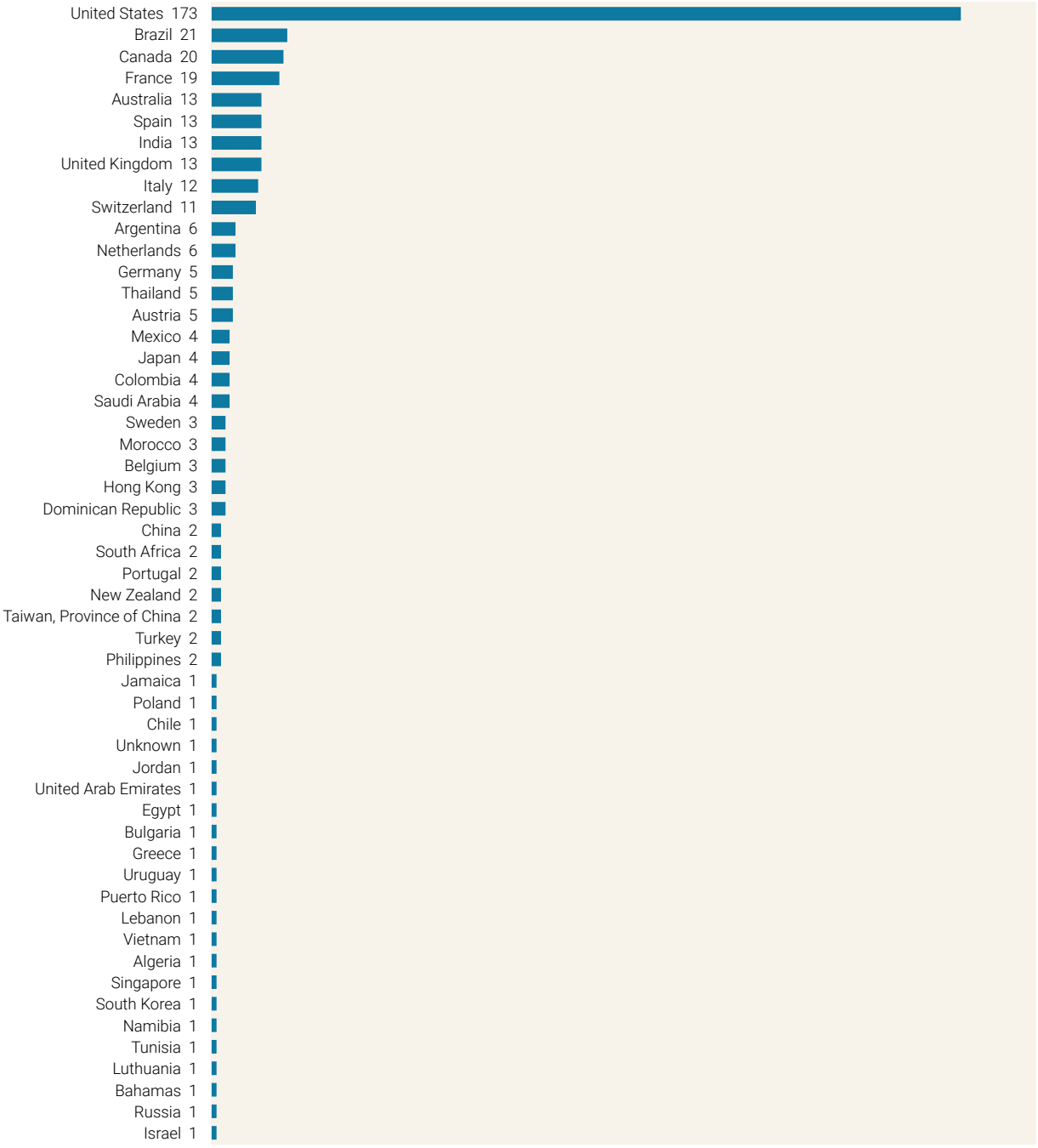
Global Events Analysis

All Sectors: 3,743 Ransomware Events Globally during 2023

- 1,806 Events Impacting Americas Entities
- 584 Events Impacting European Entities

Healthcare Sector: 304 Ransomware Events Globally during 2023

- 207 Events Impacting Americas' Healthcare Sector Entities
- 37 Events Impacting EMEA Healthcare Sector Entities
- 14 Events Impacting APAC Healthcare Sector Entities



Threat Actor Profile: BlackCat/ALPHV Ransomware Group

Health-ISAC is alerting members of the BlackCat/ALPHV ransomware group's increased activities. Since the beginning of this year, Health-ISAC has observed at least 30 ransomware attacks on healthcare facilities orchestrated by BlackCat/ALPHV and its affiliates, as reported by members and intelligence partners. The victims within the industry range from hospitals and medical practices to pharmaceutical companies.

On September 28, 2023, the last alleged attack was revealed on the threat actor's leak website.

In their post, ALPHV claims responsibility for the attack on an unnamed healthcare facility in Michigan. The organization's name is currently unknown, but the group claims to have stolen 6 terabytes of data. As a result, we advise members to remain vigilant and watch for any suspicious conduct or signs of compromise linked to the group's operations.

Analysis

On January 12, 2023, the United States Department of Health and Human Services (HHS) published an alert about BlackCat, also known as ALPHV, AlphaVM, recognizing that their activity threatens the healthcare sector. Health-ISAC previously distributed the original alert, which can be accessed here. Furthermore, in March of this year, in cooperation with Mandiant, Health-ISAC distributed a list of tactics, techniques, and procedures (TTPs) associated with the group.

Since its initial appearance on the cybercrime scene in November 2021, BlackCat has established itself as a stealthy and sophisticated ransomware family, showing continuous evolution, allowing it to evade security solutions and making identifying and countering BlackCat-associated attacks extremely difficult. BlackCat has created strains that are compatible with both Windows and Linux operating systems, as well as novel TTPs such as embedding RSS feeds on their leak website and providing their API to allow direct scraping of their stolen content from their leak website. The group operates as a ransomware-as-a-service (RaaS) provider and uses triple extortion tactics, including ransomware, data leak threats, and DDoS attacks, to achieve its goals.

When it comes to initial access, the group is seen deploying a multitude of techniques, including phishing campaigns, exploit kits, or malicious downloads. Furthermore, the group and its affiliates were observed exploiting the GoAnywhere MFT vulnerability tracked as CVE-2023-0669 for initial access in January 2023 attacks, and Trend Micro also observed BlackCat using malvertising to distribute malware via a cloned webpage of an open-source Windows file transfer application, WinSCP, in June 2023.

The group's arsenal of ransomware tools is constantly evolving, and they are innovative in their deployed TTPs, making their attacks especially difficult to counter. Members are advised to keep alertness at a high level and to apply recommended mitigation strategies.

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 in a timely manner and there are no vulnerabilities exposing 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 as well as to 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

New Ransom Payment Schemes Target Executives, Telemedicine
https://krebsonsecurity.com/2022/12/new-ransom-payment-schemes-target-executives-telemedicine/

Researchers Crawled Search Engines and Searched the Dark Web To Find Out the True Extent of Healthcare Ransomware Attacks
https://www.fiercehealthcare.com/health-tech/new-jama-study-scrapes-dark-web-find-true-frequency-healthcare-ransomware-attacks

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