SOCRadar®
Your Eyes Beyond

US HEALTHCARE THREAT LANDSCAPE REPORT

"The Data Breaches in U.S. Healthcare Industry Are on The Rise"

socradar.io

Executive Summary

According to the United States (US) federal records, healthcare breaches have exposed 385 million patient records from 2010 to 2022. These breaches can result in significant financial losses for healthcare organizations and potentially harm patients whose sensitive information is compromised.

The healthcare industry in the US has witnessed a significant increase in data breaches, with cybercriminals exploiting vulnerabilities in healthcare systems and networks. These breaches compromise sensitive patient information, including personal identifiable (PII), medical records, and insurance details.

Ransomware attacks have become a pervasive threat to the healthcare industry. Sophisticated threat actors leverage attack vectors, such as phishing emails, vulnerable software, and misconfigured systems, to gain unauthorized access and encrypt critical healthcare data. These attacks often result in substantial financial losses, operational disruptions, and compromised patient care.

The consequences of cybersecurity incidents in the healthcare industry extend beyond financial losses. The compromised integrity and availability of patient data can hinder critical healthcare services, resulting in delayed diagnoses, disrupted treatments, and potential harm to patient safety. The urgency to enhance cybersecurity measures is crucial to safeguard patient welfare.

Healthcare organizations face significant challenges in meeting regulatory compliance requirements, particularly concerning the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. The consequences of non-compliance can include legal repercussions, reputational damage, and substantial financial penalties.

Cyber threat actors continually adapt their tactics, techniques, and procedures (TTPs) to exploit vulnerabilities within the healthcare industry. The emergence of new attack vectors, including supply chain attacks and zero-day vulnerabilities, emphasizes the need for continuous monitoring, vulnerability management, and proactive threat intelligence.

SOCRadar's US Healthcare Industry Threat Landscape Report provides an overview of recent healthcare data breaches and cyber-attacks, highlighting the risks and consequences of such incidents.

Key Findings

- SOCRadar has reported a **35%** global rise in dark web posts regarding healthcare in the past year, with over **450** documented posts.
- In the last **12** months, **119** healthcare industry-related posts were reported in SOCRadar's Dark Web News Module for the US.
- The dark web posts targeting the healthcare industry in US are about buying, selling, and sharing illegal access to systems and illicitly gained information.
- RDP (Remote Desktop Protocol) access represented **24%** of cyber incidents and was the most commonly offered or discussed.
- Over the past year, **190** reported ransomware attacks targeting the healthcare industry worldwide have been reported. Of these, **117** attacks, or **62%,** specifically targeted organizations in the US.
- SOCRadar's dark web analysts observed a significant increase of **58.3%** in global ransomware attacks against the healthcare sector compared to the previous term, with the US experiencing a **64.8%** increase in such attacks during the same period.

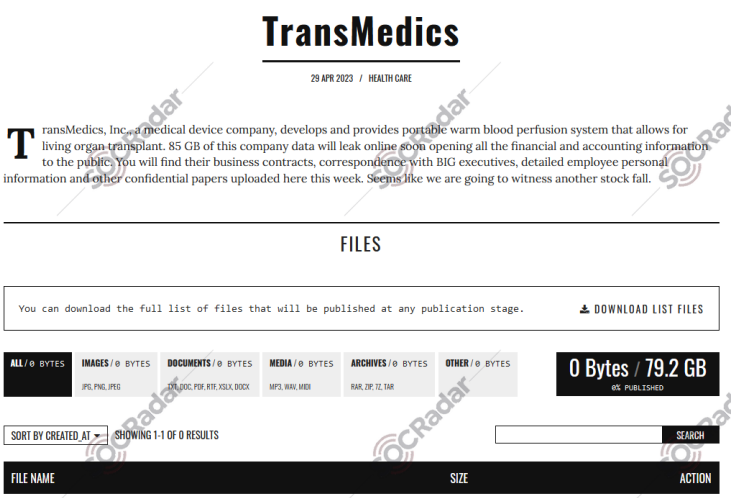
- SOCRadar's Dark Web News module has identified **117** ransomware incidents aimed explicitly at healthcare organizations in the US over the past year.
- SOCRadar's monitoring efforts uncovered approximately **537** phishing attempts directed at healthcare organizations in the US.
- Based on SOCRadar's phishing data, an alarming **61.6%** of phishing domains masquerading as websites of healthcare organizations in the past year have been utilizing the HTTPS protocol in the United States.
- CISA (the Cybersecurity and Infrastructure Security Agency) has issued several "ICS MEDICAL ADVISORIES" addressing vulnerabilities in various medical devices.

Cyber Incidents Timeline: Recent Events & Trends in the US

April 29 2023

The Data Breach Victim of Karakurt: TransMedics

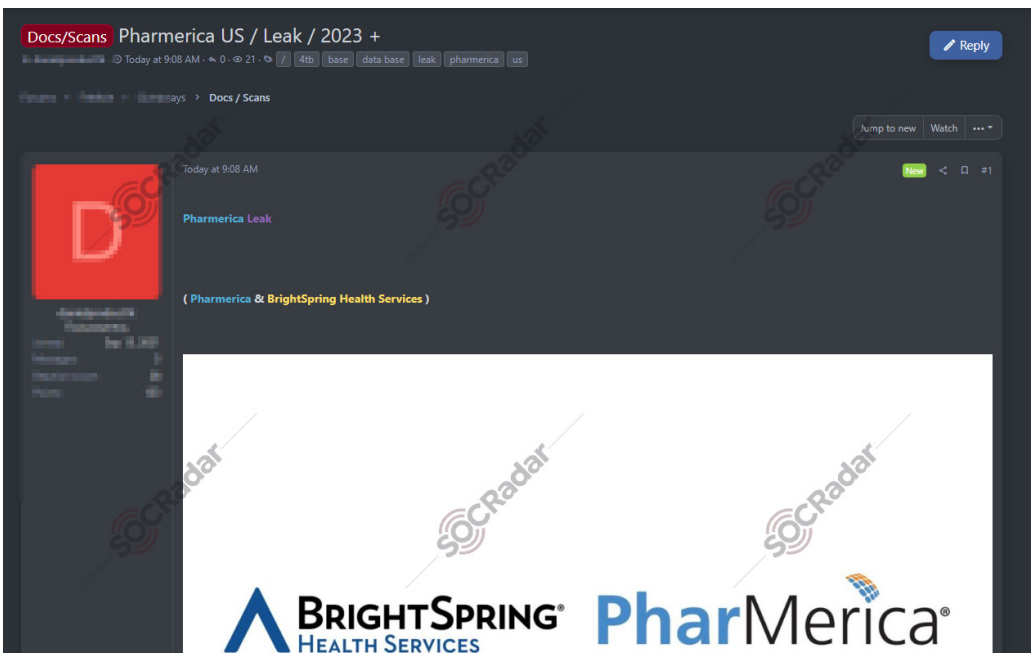
On April 23, SOCRadar researchers detected a new data breach victim allegedly announced as TransMedics, a medical device company, on the Karakurt data breach group website. On April 29, Karakurt announced they would leak sensitive information, including accounting and financial details, correspondence with other companies and business contracts, and employees' PII (Personally Identifiable Information).



April 19 2023

The customer Database of PharMerica was Leaked

In a hacker forum, SOCRadar researchers have detected a new alleged database leak for PharMerica and BrightSpring Health Services. According to the attacking group, the Money Message database contains over 2 million records and files, including at least 1.6 million personal data records such as social security numbers (SSN) and date of birth (DOB).

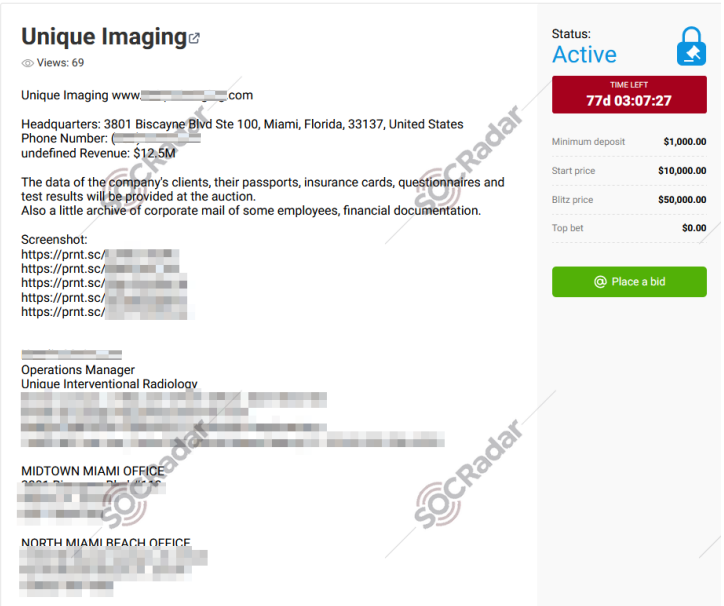


Cyber Incidents Timeline: Recent Events & Trends in the US

April 16 2023

The New Ransomware Victim of Trigona: Unique Imaging

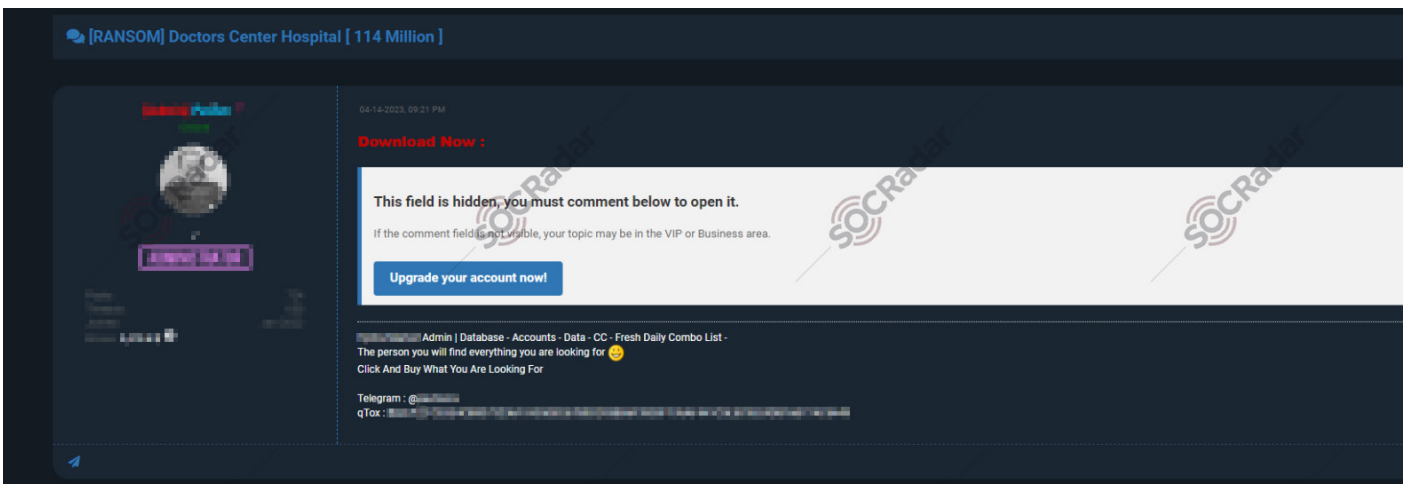
A new ransomware victim, Unique Imaging, was allegedly announced on the Trigona ransomware group website monitored by SOCRadar. The attackers claim to have obtained data belonging to the company's clients, including their passports, insurance cards, questionnaires, and test results, as well as an archive of corporate emails of some employees and financial documentation.



April 13 2023

Data of Doctors Center Hospital are Leaked

In a hacker forum monitored by SOCRadar, a new alleged data leak is detected for Doctors Center Hospital.

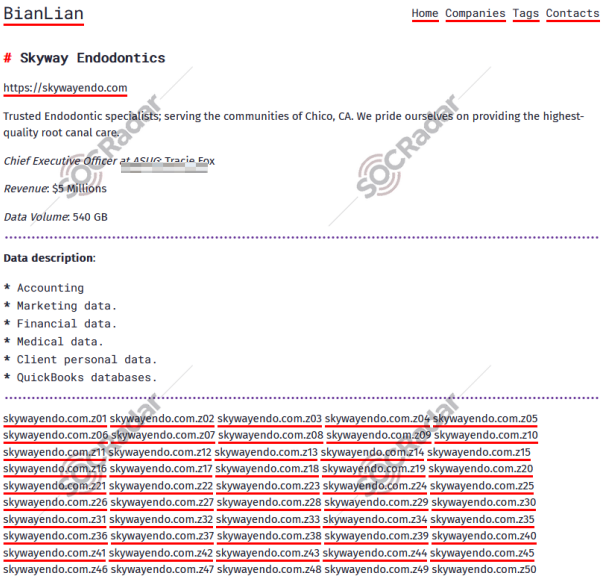


Cyber Incidents Timeline: Recent Events & Trends in the US

BianLian Ransomware Group Leaked The Data of Skyway Endodontics

March 27 2023

According to SOCRadar researchers, new data detected on the BianLian ransomware group website allegedly belonged to Skyway Endodontics. The leaked data includes information on accounting, marketing, financial, medical, and client personal data.


BianLian

Home Companies Tags Contacts

Skyway Endodontics

https://skywayendo.com

Trusted Endodontic specialists; serving the communities of Chico, CA. We pride ourselves on providing the highest-quality root canal care.

Chief Executive Officer at ASUG Tracie Fox

Revenue: $5 Millions

Data Volume: 540 GB

Data description:

* Accounting
* Marketing data.
* Financial data.
* Medical data.
* Client personal data.
* QuickBooks databases.

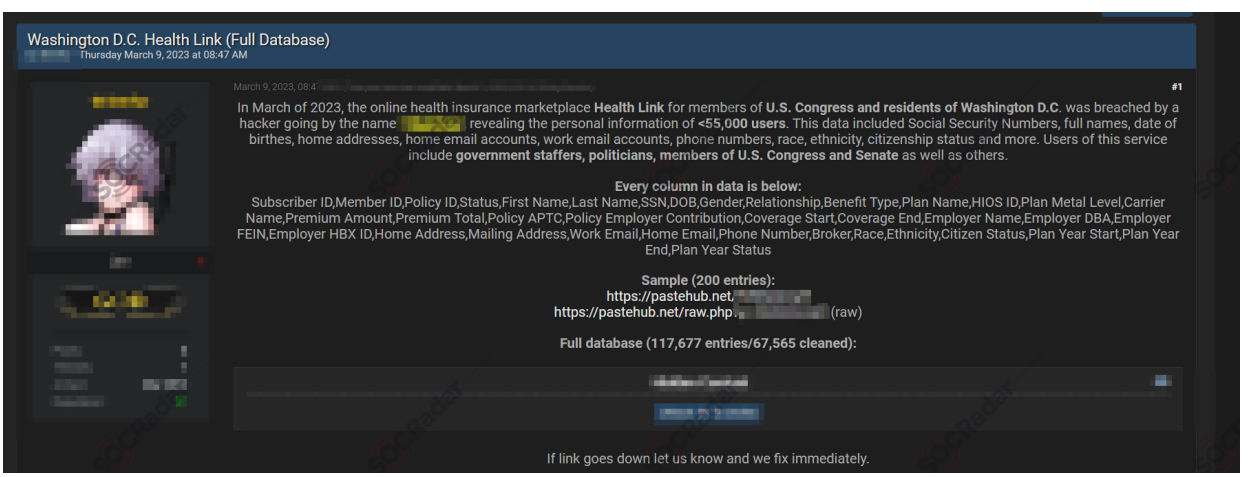
skywayendo.com.z01 skywayendo.com.z02 skywayendo.com.z03 skywayendo.com.z04 skywayendo.com.z05
skywayendo.com.z06 skywayendo.com.z07 skywayendo.com.z08 skywayendo.com.z09 skywayendo.com.z10
skywayendo.com.z11 skywayendo.com.z12 skywayendo.com.z13 skywayendo.com.z14 skywayendo.com.z15
skywayendo.com.z16 skywayendo.com.z17 skywayendo.com.z18 skywayendo.com.z19 skywayendo.com.z20
skywayendo.com.z21 skywayendo.com.z22 skywayendo.com.z23 skywayendo.com.z24 skywayendo.com.z25
skywayendo.com.z26 skywayendo.com.z27 skywayendo.com.z28 skywayendo.com.z29 skywayendo.com.z30
skywayendo.com.z31 skywayendo.com.z32 skywayendo.com.z33 skywayendo.com.z34 skywayendo.com.z35
skywayendo.com.z36 skywayendo.com.z37 skywayendo.com.z38 skywayendo.com.z39 skywayendo.com.z40
skywayendo.com.z41 skywayendo.com.z42 skywayendo.com.z43 skywayendo.com.z44 skywayendo.com.z45
skywayendo.com.z46 skywayendo.com.z47 skywayendo.com.z48 skywayendo.com.z49 skywayendo.com.z50

March 8 2023

The Database of DC Health Link Has Been Leaked

SOCRadar researchers detected an alleged database leak for DC Health Link in a hacker forum. The online health insurance marketplace, which serves members of the US Congress and residents of Washington D.C., was allegedly breached by a hacker, exposing the personal information of 55,000 users.

The leaked data includes sensitive information such as social security numbers, full names, dates of birth, home addresses, email accounts, phone numbers, race, ethnicity, citizenship status, and more. The affected users included government staffers, politicians, and US Congress and Senate members.


Washington D.C. Health Link (Full Database)

Thursday March 9, 2023 at 08:47 AM

In March of 2023, the online health insurance marketplace **Health Link** for members of **U.S. Congress and residents of Washington D.C.** was breached by a hacker going by the name revealing the personal information of **<55,000 users**. This data included Social Security Numbers, full names, date of births, home addresses, home email accounts, work email accounts, phone numbers, race, ethnicity, citizenship status and more. Users of this service include **government staffers, politicians, members of U.S. Congress and Senate** as well as others.

Every column in data is below:

Subscriber ID,Member ID,Policy ID,Status,First Name,Last Name,SSN,DOB,Gender,Relationship,Benefit Type,Plan Name,HIOS ID,Plan Metal Level,Carrier Name,Premium Amount,Premium Total,Policy APTC,Policy Employer Contribution,Coverage Start,Coverage End,Employer Name,Employer DBA,Employer FEIN,Employer HBX ID,Home Address,Mailing Address,Work Email,Home Email,Phone Number,Broker,Race,Ethnicity,Citizen Status,Plan Year Start,Plan Year End,Plan Year Status

Sample (200 entries):

https://pastehub.net/

https://pastehub.net/raw.php (raw)

Full database (117,677 entries/67,565 cleaned):

If link goes down let us know and we fix immediately.

Rising Cyber Attacks Targeting Healthcare Organizations in the US

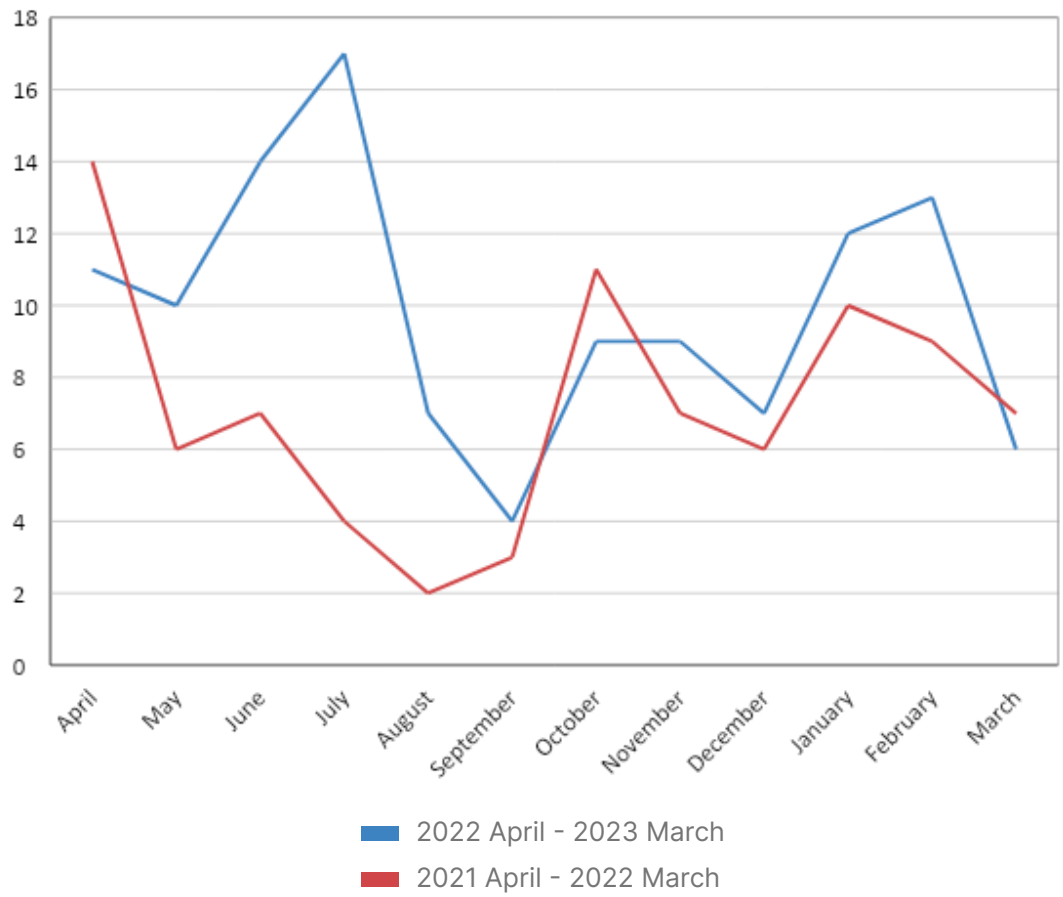
The portrayal of cybercriminals in movies and media often depicts them as hacktivists fighting for freedom or some other morally acceptable cause. However, cyber threat actors are primarily motivated by financial gain, even if it endangers people's lives. For example, attacks on hospitals have become increasingly common, with cybercriminals using ransomware to encrypt critical systems and demanding large sums of money in exchange for the decryption key. These attacks can devastate patients, as they may prevent access to critical medical equipment and records.

Therefore, healthcare organizations have increasingly paid large sums to regain access to critical patient data, resulting in a surge in the frequency and cost of healthcare security breaches.

SOCRadar has reported a 35% global rise in dark web posts regarding healthcare in the past year, with over 450 documented posts. Additionally, the IBM Cost of a Data Breach Report from 2022 shows that the healthcare sector has the highest average cost for a breach, averaging $10.1 million, representing a 10% increase from the previous year.

In the last 12 months, 119 healthcare industry-related posts were reported in SOCRadar's Dark Web News Module for the US. The number of healthcare industry-related postings shared on underground forums increased by 38% in the last 12 months compared to the previous term.

Healthcare Industry Related Dark Web Posts in The Us

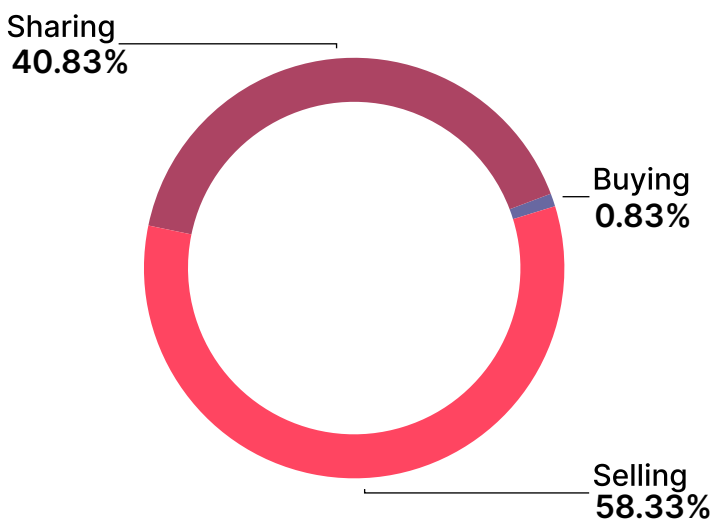


Rising Cyber Attacks Targeting Healthcare Organizations in the US

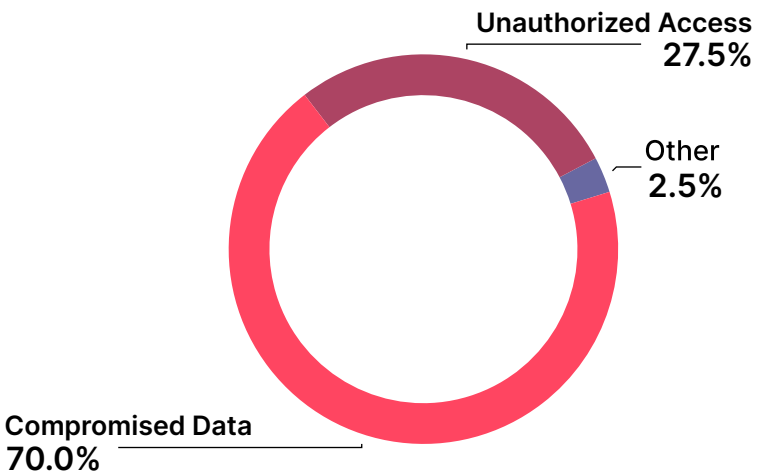
SOCRadar research team analysis also revealed that global underground posts in the healthcare industry are primarily focused in the US, Indonesia, and Russian Federation.

The dark web posts targeting the healthcare industry in US are about buying, selling, and sharing illegal access to systems and illicitly gained information.

Breakdown of Sharing, Selling, and Buying Posts

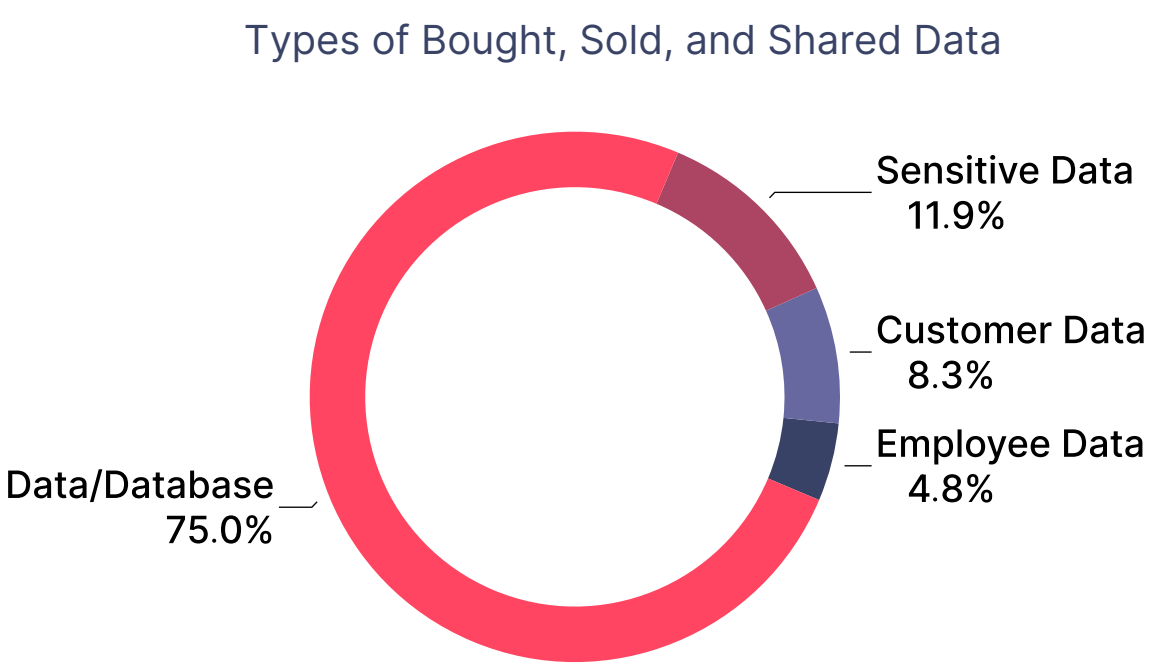


A closer look at the posts with selling, sharing, and buying topics revealed that in 70% of cases, threat actors in healthcare are interested in already compromised data. This makes sense because the PHI (Protected Health Information) data is more valuable in the dark market, and the healthcare industry is the primary target for this information. 27.5% of cases were focused on unauthorized access to the health systems.

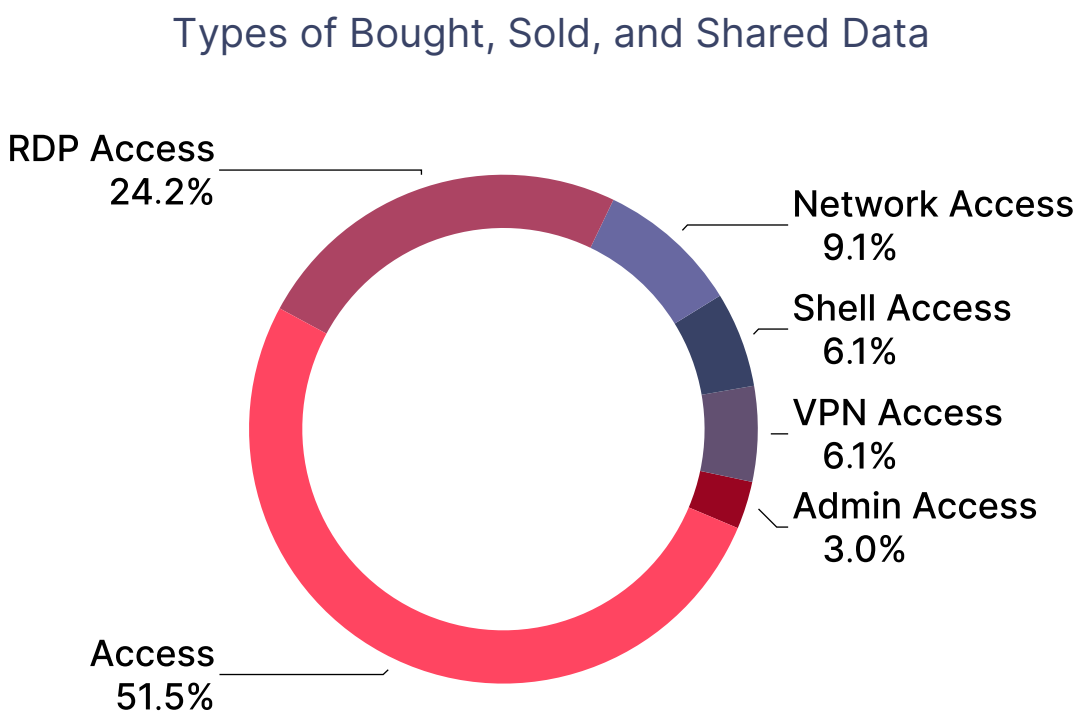


Rising Cyber Attacks Targeting Healthcare Organizations in the US

When the post contains adequate information, SOCRadar analysts use secondary tags for what was shared. Approximately 12% of bought, sold, and shared data was tagged as sensitive, and more than 8% was specific data about the customers.

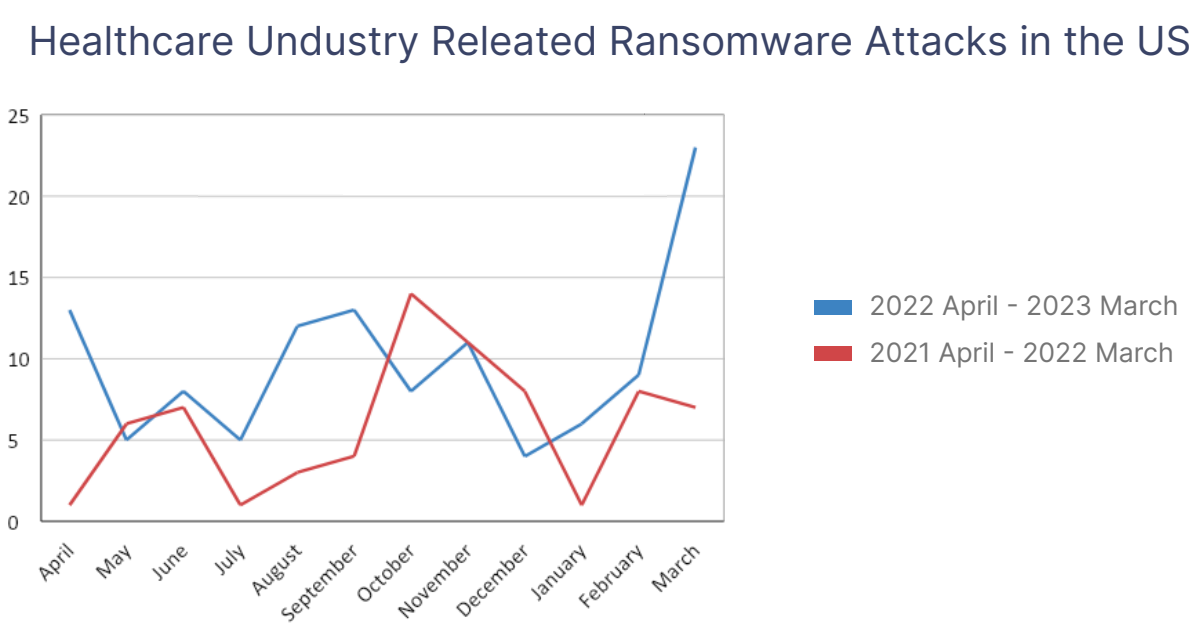


Again, when we looked at the secondary tags, RDP (Remote Desktop Protocol) access represented 24% of incidents and was the most commonly offered or discussed.

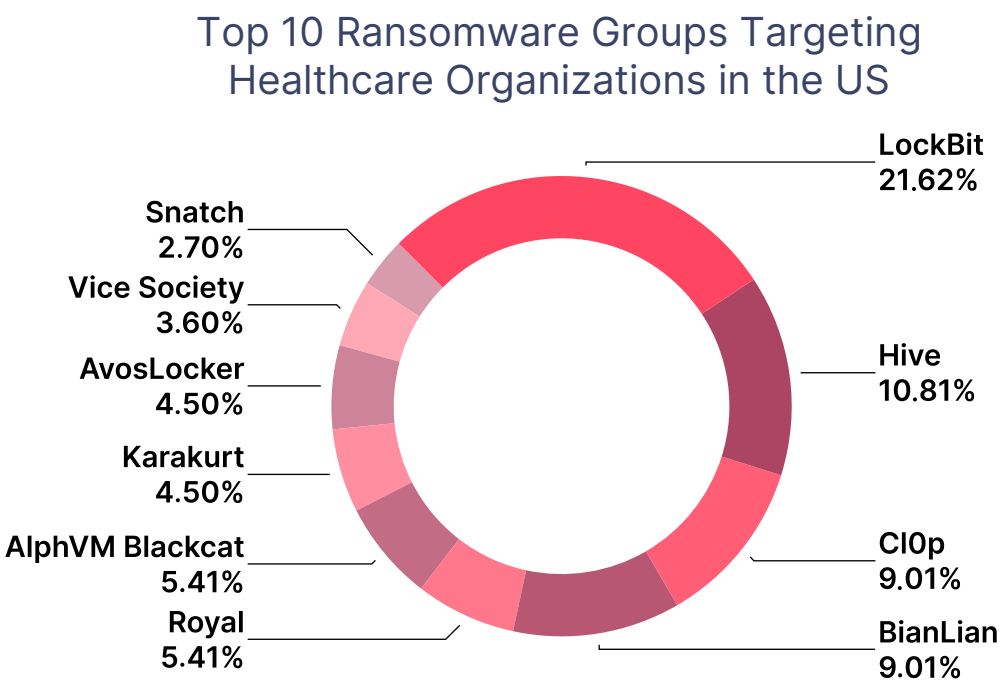


Healthcare Industry-Related Ransomware Attacks in the US

Over the past year, 190 reported ransomware attacks targeting the healthcare industry worldwide have been reported. Of these, 117 attacks, or 62%, specifically targeted organizations in the US. SOCRadar's dark web analysts observed a significant increase of 58.3% in global ransomware attacks against the healthcare sector compared to the previous term, with the US experiencing a 64.8% increase in such attacks during the same period.



SOCRadar's Dark Web News module has identified 117 ransomware incidents aimed explicitly at healthcare organizations in the US over the past year. These attacks were carried out by 25 distinct ransomware gangs, with LockBit 3.0 being the most prolific. In addition to LockBit 3.0, notable ransomware groups that have targeted the healthcare sector were HiveLeaks, Cl0p, and BianLian.

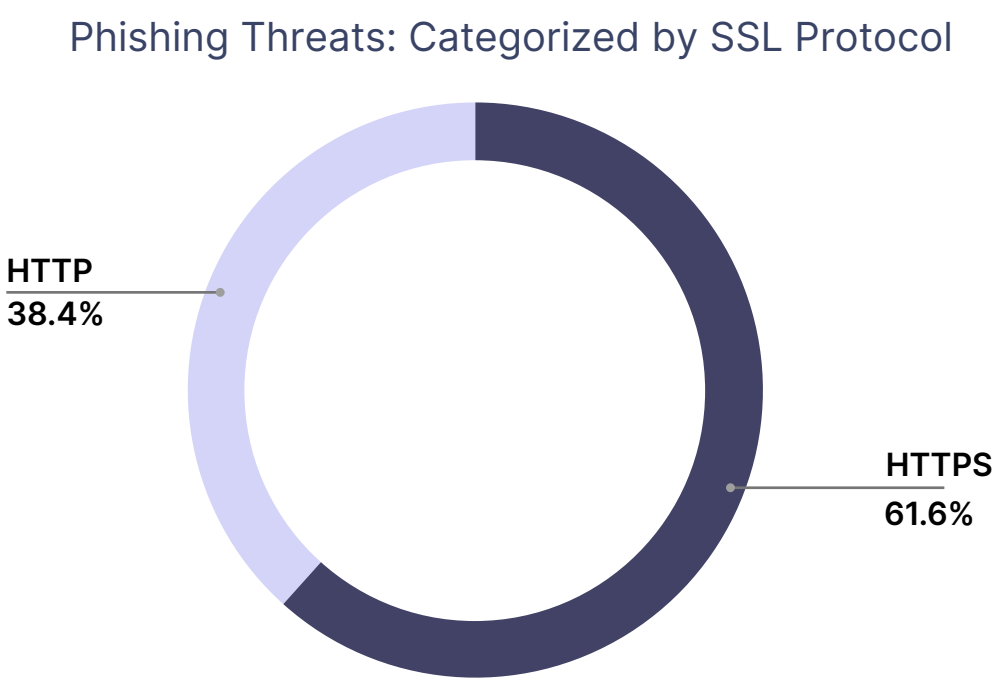


Phishing Attacks Against the Healthcare Industry in US

Phishing, a highly impactful cyber-attack method, is frequently utilized by threat actors to illicitly obtain sensitive information, such as login credentials, to enable initial access to a victim's network. Healthcare organizations are not exempt from this threat.

SOCRadar's monitoring efforts uncovered approximately 1.200 phishing attempts directed at healthcare organizations worldwide between April 2022 and March 2023. This emphasizes the significant threat posed by phishing in the healthcare sector. Of these attempts, 537 of these attemps were targeted explicitly at organizations in the US.

Based on SOCRadar's phishing data, an alarming 61.6% of phishing domains masquerading as websites of healthcare organizations in the past year have been utilizing the HTTPS protocol. This trend highlights how threat actors leverage HTTPS to deceive victims by exploiting the trust of the little padlock icon typically associated with secure connections.



Using HTTPS is particularly insidious as it is commonly associated with legitimate and secure websites. Hence attackers aim to trick individuals into clicking on malicious URLs and potentially compromising sensitive information. This emphasizes the need for individuals to exercise caution and employ additional layers of security measures to protect against such deceptive tactics.

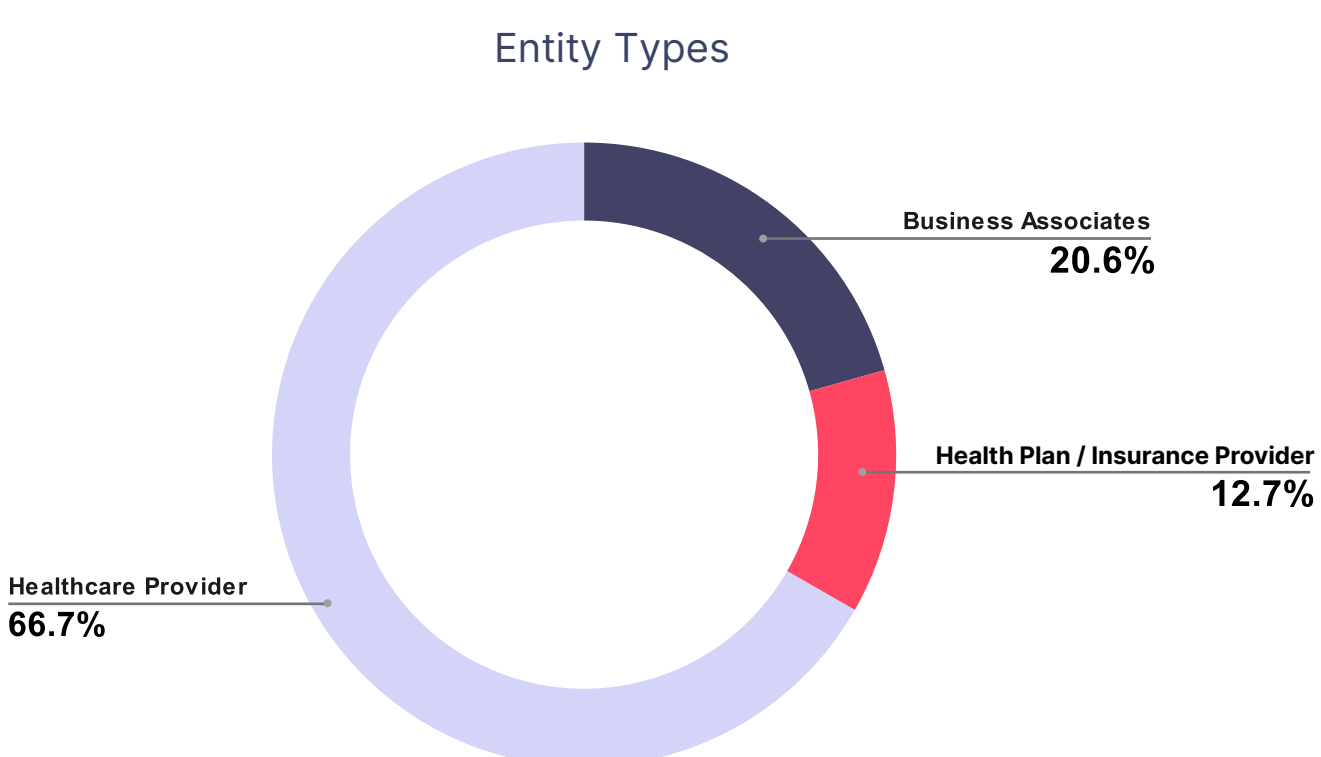
Data Breaches in the US

The Department of Health and Human Services (HHS) is a US federal executive department responsible for protecting and enhancing the health and well-being of Americans. The data managed by HHS encompasses a wide range of health-related information. This includes health statistics, research findings, public health data, healthcare quality and performance metrics, healthcare utilization, and cost data, health insurance information, Medicare and Medicaid data, and much more.

Under the HIPAA Breach Notification Rule, covered entities (such as healthcare providers, health plans, and healthcare clearinghouses) and their business associates must report breaches of unsecured PHI to HHS. A breach is the unauthorized acquisition, access, use, or disclosure of PHI that compromises its security or privacy.

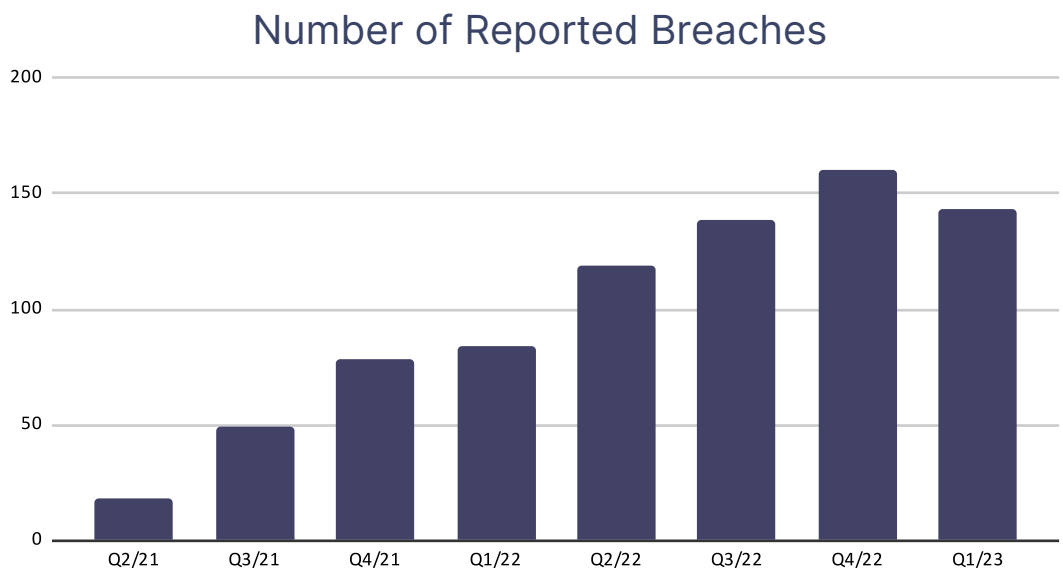
U.S. Department of Health and Human Services Office for Civil Rights is posting a list of unsecured protected health information breaches affecting 500 or more individuals according to section 13402(e)(4) of the HITECH Act. We analyzed the reported breach data from April 2021- March 2023.

There were 790 incidents in use, affecting more than 68.2 million citizens. Affected entities were in 3 groups, and the breaches hit mostly healthcare organizations.

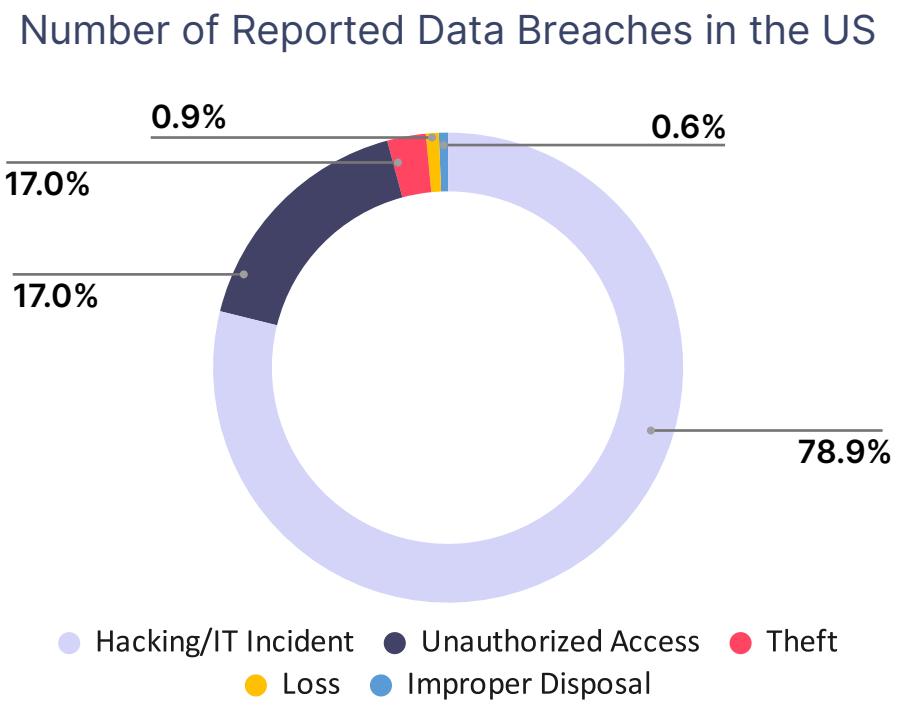


Data Breaches in the US

When we look at the change in the number of reported breaches, it shows almost a linear increase. This certainly indicates an increase in cyber attacks against the healthcare industry. Still, it also represents that the breached organizations chose to be more transparent about the attacks and involve the authorities more quickly and with increasing frequency.



We also noticed that most breaches were classified as hacking incidents (78.9%) and unauthorized access (17.0%). In another category, the location of breached information, we saw that the threat actors reached the network servers in most cases (more than 500 times out of 790). It is not hard to speculate that these threat actors were sophisticated and either stayed in the system long enough to escalate privilege or already had the privileged credentials. In either case, dark web monitoring is necessary for healthcare organizations to augment more traditional cyber defenses.

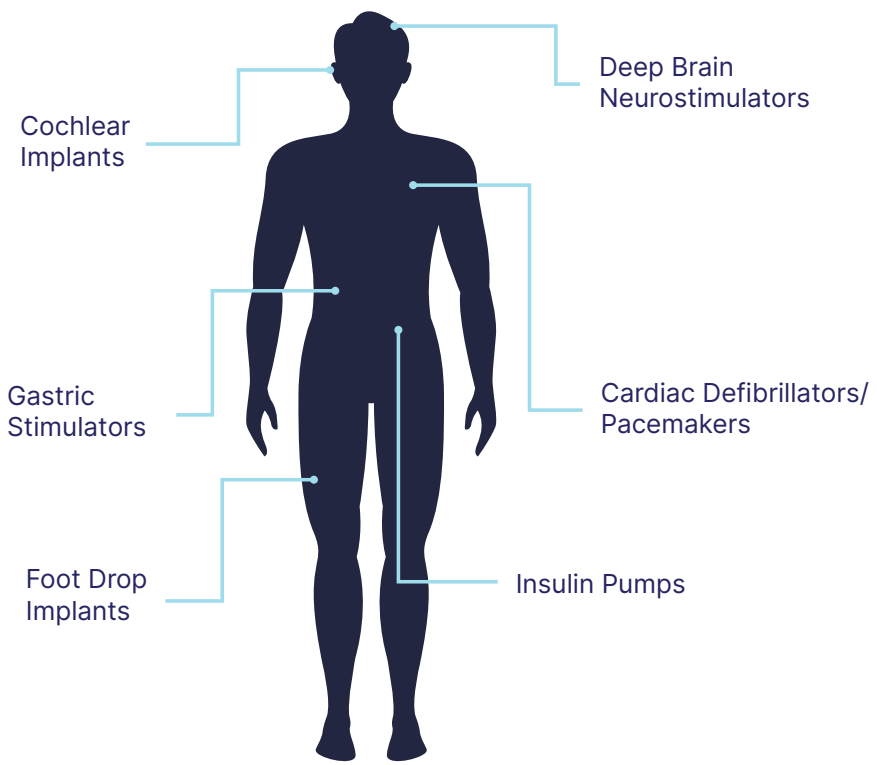


Medical IoT Devices

IoT, which stands for the Internet of Things, is a network of physical devices embedded with sensors, software, and connectivity that enables them to exchange data. These devices can range from everyday objects to industrial machinery or medical devices and are designed to communicate with each other without human intervention.

IoT aims to create a seamless network where devices can collect data from their environment, analyze that collected data, and take appropriate actions. This data can be utilized for various purposes, including monitoring systems, optimizing processes, and enhancing user experiences.

Wireless Implantable Medical Devices



While IoT offers numerous benefits, such as automation and improved efficiency, there are also concerns regarding security and privacy. As more devices become interconnected, it is crucial to implement robust security measures and safeguard sensitive data to mitigate potential vulnerabilities. This risk of compromising IoT assets is critical and potentially lethal, as medical IoT may include devices such as insulin pumps or pacemakers.

Medical IoT devices present a notable vulnerability in the healthcare industry as the adoption of digital healthcare solutions continues to rise. With the integration of various connected devices, including wearables like patient tracking wristbands and critical medical equipment such as pacemakers and ventilators, ensuring the security of these devices becomes a life-saving concern.

Medical IoT Devices

These devices interact through networks, enabling healthcare providers to access essential patient information and make informed decisions. However, similar to other digital devices, it is necessary to regularly update and secure medical IoT devices to maintain their functionality and protect against potential risks.

Issues arise when these devices remain unpatched or lack sufficient security measures, creating opportunities for cybercriminals to exploit vulnerabilities. This can lead to unauthorized access to healthcare networks, compromising patient data, and disrupting vital healthcare operations. The FBI released a white notification (20220912-001) in September of 2022, highlighting the growing concerns regarding the vulnerabilities presented by unpatched medical devices operating on outdated software and lacking sufficient security features. The notification underscored the consequences of cyber threat actors exploiting these vulnerabilities in medical devices, disrupting the operational functions of healthcare facilities, and compromising patient safety, data integrity, and confidentiality.

In addition, CISA (the Cybersecurity and Infrastructure Security Agency) has issued several "ICS MEDICAL ADVISORIES" addressing vulnerabilities in various medical devices. These advisories include:

- **B. Braun Battery Pack SP with Wi-Fi (ICSMA-23-103-01), April 13, 2023,**
- **B. Braun Infusomat Space Large Volume Pump (Update A) (ICSMA-21-294-01), October 20, 2022,**
- **Baxter Sigma Spectrum Infusion Pump (Update A) (ICSMA-22-251-01), September 29, 2022,**
- **Hillrom Medical Device Management (ICSMA-22-167-01), June 16, 2022,**

Another cyber security organization in healthcare, the US Health Sector Cybersecurity Coordination Center (HC3), also releases sector alerts to keep all the stakeholders in the healthcare industry up to date with recent cyber attack trends. A recent example cited cyber attacks launched against Veeam Backup & Replication (VBR) software in medical systems on May 10, 2023. Another one on January 31, 2023, was about Multiple Vulnerabilities in OpenEMR Electronic Health Records Systems.

5 Lessons Learned from Cyberattacks in the Healthcare Industry in the US

Lesson 1:
Small hospitals and clinics are targeted since they are considered more accessible targets for attackers. Most minor medical institutions need more human and capital resources to implement cybersecurity precautions. To fill this gap, institutions should consider external support from security companies.

Lesson 2:
Connected medical devices are one of the healthcare industry's most severe cybersecurity weak points. According to Cynerio and Ponemon Institute's 'The Insecurity of Connected Devices in Healthcare 2022' survey, 56% of respondents have encountered at least one cyberattack involving connected devices in the recent 24 months.

Connected medical devices will be more secure when listed in the digital asset inventory, and their network activity is monitored and encrypted. It is also crucial to use network segmentation to prevent these devices from accessing critical databases. Also, it is essential to follow the security updates of the devices regularly.

Lesson 3:
Pay close attention to phishing attacks, which are the first point(s) of compromise for many cyber breaches. Healthcare employees and patients are vulnerable to attacks such as phishing and social engineering, and the increased utilization of HTTPS presents an additional risk of deception. The risk factor should be reduced by training that increases the cybersecurity awareness of healthcare professionals.

Lesson 4:
Ransomware attacks are one of the most common cyberattacks in the healthcare industry. Identifying the security vulnerabilities commonly used against the healthcare industry for ransomware attacks and taking proper precautions is crucial. To save data, apply the 3-2-1 backup strategy the CISA advised. The 3-2-1 backup strategy simply states that you should have three copies of your data (your production data and two backup copies) on two different media (disk and tape) with one copy off-site for disaster recovery.

Lesson 5:
Encryption is one of the effective ways to prevent a threat actor from accessing sensitive data in healthcare systems. Encryption must be utilized during data storage and transmission to mitigate data breaches.

5 Lessons Learned from Cyberattacks in the Healthcare Industry in the US

In addition to any organization's cybersecurity threats, healthcare providers must handle industry-specific challenges. They must protect networks, databases, and endpoints from internal and external cyber threats. They are also responsible for the availability of medical services, the proper operation of medical systems and equipment, and the security and integrity of patients' and employees' private financial and medical information.

It is essential to increase security visibility to provide a solid cyber security posture. With SOCRadar's External Attack Surface Management service, you can proactively identify and monitor all digital assets 24/7 and detect security vulnerabilities.

Using Cyber Threat Intelligence solutions is also critical to identify, mitigating, and remediating security risks effectively. In particular SOCRadar's Cyber Threat Intelligence service that provide intelligence from the dark web can offer an early warning of PHI data leaks for predictive measures.

SOCRadar Digital Risk Protection (DRP) solution builds on industry-leading instant phishing domain identification, internet-wide scanning, and compromised credential detection technologies.

Who is SOCRadar®?

Your Eyes Beyond

As an Extended Threat Intelligence (XTI) platform and inventor of the concept, SOCRadar's approach effectively integrates Threat Intelligence, Digital Risk Protection, and External Attack Surface Management (EASM). Adapting proactive security with a hacker mindset, we aim to help security teams to detect blindspots before attackers.

The shortage of cybersecurity experts is a growing problem worldwide. All companies around the world must use resources efficiently to provide adequate cyber security with their limited resources. Automated security solutions offer precisely the opportunity that corporations are looking for. With its AI-powered automation technology. **With providing protection against threats for more than 6.000+ companies from 157 countries, SOCRadar has become an extension of SOC teams from every industry.**

SOCRadar provides extended cyber threat intelligence (XTI) that combines: **"Cyber Threat Intelligence, Digital Risk Protection, and External Attack Surface Management Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

8.400
Free Users

Dark Web Monitoring: SOCRadar's fusion of its unique dark web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and dark web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS 12 MONTHS FOR FREE

Gartner Peer Insights 5/5

Contact Us info@socradar.io +1 (571) 249-4598 651 N Broad St, Suite 205, Middletown, DE 19709