THREAT LANDSCAPE REPORT

Emerging Threats to the U.S. Healthcare Sector in 2024

www.cyble.com
contact@cyble.com
+1 888 673 2067

CONTENTS

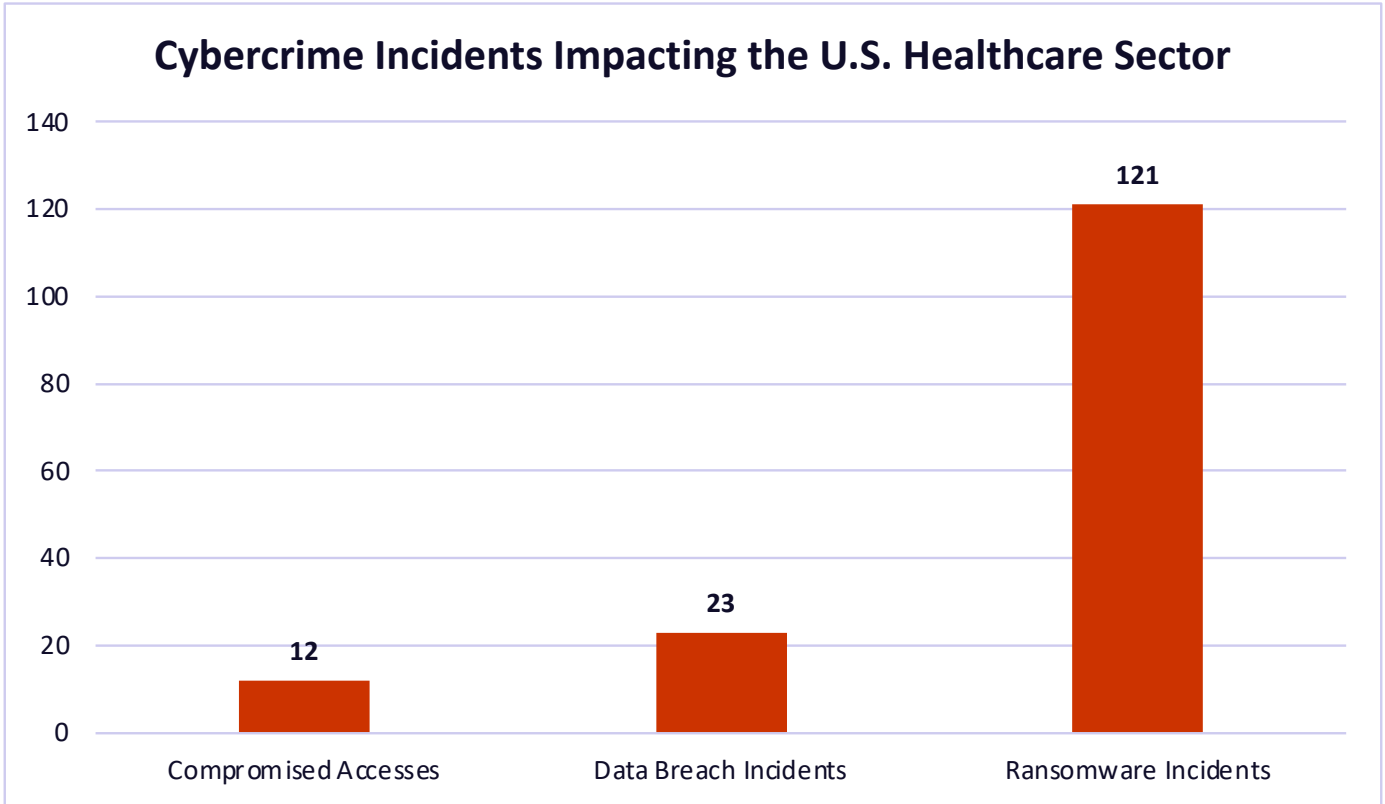
EXECUTIVE SUMMARY

Cyble's cyber threat activity report brings to light specific cyber threat activity targeting the Healthcare sector in the United States from January to June 2024.

In this report, Cyble Research & Intelligence Labs (CRIL) will meticulously outline the cyber security threats targeting the Healthcare sector in the United States and highlight a worrying trend in compromised access sales and data breach incidents. This analysis highlights that 10 distinct threat actors (TAs) and numerous ransomware groups, such as LockBit, ALPHV, and RansomHub, are responsible for 18 verified data breaches and 121 ransomware attacks impacting Healthcare providers like United Seating and Mobility, Numotion, and Change Healthcare.

These attacks were highly targeted in nature, as we can conclude from the sheer scale of compromised network accesses for sale, most prominently including the auction of an American clinical laboratory's network credentials and access sale to a U.S. teleradiology company.

This report extensively covers ransomware and the evolving threat it poses. Over $1.1 billion in ransom payments have been paid worldwide, further evidenced by the attempted takedown of the LockBit infrastructure in global law enforcement actions.

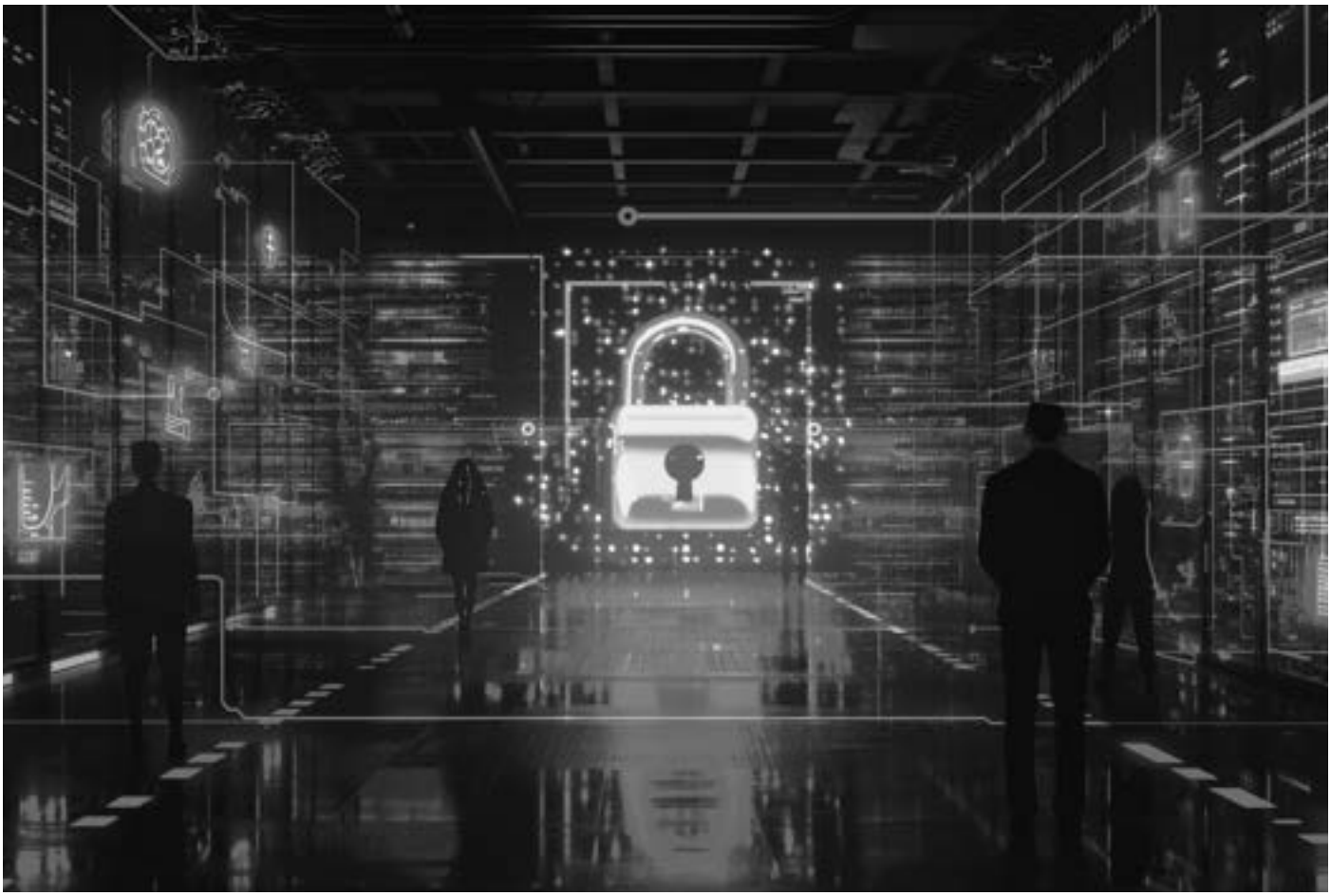


INITIAL ACCESSES ON SALE

Between January 1 and June 30, 2024, Cyble Research & Intelligence Labs (CRIL) has meticulously monitored and analyzed cybercrime forums for the sale of compromised accesses across various sectors. During this period, we identified 10 incidents in the Healthcare sector wherein access credentials were compromised and subsequently offered for sale on different underground marketplaces.

This finding is particularly alarming because it underscores the significant cybersecurity risks faced by the Healthcare industry. Such unauthorized access could potentially lead to data breaches, compromising patient privacy and the integrity of Healthcare services, a breach in doctor-patient confidentiality, and other severe consequences. This highlights a critical need for enhanced cybersecurity measures and vigilance among Healthcare providers to protect against such intrusions.

11 distinct TAs were identified, each responsible for posting once about their illicit offerings. This diversity of actors suggests a fragmented approach to targeting the Healthcare sector, with no single entity dominating during the observed period.



NOTABLE ACCESSES ON SALE

Alleged Access to an Addiction Recovery and Support Institute of the U.S. State Government on Private Sale

On February 2, 2024, a TA on a darkweb forum auctioned administrative access to the SQL server via remote desktop protocol (RDP) belonging to an undisclosed American Healthcare Institute with significant revenue. The TA had mentioned that the allegedly compromised server was protected with Windows Defender. Recent information from a source suggested that the TA continued to privately sell access to the SQL server after receiving a ban on the forum and disclosed the names of the entities to which they allegedly gained access.

American Clinical Laboratory Network Access Illegally Auctioned

Threat activity concerning an undisclosed American full-service clinical laboratory was announced by a TA on a Russian cybercrime forum in February 2024. The TA later claimed to have successfully auctioned the unauthorized access to the clinical laboratory's network, which boasts a substantial yearly revenue of USD 56.6 million and employs 200 people. The TA further disclosed that the compromised network consists of 130 active hosts, specifically pointing out the exclusion of systems operating on Linux.

Unauthorized Sale Offer of Access to U.S. Teleradiology Company Reported

On March 12, 2024, a TA reportedly offered unauthorized access for sale on a darkweb forum. This access, which was through RDP, belonged to a U.S.-based teleradiology services company. The TA claimed the access included domain administrative privileges without disclosing a price. Due to the absence of comprehensive details, the legitimacy of these claims could not be verified, casting a shadow over the security posture of entities involved in sensitive Healthcare data handling.

TA Offering Unauthorized Access to U.S.-based Healthcare Organizations

In June, a TA offered access to a U.S.-based Healthcare organization on a cybercrime forum. The TA alleged that this included CRM system usernames and passwords. They went on to back up their claims by sharing proof of compromise, demonstrating their ability to access the web-based client application interface used by the affected entity for administrative purposes and clinical management.

Earlier in June, the same TA was also observed privately offering unauthorized access to the CRM systems of a major pharmaceutical firm, including login credentials, on the same cybercrime forum. According to the TA, the compromised CRM is also linked to the affected entity's affiliated centers or hospitals, thereby putting protected health information (PHI) at risk. The TA released a proof of compromise showcasing their access to this CRM system as well.

DATA BREACHES AND LEAKS

CRIL has detected and verified 18 data breach incidents over the past six months that have directly impacted the Healthcare industry in the United States. These incidents have been observed across various cybercrime forums and a diverse group of TAs, highlighting a significant threat to the confidentiality, integrity, and availability of sensitive patient information.

NOTABLE DATA BREACHES AND LEAKS

Ransomware Group Offers Data of U.S. Healthcare Provider for Sale on Cybercrime Forum

On February 1, 2024, a TA with supposed ties to a major ransomware group was reportedly selling data belonging to a U.S.-based Healthcare provider on a cybercrime forum. This move comes after the ransomware group had previously announced the Healthcare provider as a victim on their Tor-based data leak site on January 12, 2024. The data set, which is being offered for USD 20,000, allegedly contains 1.8 TB of sensitive information, including medical records, client and employee details, and passports.

While the TA has not provided definitive proof of the compromise, multiple screenshots were shared to support these claims. This incident underscores the evolving tactics of ransomware groups, which are increasingly exploring various methods to monetize stolen data or apply pressure on victims to comply with their demands, especially in cases where direct extortion efforts prove challenging.

Patient Data Breach at Major Hospital's Labs Potentially Affects Thousands

On March 28, 2024, an alarming cybersecurity incident was brought to light. An acknowledged TA put forth an offer on a Russian cybercrime forum to sell 60 GB of data purportedly swiped from a U.S.-based Hospital and its research facilities. The compromised database is believed to contain Personally Identifiable Information (PII) of an undisclosed number of patients. In an effort to substantiate the claim of the database breach, the TA provided a screenshot along with a PDF document. These attachments included scanned copies of consent forms from the implicated entity. These forms were filled out by patients and included sensitive personal details such as names, dates of birth, phone numbers, physical addresses, and Social Security Numbers (SSNs), thereby underscoring the potential gravity of the privacy violation.

HealthEquity Inc. Reports a Data Breach of PHI from Health Savings Accounts

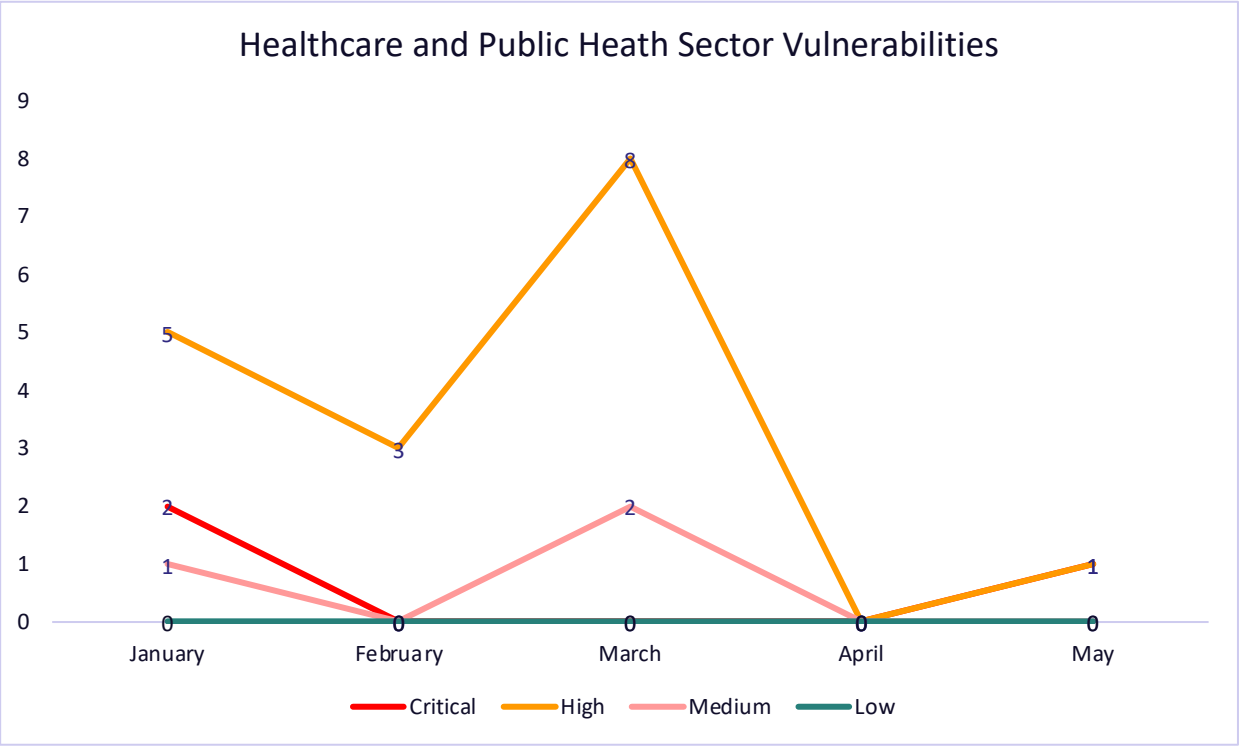
HealthEquity Inc. reported a data breach in March 2024 affecting the PHI from its Health Savings Accounts (HSAs). In their disclosure to U.S. authorities on July 2, 2024, HealthEquity mentioned that an illicit user accessed the company's database through a personal device belonging to an undisclosed business partner, using compromised user credentials.

This TA proceeded to exfiltrate an unknown amount of PHI from the company's database to the partner's computer. It's worth noting that Health Equity has also been the victim of cyberattacks in the past, with a phishing attack in 2018 and a ransomware attack by the CL0P group exploiting the MOVEit vulnerability in 2023.

However, in this incident, further internal investigations have not revealed any disruption to their business operations or malicious persistence on their networks.

VULNERABILITY INSIGHTS

For the period from January 1, 2024, to June 30, 2024, CRIL observed a 130% increase in vulnerabilities disclosed within a wide range of products used in the Healthcare and Public Health sectors compared to the same period last year.

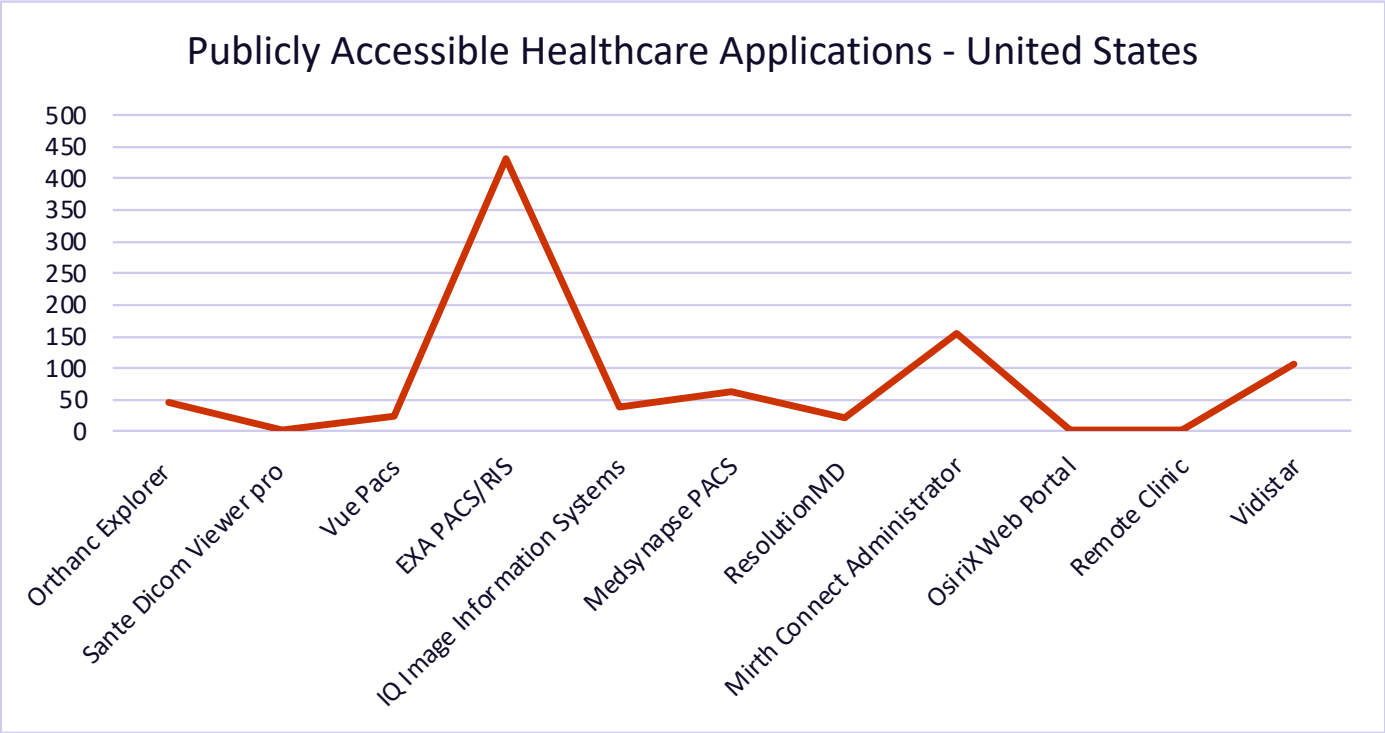


CRIL researchers observed that vulnerable products fall into various categories within the Healthcare and Public Health sectors, including medical imaging, simulation software, remote connectivity and management, medical device monitoring, configuration tools, engineering design software, and health screening devices. The majority of vulnerabilities disclosed for the given timeline fall under two categories: medical imaging solutions and simulation software.

`

CRITICAL EXPOSURES

CRIL researchers investigated internet-exposed assets pertaining to the United States. They observed that hundreds of Picture Archiving and Communication Systems (PACS) and Digital Imaging and Communications in Medicine (DICOM) from various vendors are remotely reachable and might be targeted by TAs to gain access to confidential PHI. The figure below depicts the number of public-facing Healthcare applications.



The above graph does not represent vulnerable applications but rather provides a holistic view into the attack surface that TAs can leverage to target public-private entities dealing within the Healthcare and Public Health sectors.

CRIL researchers believe that the risk of exploitation of limited products (above graph) intensifies with the existence of known vulnerabilities publicly available in them. The use of outdated Healthcare applications provides an easy entry point to attackers as these products have multiple high-severity vulnerabilities.

Recently, in May 2024, the Cybersecurity and Infrastructure Security Agency (CISA) added Unauthenticated Remote Code Execution (CVE-2024-43208, announced in October 2023) to its Known Exploited Vulnerability (KEV) catalog, impacting a widely used Healthcare application. Based on the evidence of active exploitation, the

corporation of this critical vulnerability in KEV, with the availability of publicly available exploit and 155 internet-exposed instances in the U.S., highlights one of the major risks for the U.S. Healthcare industry.

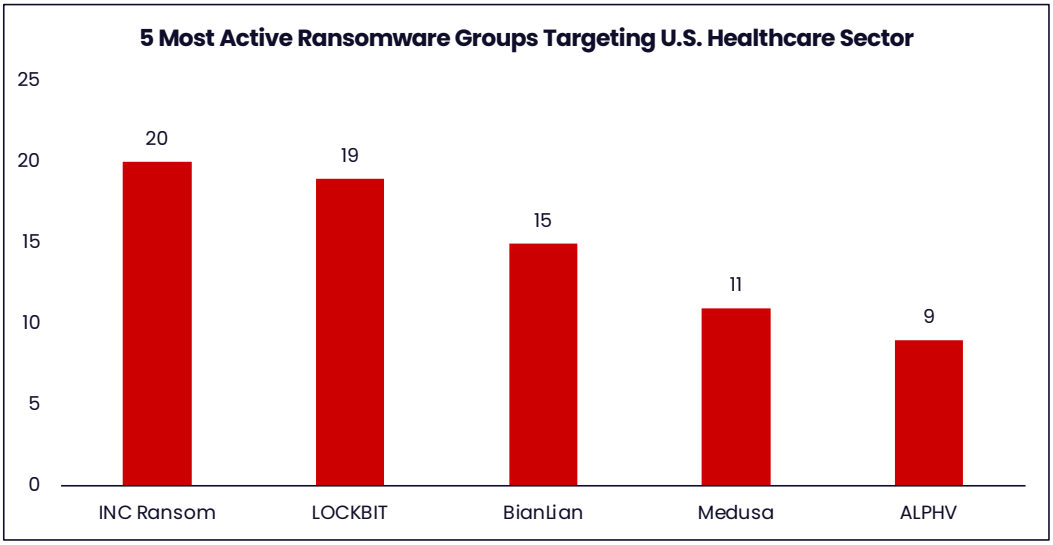
The severity of this vulnerability can also be highlighted by the fact that Chinese APT Storm-1175, known for deploying Medusa ransomware in their recent attacks on the Healthcare sector, may have weaponized this vulnerability for maximum impact.

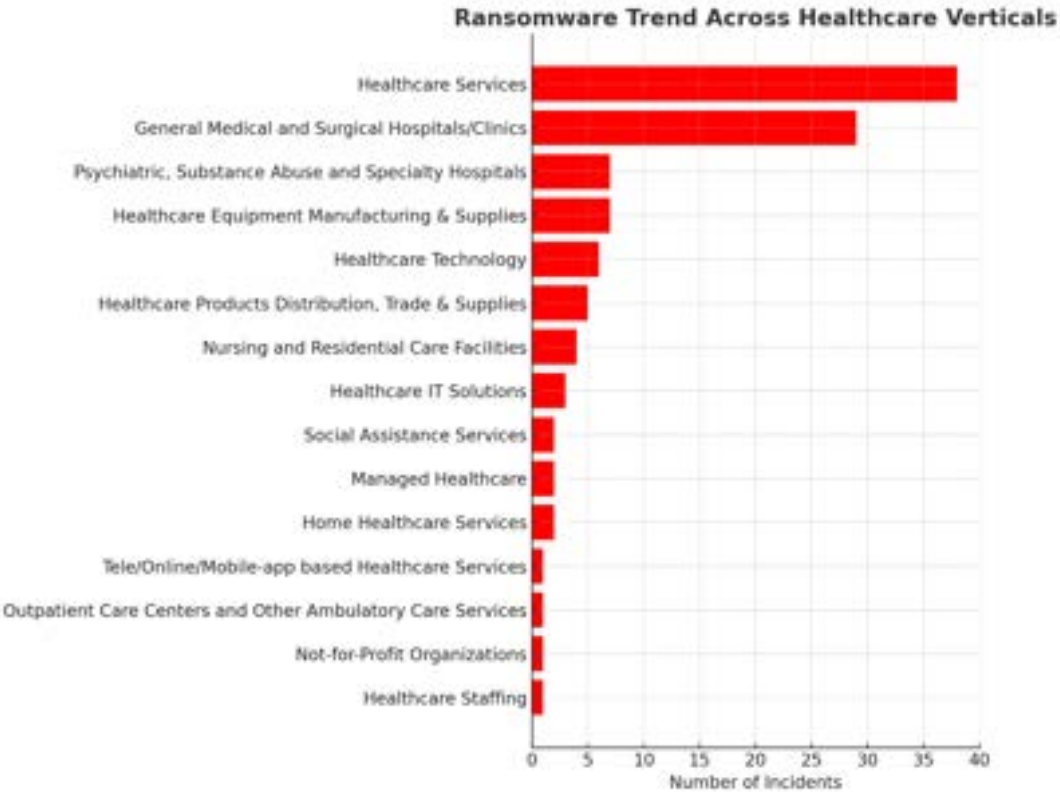
CRIL researchers observed that the risk in the U.S. Healthcare industry originates not only from internet-exposed Healthcare applications but also from networking devices, virtualization software, and secure access solutions.

Upon investigation, it was found that multiple hospitals in the United States are relying on these various Healthcare applications. These products have been lucrative targets for TAs in the past, and CRIL researchers strongly believe that in the near future, the same products might be used to gain access to Healthcare facilities in the United States.

RANSOMWARE THREATS

CRIL, closely monitoring the ransomware attacks on the Healthcare sector in the United States, detected a concerning spate of 121 ransomware attacks in the last six months. Ransomware groups such as Inc Ransom, LOCKBIT, BianLian, Medusa, 8Base, ALPHV, Qilin, Ransomhub, Rhysida, and ThreeAM were among the perpetrators identified, targeting a wide range of Healthcare organizations.





Notable Ransomware Attacks

ALPHV Claims Compromise of BrightStarCare

ALPHV claimed to have compromised Healthcare and assisted living service provider BrightStarCare and threatened to report the breach to the U.S. Department of Health and Human Services.

Change Healthcare Compromise Claimed by Two Different Ransomware Groups; Supply Chain Attacks Threatened

In February, the ALPHV ransomware group claimed to have successfully compromised Change Healthcare, a subsidiary of United Health Group, threatening to target its clients and claiming to have exfiltrated over 6 TB of data from the company's production environment. This data allegedly included personal information, medical and dental records, payment information, claims information, product source codes, and insurance records, including the PHI of U.S. Military Personnel. ALPHV named several big clients of Change Healthcare that may have been impacted due to this data breach.

Notably, the group turned down initial speculations from cybersecurity firms that it had leveraged the ConnectWise exploit to gain initial access to Change Healthcare's networks.

In April, RansomHub, another prominent ransomware group, claimed to have exfiltrated 4 TB of Change Healthcare's data. It claimed that ALPHV "stole" the ransom and threatened to sell this data to the highest bidder following non-payment of the ransom within the stipulated timeline. It is worth mentioning that the description of the documents shared by RansomHub is similar to the ALPHV breach post.

Hunters Ransomware Group Targets Carespring, Which Suffers from Its Second Ransomware Attack in a Year

The Hunters ransomware group claimed to target Carespring, a Healthcare management company, allegedly exfiltrating 391.4 GB of data containing 182,725 files. However, no samples were published as proof of compromise, and no deadline for leaking the data was provided. Notably, the company was previously targeted by the NoEscape ransomware group in November 2023.

Dermatology Clinic and Customer Intermediary Organization Targeted by BianLian

The BianLian ransomware group claimed to target the Better Business Bureau, a U.S.-based business rating and customer intermediary organization. It allegedly exfiltrated 1.2 TB of data, including financial data, files from the CFO, archives, and business files, and posted executives' email addresses and contact information.

The group also claimed to have targeted U.S. Dermatology Partners, a dermatology clinic chain. It claimed to have exfiltrated 300 GB of data, including accounting, budget, contracts, and NDAs and posted executives' emails and phone numbers.

CONCLUSION

The Healthcare industry is the custodian of a vast trove of sensitive data such as PHI, research and development, and valuable technology, making it a lucrative target for cybercriminals. With the increasing implementation of technology in the sector, it is inevitable that the threat footprint also accordingly increases, broadening the scope for attacks on automation tools, third-party vendors, and other avenues for compromise that threaten the industry.

The U.S. Healthcare industry's increasing reliance on technology and the scale of its growth necessitate a dedicated effort and commitment to proactively secure cyber assets, PHI, intellectual property, and research.

Recommended mitigation strategies include enhanced surveillance of underground marketplaces, robust cybersecurity defenses, and proactive threat intelligence efforts. The report also calls for sector-wide collaboration and intelligence sharing to preempt future incidents. This comprehensive overview underscores the urgent need for improved cybersecurity measures and a proactive cyber defense posture within the Healthcare sector to protect sensitive patient information and Healthcare services from the ever-evolving cyber threat landscape.

RECOMMENDATIONS

- Implement proper network segmentation to prevent attackers from performing lateral movement and minimize the exposure of critical assets over the internet.
- Keeping software, firmware, and applications updated with the latest patches and mitigations released by the official vendor is necessary to prevent attackers from exploiting vulnerabilities.
- Engage with industry partners, government agencies, and cybersecurity organizations to stay updated on the latest threats, share information, and collaborate on cybersecurity initiatives.
- Implement robust monitoring systems to detect and respond to any unusual or suspicious activities in real time.
- Conduct regular assessments to identify vulnerabilities and weaknesses in systems and networks and perform penetration testing to simulate real-world attacks.
- Provide regular training and education to employees on cybersecurity best practices, such as identifying phishing emails, using strong passwords, and reporting suspicious activities.
- Ensure that access to sensitive data and systems is granted only to authorized individuals and implement strong authentication mechanisms, such as multi-factor authentication.

OUR INVESTORS

BLACKBIRD · KING RIVER · Xoogler.co · Singtel innov8 · Aditya Birla Bizlabs · Summit Peak · Y · Spider Capital

CYBLE®

About Cyble

Cyble (YC W21) is a leading global cyber intelligence firm that helps organizations manage cyber risks by utilizing patent-pending AI-powered threat intelligence. With a focus on gathering intelligence from the deep, dark, and surface web, the company has quickly established itself as one of the pioneers in the space. Cyble has received recognition from Forbes and other esteemed organizations for its cutting-edge threat research.

The company is well-known for its contributions to the cybersecurity community and has been recognized by organizations such as Facebook, Cisco, and the US Government. To learn more about Cyble, visit www.cyble.com

contact@cyble.com I +1 888 673 2067

11175 Cicero Drive Suite, 100 Alpharetta, GA 30022, US.