CYBLE

Cybersecurity in the Healthcare Industry: Opening Pandora's Box

Table Of Contents

OVERVIEW 3

THREAT VECTORS & ATTACK SURFACE 4

» RANSOMWARE INCIDENTS 5

» THREAT GROUPS TARGETING HEALTHCARE SECTOR 5

» INCIDENTS FROM UNDERGROUND FORUMS 9

» INTERNET EXPOSURE OF MEDICAL DEVICES AND APPLICATION 12

» MISCONFIGURATIONS LEADING TO DATA LEAKS 13

» VULNERABILITIES 14

SENSOR INTELLIGENCE 15

PREDICTIONS 16

CONCLUSION 17

RECOMMENDATIONS 18

REFERENCES 18

Overview

In times to come, the Healthcare industry faces a new challenge – an e-pandemic of cyberattacks in 2023. Based on data from government references, over 44 million health records were leaked in the US alone in 2022. In the first quarter of 2023, we have already observed breaches of over 25 million worldwide patient records in underground forums. These breaches are far higher than in the pre-pandemic and pandemic periods.

In terms of cyber threats to the Healthcare sector, we saw numerous long-standing tendencies like ransomware attacks, data breaches, etc. Threat actors evolved with new tools and techniques to destabilize the industry, especially weaponizing the numerous sector-specific vulnerabilities reported in 2022.

In 2022, cyberattacks on advanced Healthcare facilities like India-based, All India Institute of Medical Sciences (AIIMS) led to the disruption of caregiving facilities and the threat of the leak of sensitive health information of several high-profile patients in the country.

Similarly, the attack on Shields Healthcare group in the US in May 2022 led to the compromise of over 2 million patient records. A misconfiguration at Advocate Aurora Health's website tracking for patients led to the exposure of 3 million patient information.

It is, therefore, imperative to safeguard Protected Health Information (PHI) due to the growing interest of threat actors in acquiring such datasets via cybercrime channels. Unauthorized access by TAs to PHI databases may lead to database compromise, which can be used for financial gain and can lead to various other identity theft attacks. Moreover, losing access to medical records may jeopardize patient safety and care delivery.

The pandemic has led to increased research of drugs and vaccines to prepare for future viruses and counter their spread. State-backed threat actors also aim for medical research and governance organizations to steal sensitive information that can disrupt the research or gain information about disease control in that nation. A similar situation was created when the Indian Council of Medical Research (ICMR) in November 2022 suffered an onslaught of DDoS attacks.

Last year also saw the sector's third-party and supply chain vendors being particularly targeted by cybercriminals to disrupt Healthcare services.

Further, the Healthcare industry's increased interdependence on the Internet of Medical Things (IoMT) and growing network of these devices to facilitate effective, connected, and smarter health services; have provided a larger attack surface to the threat actors.

Cyble Research & Intelligence Labs (CRIL) monitors ongoing developments in the cybercrime ecosystem and cybersecurity risks affecting the Healthcare industry.

Threat Vectors & Attack Surface

The Healthcare sector faces numerous challenges in safeguarding its cybersecurity. CRIL investigated the various factors posing a threat to PHI data loss, and these are:

- Ransomware Attacks
- Data Breaches
- Compromised Access Sales
- DDoS Attacks
- Misconfigured Cloud Storage
- Vulnerable IoMT Devices
- Internet Exposed Healthcare Devices
- Network and Email Servers
- Electronic Health Records (EHR) Systems
- Employees

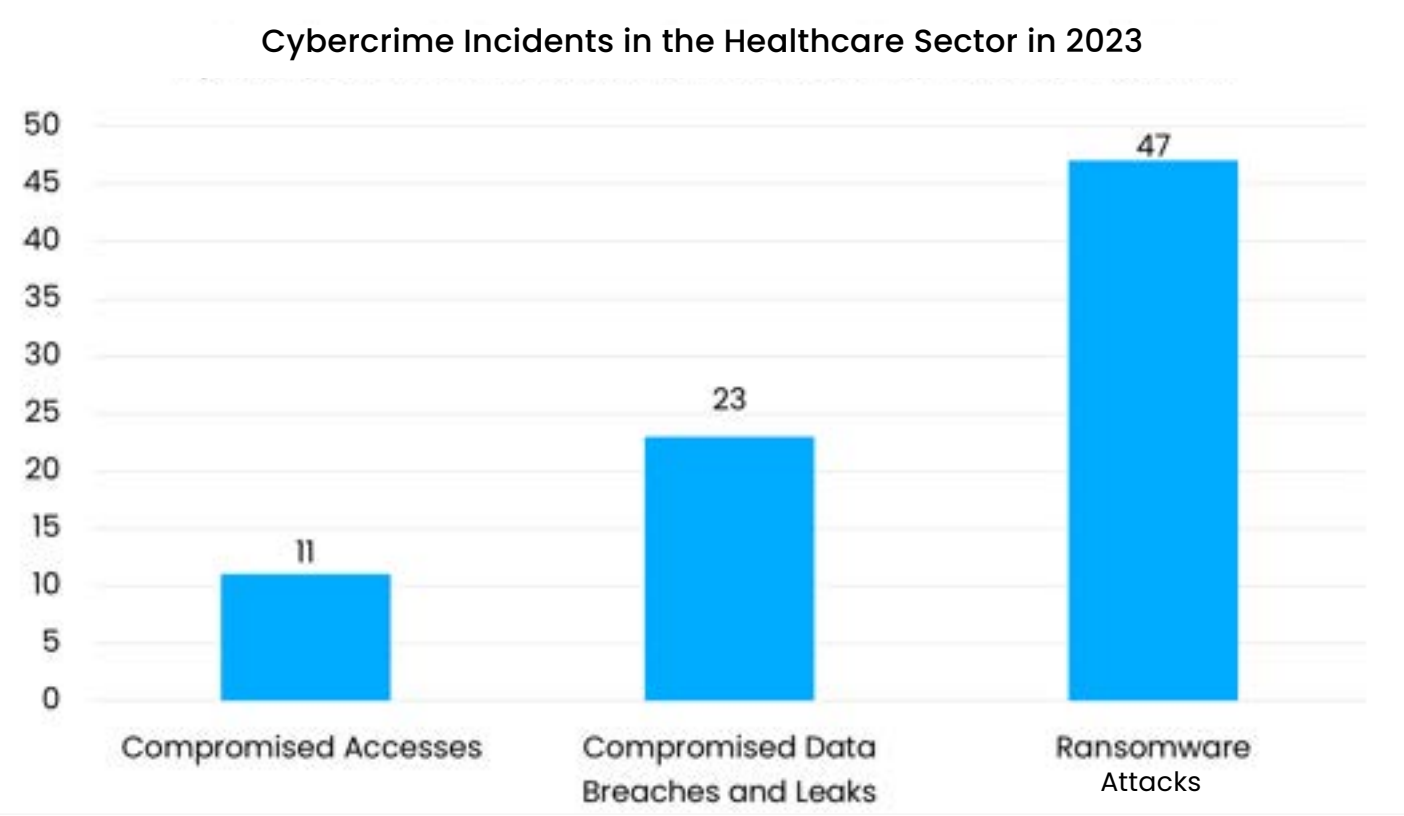


Figure 1: Cybercrime Incidents in the Healthcare Sector in 2023

Threat Vectors & Attack Surface

RANSOMWARE INCIDENTS

Healthcare organizations heavily depend on patient data access to maintain their operations. Ransomware attacks on this critical sector are not only cybercrimes but a threat to human life as ransomware attacks directly impact the hospitals' infrastructure and compromise their ability to provide suitable care to patients, putting them at risk.

In early 2023, we have come across 47 attacks impacting the sector. These attacks are acknowledged by ransomware groups due to failed negotiations, whereas the real number can be much higher. From this trend, we have observed that, on average, a Healthcare company is compromised by ransomware attacks every two days.

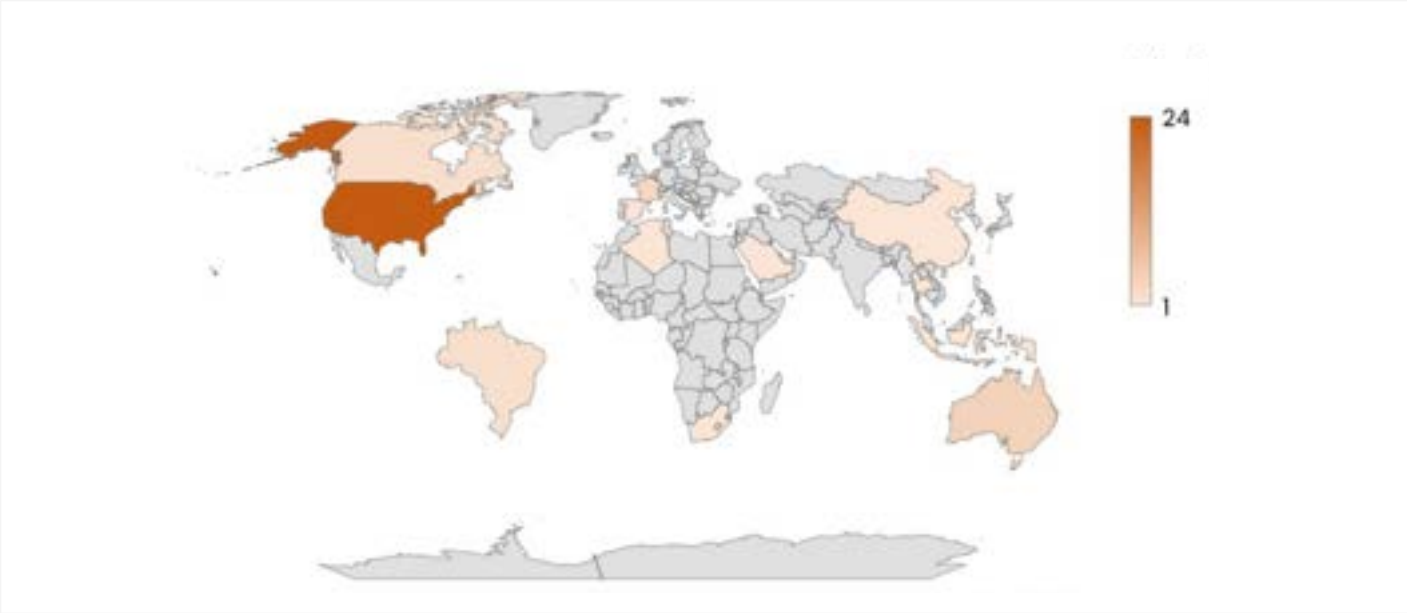


Figure 2: Ransomware Incidents Targeting Healthcare Sector 2023

THREAT GROUPS TARGETING HEALTHCARE SECTOR

The various types of threat groups observed to be attacking Healthcare and associated industries are:

LOCKBIT 3.0

The LOCKBIT ransomware group has evolved over the years, especially since the LOCKBIT Black or LOCKBIT 3.0 builder was leaked at the end of 2022.

As reported earlier in February 2023, The LOCKBIT ransomware operation has recently progressed to a new version, referred to as "LOCKBIT Green", the fourth iteration of their ransomware. It uses an encryptor derived from the leaked source code of Conti ransomware.

LOCKBIT has significantly increased its activities since December 2022 and continues to be among the most notorious group in 2023, targeting 15 Healthcare organizations to date.

Threat Vectors & Attack Surface

Alphavm

This prolific ransomware, also known as Noberus, BlackCat, AlphaVM, Coreid, FIN7, Carbon Spider, or ALPHV, was first observed in November 2021. It is coded in Rust language and extends Ransomware-as-a-Service (RaaS). Alphavm group utilizes the triple extortion methodology on their victims and has suspected links with the previously active, Russia-based REvil ransomware group. ALPHV Ransomware groups are constantly adopting different extortion techniques, such as extending a searchable database from victim data in June 2022.

Threat Actors (TAs) using the ransomware have also been spotted evolving their tactics by leveraging a new version of the Exmatter (data exfiltration tool) and an information stealer called Eamfo as part of their attack chain.

BianLian

BianLian, a Go language-based ransomware group that emerged in late-2021. The group uses a double-extortion technique to pressurize their victims. BianLian has been observed to be specifically targeting the Healthcare sector in 2023.

Lorenz

Lorenz ransomware, first discovered in early- 2021, shares many similarities with sZ40 and ThunderCrypt ransomware.

CL0P

CL0P ransomware group was first discovered in February 2019 and is considered a successor to CryptoMix ransomware, which is believed to have originated in Russia and is frequently used by various Russian affiliates, including Threat Actor (TA) FIN11. The ransomware has both Linux and Windows variants.

The Clop ransomware group has been recently observed exploiting a zero-day vulnerability in the Fortra GoAnywhere MFT solution to steal data and extort companies. GoAnywhere MFT had previously alerted its customers in February 2023 about the Remote Code Execution vulnerability that was being exploited on exposed administrative consoles.

Royal

Royal ransomware is currently one of the most active ransomware groups targeting the Healthcare Industry. It has been active since January 2022 and was known as “Zeon” before rebranding itself in September 2022. It is understood to be run by experienced cybercriminals with a history of involvement with the Conti group. Unlike many other ransomware operations, Royal does not offer its services to affiliates but instead operates as a private group.

Initially, the group used encryptors from other ransomware operations, such as BlackCat. After rebranding, however, they began using a new encryptor to generate ransom notes under their current name.

The ransomware group recently developed a Linux variant targeting ESXi servers.

Unlike other ransomware groups, Royal actors do not typically include ransom amounts and payment instructions in their initial ransom note. Instead, victims are directed to a .onion URL via the Tor browser to interact with the threat actor. Ransom demands made by the group have ranged anywhere from ~$1 million to $11 million in Bitcoin.

Threat Vectors & Attack Surface

Medusa

The Medusa ransomware group was first detected back in September 2019 and was particularly notorious during the pandemic. It operates under the RaaS model. The group has recently been observed targeting open Remote Desktop Protocol (RDP) ports – adopting a new technique to gain an initial foothold, apart from phishing and spam emails.

APT41

APT41, aka Wicked Panda, is reported to be a Chinese state-sponsored threat group that has been active since 2012.

Deep Panda

Deep Panda, aka APT19, Shell Crew, WebMasters, KungFu Kittens, Black Vine, and PinkPanther, is a suspected Chinese threat group targeting the Healthcare sector.

EXOTIC LILY

EXOTIC LILY is a financially motivated group that has been closely linked with Wizard Spider and the deployment of ransomware, including Conti and Diavol. EXOTIC LILY may be acting as an initial access broker for other malicious actors and has targeted a wide range of industries, including Healthcare, since at least September 2021.

FIN4

FIN4 is a financially motivated threat group that has targeted confidential information related to the public financial market, particularly regarding Healthcare and Pharmaceutical companies, since at least 2013.

Fox Kitten

Fox Kitten, aka UNC757, Parisite, Pioneer Kitten, is a threat actor with suspected ties to the Iranian government that has been active since at least 2017 against entities in the Middle East, North Africa, Europe, Australia, and North America.

LAPSUS$

LAPSUS$ is a threat group that has been active since at least mid-2021. LAPSUS$ specializes in large-scale social engineering and extortion operations.

Leviathan

Leviathan aka MUDCARP, Kryptonite Panda, Gadolinium, BRONZE MOHAWK, TEMP.Jumper, APT40, TEMP. Periscope is a Chinese state-sponsored cyber espionage group that has been attributed to the Ministry of State Security's (MSS) Hainan State Security Department and an affiliated front company.

menuPass

menuPass, aka Cicada, POTASSIUM, Stone Panda, APT10, Red Apollo, CVNX, and HOGFISH, is a threat group that has been active since at least 2006. Individual members of menuPass are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company.

Threat Vectors & Attack Surface

Orangeworm

Orangeworm is a group that has targeted organizations in the Healthcare sector in the United States, Europe, and Asia since at least 2015.

Tonto Team

Tonto Team, aka Earth Akhlut, BRONZE HUNTLEY, CactusPete, Karma Panda is a suspected Chinese state-sponsored cyber espionage threat group that has primarily targeted South Korea, Japan, Taiwan, and the United States since at least 2009; by 2020, they expanded operations to include other Asian as well as Eastern European countries.

Tropic Trooper

Tropic Trooper, aka Pirate Panda, KeyBoy, has been active since 2011 and has led targeted campaigns against targets in Taiwan, the Philippines, and Hong Kong.

Whitefly

Whitefly is a cyber espionage group that has been operating since at least 2017. The group has targeted organizations based mostly in Singapore.

Killnet

In early 2023, hacktivist group KillNet began actively targeting the US Healthcare industry with Distributed Denial-Of-Service (DDoS) cyberattacks. KillNet is known to sympathize with Russia and is actively targeting Ukraine and other nations supporting Ukraine with DDoS attacks.

Threat Vectors & Attack Surface

INCIDENTS FROM UNDERGROUND FORUMS

Threat actors leverage the anonymity of underground forums to buy and sell unauthorized accesses and data, which are then used as initial vectors for large-scale cyberattacks. In the first quarter of 2023, CRIL observed and investigated the following noteworthy leads from the underground forums:

» A TA was observed selling the VPN and MS Office accesses of 7 users of a health insurance provider in Brazil, with revenue of USD 308 Million. The TA also claimed that the accesses are from multiple departments such as IT, Auditing, Finance, etc.

Figure 3: Brazilian Healthcare Company's Access on Sale

» A TA offered to sell a Cisco Anyconnect VPN client and Microsoft Office 365 account of an undisclosed Medical Equipment Manufacturing organization with USD 2.1 Billion in revenue.

Figure 4: User Access to a Medical Equipment Manufacturer's VPN and Microsoft Office 365 account on sale

Threat Vectors & Attack Surface

» A nefarious and persistent initial access broker known for selling compromised high-revenue companies' access was observed auctioning the domain and enterprise administrator account of an undisclosed US-based Medical Devices & Equipment manufacturer. The USD 10 Billion revenue company's 150 TB compromised data was also being auctioned along with the access.

Figure 5: Admin Access to an undisclosed US-based Medical Devices & Equipment Manufacturer on Sale

» A TA offered to sell a database of 3 million users, allegedly belonging to an Asian country's Ministry of Health.

Figure 6: Excerpt from TA's post

Threat Vectors & Attack Surface

» A Threat Actor leaked an Indian hospital database containing patient and doctor information. The same TA has also consistently been leaking Healthcare data from other countries.

Figure 7: Indian Hospital Database on Sale

» A TA leaked a dataset related to a US-based health insurance provider, containing a database of consumers as well as the source code of the website.

Figure 8: Data of US-based Health Insurance Provider on Sale

Threat Vectors & Attack Surface

INTERNET EXPOSURE OF MEDICAL DEVICES AND APPLICATIONS

The increasing use of Internet of Things (IoT) devices and web-based applications in the public Healthcare sector has provided numerous benefits to patients, Healthcare providers, and organizations.

These devices and applications are critical for performing day-to-day activities such as transferring data, storing patient records, and keeping track of patient's health history. However, their widespread use has also resulted in a broader attack surface for malicious attackers, which can have devastating consequences for patients, organizations, and the national public Healthcare sector.

When these devices and applications are exposed to the public network, they become vulnerable to cyberattacks. Attackers can gain unauthorized access to these assets, manipulate them, and corrupt the stored data. This can compromise patient safety, violate their privacy, and even result in fatalities. Additionally, a breach in the Healthcare network can cause severe damage to the organization's reputation and financial losses.

Moreover, Healthcare devices are often interconnected, creating a complex web of vulnerabilities that attackers can exploit to gain access to the organization's network. Once inside, they can move laterally, escalate privileges, and exfiltrate sensitive data. This can be particularly dangerous in the public Healthcare sector, where the stored data often includes personal and sensitive information such as medical history, Social Security Numbers, and financial information.

CRIL investigated various assets belonging to the Healthcare Industry, including Electronic Health Record systems, Medical Practice Management Software, Patient Monitoring Systems, Health Management Information systems, PACS, DICOM, etc.

During our investigation, we found over **seven thousand** exposed assets in the Healthcare industry.

The figure below shows a graphical representation of the same.

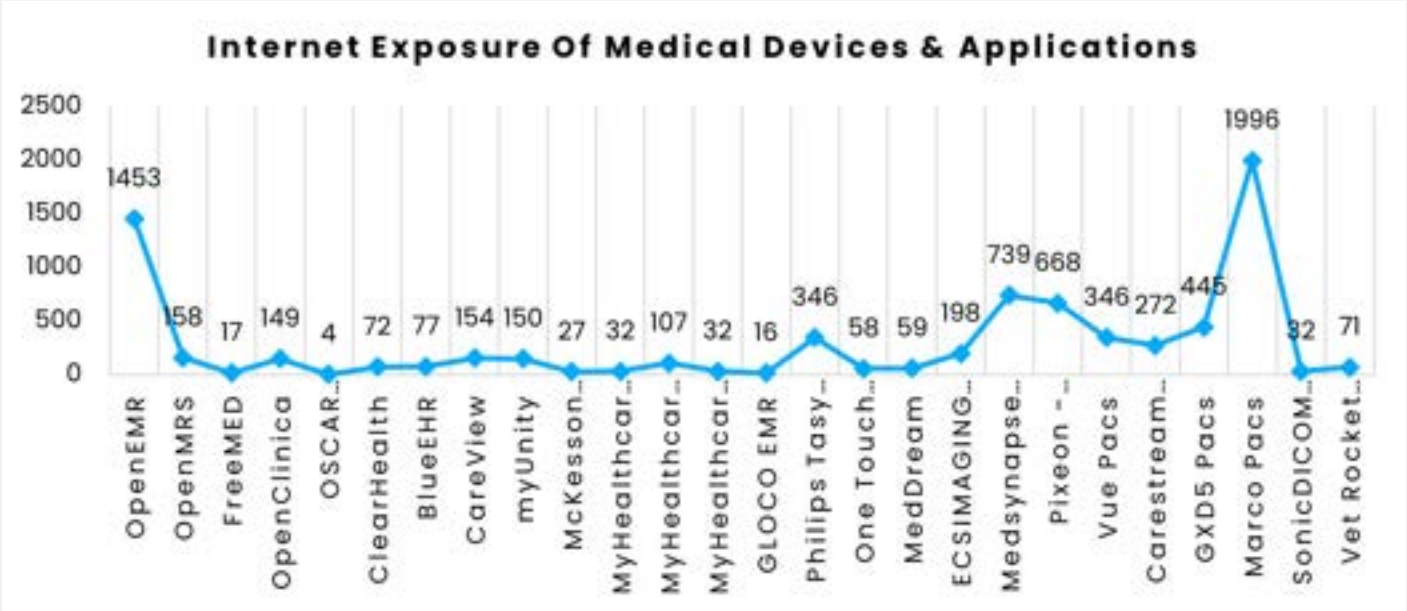


Figure 9: Internet Exposure of Medical Devices & Applications Note: Exposed instances do not indicate vulnerable products

In conclusion, while using IoT devices and web-based applications in the public Healthcare sector provides numerous benefits, it also creates a broad attack surface that malicious attackers can exploit. Securing these devices and applications is critical to ensure patient safety and protect the organization's network, and failure to do so can have catastrophic consequences.

Threat Vectors & Attack Surface

MISCONFIGURATIONS LEADING TO DATA LEAKS

During our investigation, we found several directories are exposed over the internet. These directories can leak PHI data, including patient records, PII, medical records, etc. The image below shows a graphical representation of internet-exposed misconfigured directories leaking PHI.

Figure 10: Misconfigured Instances Exposing PHI

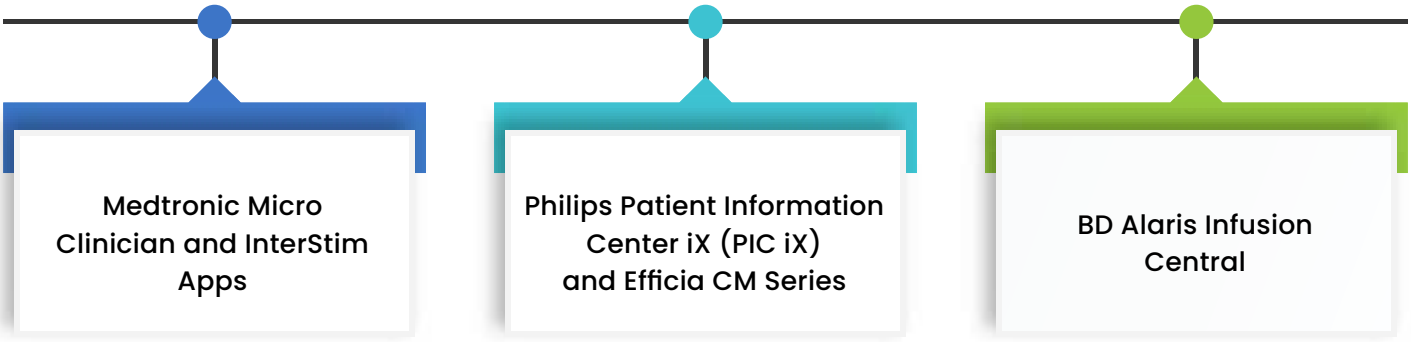
Threat Vectors & Attack Surface

VULNERABILITIES

Several vulnerabilities exist in the public Healthcare sector due to outdated technology systems, lack of proper cybersecurity measures, and limited resources. Many Public Healthcare organizations are still using legacy systems that are no longer supported by vendors, leaving them vulnerable to attacks. Additionally, the Healthcare sector holds a vast amount of sensitive patient data, making it an attractive target for hackers.

The Cybersecurity and Infrastructure Agency (CISA) regularly releases security alerts and advisories related to the Public Healthcare sector to notify owners of the affected product to update their firmware or follow the mitigation steps provided by the official vendor.

Between 01 January 2023 and 15 March 2023, CISA released 3 ICS Medical Advisories. Details for the same are given below:



But apart from these Medical specific security alerts, a massive amount of vulnerabilities are being reported, researched, and published daily. These vulnerabilities might belong to assets falling under Information Technology (IT) or the Internet of Things (IoT), which are heavily relied upon by the Healthcare sector.

Multiple internet-exposed assets shown in Figure-9 have Critical and High Severity vulnerabilities in them. Given below are two examples of the same.

OpenEMR	Picture Archiving and Communication System (PACS)
One online scanner shows nearly **1,500 OpenEMR exposed over the internet.** OpenEMR is a free and open-source Electronic Health Record (EHR) and medical practice management software. It includes features such as patient scheduling, electronic prescribing, medical billing, and clinical documentation. There are over 50+ exploits available & 100+ vulnerabilities for various versions of OpenEMR. Last month, a High-Severity vulnerability (CVE-2023-22973) was published for OpenEMR.	Picture Archiving and Communication Systems (PACS) are a type of medical imaging technology used by Healthcare organizations to store, retrieve, manage, and distribute digital medical images and related patient information. There are **thousands of PACS exposed over the internet,** and multiple exploits and vulnerabilities exist within them.

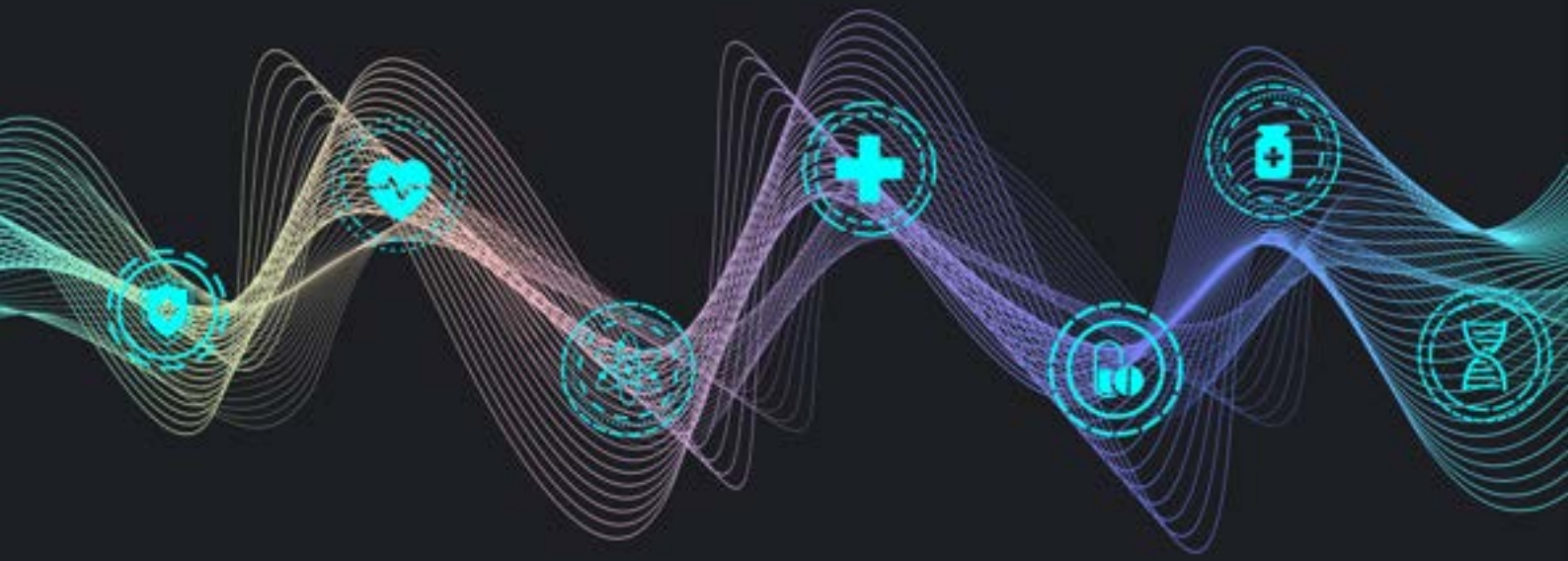
Besides the vulnerabilities discovered in IT devices, medical devices such as fitness trackers, remote patient monitoring systems, building automation systems, smart wearables, and other smart technologies also have flaws that malicious attackers can exploit.

Sensor Intelligence

CRIL monitors Threat Actors targeting medical devices via its CGSI sensors. The figure below shows exploitation attempts on a medical device from 01 January 2023 to 13 March 2023.

Figure 11: Exploitation attempts on a medical device

CGSI sensors picked up high exploitation attempts near the end of February. The findings point out that medical devices are still under the scope of attackers, and TAs are actively scanning the internet for medical devices for exploitation.



Predictions

Ransomware attacks will surely continue targeting Healthcare organizations, potentially causing disruptions to patient care and significant financial damage. These attacks are becoming more sophisticated, and cybercriminals are increasingly using social engineering tactics to gain access to Healthcare systems.

The growth of IoT and IoMT in Healthcare is likely to continue, creating an increasingly complex threat landscape. The proliferation of connected devices will create more potential vulnerabilities for cybercriminals to exploit. It will be important for Healthcare organizations to implement strong security controls to protect against these threats.

Machine Learning (ML) and Artificial Intelligence (AI) are increasingly being used in the Healthcare sector to improve patient outcomes and reduce costs. However, these technologies also create new security risks, and Healthcare organizations must ensure that they are implementing appropriate security controls to protect against AI-based attacks.

Smart wearables, such as fitness trackers and smartwatches, are becoming increasingly popular in the Healthcare sector as they can track vital signs, monitor activity levels, and provide other health-related data, including a significant amount of sensitive data about the wearer, such as their heart rate, activity levels, and sleep patterns. This data can be vulnerable to hacking, and if it falls into the wrong hands, it can be used for identity theft, insurance fraud, or other malicious activities.

The recent geopolitical turmoil will disrupt supply chains, making it more difficult for Healthcare organizations to obtain critical medical supplies and equipment. Threat actors may exploit these disruptions by launching supply chain attacks, compromising the integrity of medical devices and other supplies.

In the coming months, we will see an increase in PHI data leaks. TAs will further utilize these leaks to create distrust among the public, launch social engineering attacks on HVTs, and sabotage the brand reputation of the victim organizations.

Threat Actors are likely to launch more cyberattacks on research facilities and personnel dealing with these facilities to gain access to confidential medical research.

In the coming months, we will likely see TAs spreading malicious mobile applications masquerading as Government Healthcare schemes and plans.

With the development of nanomedicine technology for improved theranostics, potential threats from ransomware and state-backed actors are likely to increase in the next three years.

Conclusion

Cyberattacks like ransomware and Denial of Service attacks are a threat to patient health as well the digital infrastructure of the Healthcare industry. Delays in tests and procedures due to the inaccessibility of medical infrastructure caused by a cyberattack may lead to catastrophe. Losing access to medical records may jeopardize patient safety and care delivery.

To effectively protect patient data and maintain trust in the Healthcare system, Healthcare organizations need to stay up to date on the latest security threats and best practices for mitigating them. Collaboration and information-sharing between Healthcare organizations, government agencies, and security experts will play a critical role in identifying and responding to emerging threats in real-time.

Darkweb monitoring for organizations dealing in the Healthcare industry is necessary with the barrage of PHI data and access of Healthcare industries being sold for monetary purposes.

Recommendations

Enterprises may implement the following measures to counter such cyberattacks:

- If supported by the medical device, use antivirus software on an endpoint. If not supported, provide integrity verification whenever the device is disconnected for service and before it is reconnected to the IT network.
- Encrypt medical device data while in transit and at rest.
- Utilize Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) solutions provide visibility on medical devices and offer protection.
- Ensure that default passwords are changed to secure and complex passwords specific for each medical device. If supported by a medical device, limit the number of login attempts per user.
- Maintain an electronic inventory management system for all medical devices and associated software, including vendor-developed software components, operating systems, version, and model numbers.
- Use inventory results to identify critical medical devices, operational properties, and maintenance timeframes.
- Consider replacement options for affected medical devices as part of the purchasing process. If replacing the medical device is not feasible, take other mitigation precautions, such as isolating the device from the network or auditing the device's network activities.
- Work with manufacturers to help mitigate vulnerabilities on operational medical devices.
- Monitor and review medical devices' software vulnerabilities disclosures by vendors and conduct independent vulnerability assessments.
- Implement a routine vulnerability scan before installing any new medical device onto the operating IT network.
- Implement required training for employees on identifying and reporting potential threats, including insider threats.
- Continuous education and awareness to the employees and third-party vendors to avoid spear-phishing campaigns.

References

1. https://www.cisa.gov/news-events/alerts/2023/03/02/fbi-and-cisa-release-stopransomware-royal-ransomware
2. https://attack.mitre.org/groups/

About us

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.

To learn more about Cyble, visit www.cyble.com