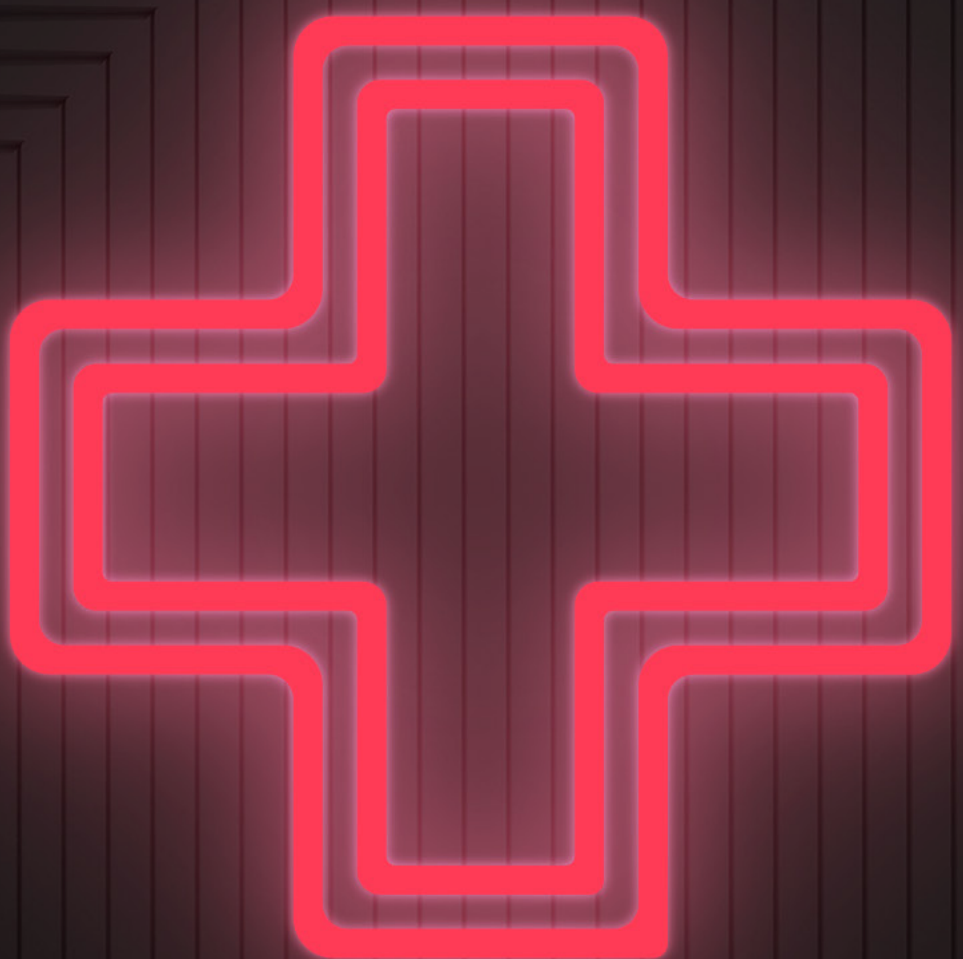
SOCRadar®
Your Eyes Beyond

HEALTHCARE THREAT LANDSCAPE REPORT

"Healthcare organizations have increasingly paid large sums to regain access to critical patient data"



socradar.io

Table of Contents

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.

Healthcare professionals are particularly vulnerable to attacks such as phishing and social engineering.

The consequences of healthcare data breaches can be severe for both patients and healthcare providers. ***"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."***

Training programs can increase cybersecurity awareness among healthcare professionals to reduce this risk factor. Ransomware attacks are one of the most common cyberattacks in the healthcare industry. Also, identifying security vulnerabilities commonly used against the healthcare industry for ransomware attacks and taking proper precautions are crucial.

SOCRadar has reported a 35% 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.

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

Healthcare data breaches and cyber attacks pose significant risks to patient privacy and financial stability for healthcare organizations. Healthcare professionals must know these risks and take necessary precautions to protect sensitive information.

SOCRadar's Healthcare Threat Landscape Report reaffirms the importance of implementing encryption measures, training programs to increase cybersecurity awareness, and backup strategies to recover data. In the last part of the report, you can also find our suggestions for a few steps as a lesson for healthcare organizations. By taking these steps, organizations can reduce the risk of data breaches and protect patients and their financial stability.

Key Findings

- Healthcare data breaches and cyber attacks are rising, with a **35%** increase in dark web posts, with over **450** posts, regarding healthcare from April 2022 to March 2023.

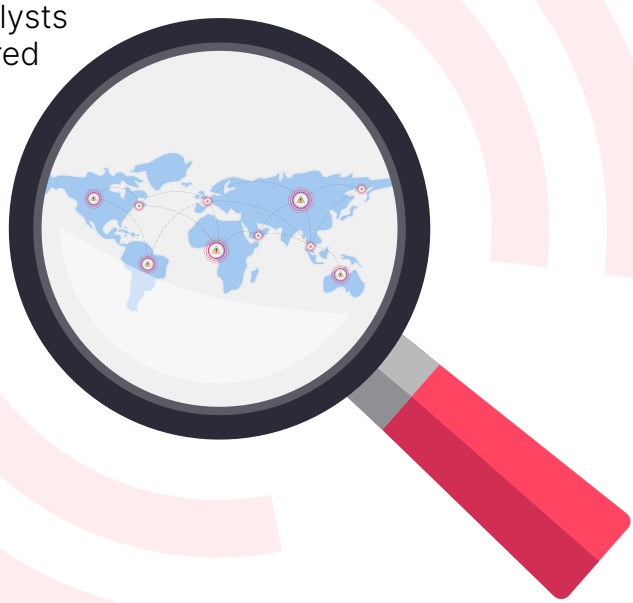
- Ransomware attacks are among the most common cyberattacks in the healthcare industry, with 190 attacks reported between April 2022 and March 2023.

- 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.

- The healthcare sector has the highest average cost for a breach, averaging **$10.1 million,** representing a **10%** increase from the previous year.

- SOCRadar research team analysis revealed that confidential posts in the healthcare industry are primarily focused in the United States, Indonesia, and Russian Federation.

- The number of ransomware attacks on the healthcare industry detected by SOCRadar dark web analysts increased by **58.3%** in the last 12 months compared to the previous term.



- SOCRadar's monitoring revealed nearly **1,200** phishing attempts targeting healthcare entities from April 2022 to March 2023.

- Based on SOCRadar's phishing data, an alarming **63.5%** of phishing domains masquerading as websites of healthcare organizations in the past year have been utilizing the HTTPS protocol.

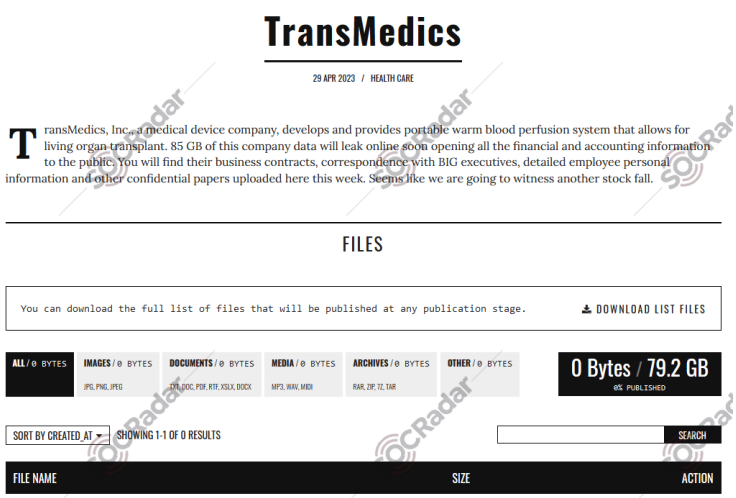
- Medical IoT devices present a notable vulnerability in the healthcare industry as the adoption of digital healthcare solutions continues to rise.

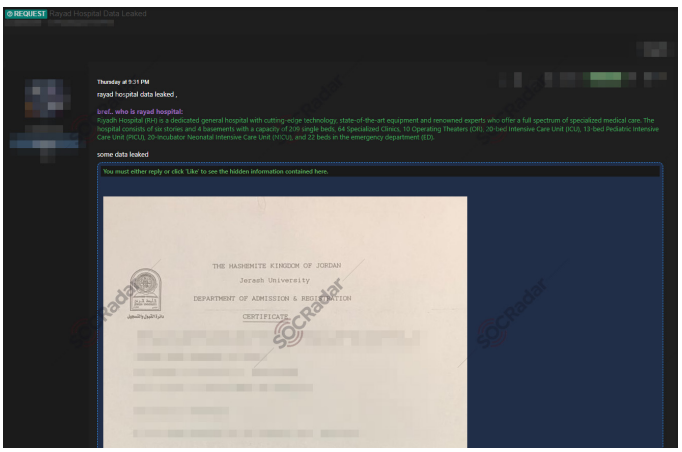
Healthcare Cyber Incidents: Recent Events and Trends

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 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 27 2023

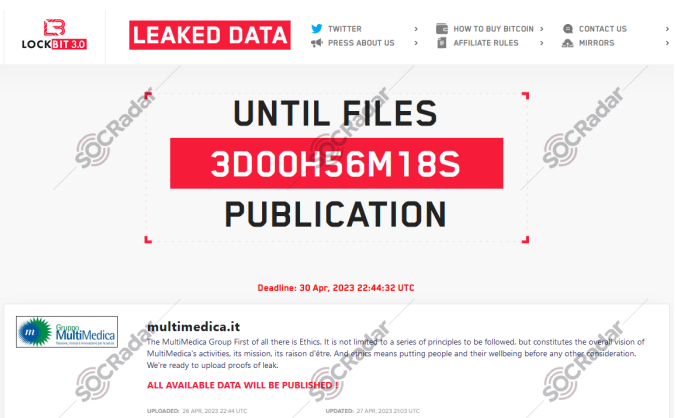
A Hacking Announcement was Detected for Riyadh Hospital

SOCRadar has detected a new announcement regarding a hacking incident at Riyadh Hospital on a hacker forum.

April 26 2023

The Ransomware Victim of LockBit 3.0: MultiMedica Group

SOCRadar analysts documented a new ransomware victim, MultiMedica Group from Italy, allegedly announced on the Lockbit 3.0 ransomware group website.



Healthcare Cyber Incidents: Recent Events and Trends

April 25
2023

The New Ransomware Victim of Akira: Family Day Care Services

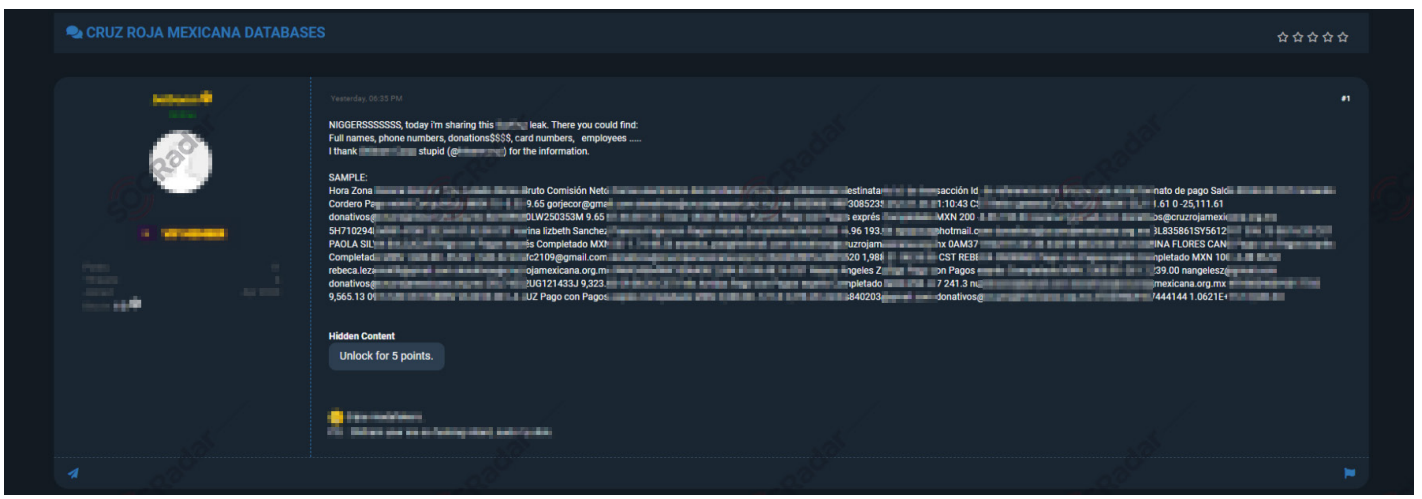
On the Akira ransomware group website monitored by SOCRadar researchers, a new ransomware victim was allegedly announced as Family Day Care Services of Toronto, Canada.

2023-04-26	Family Day Care Services	Family Day Care Services is a licensed home child in Toronto. They use evidence-based approaches in of our services to ensure we offer quality based on sound knowledge. If you see Family Day data post here, it means that not all services company provides are of great quality. Personal of their customers was not protected almost at and will be published on our blog soon. Their data turned out to be very interested as well. wait for the release.

April 23
2023

The database of Cruz Roja Mexicana (Mexican Red Cross) was Leaked

In a hacker forum monitored by SOCRadar researchers a new alleged database leak was detected for Cruz Roja Mexicana (Mexican Red Cross). The database reportedly included full names, phone numbers, donation amounts, card numbers, and employee names.

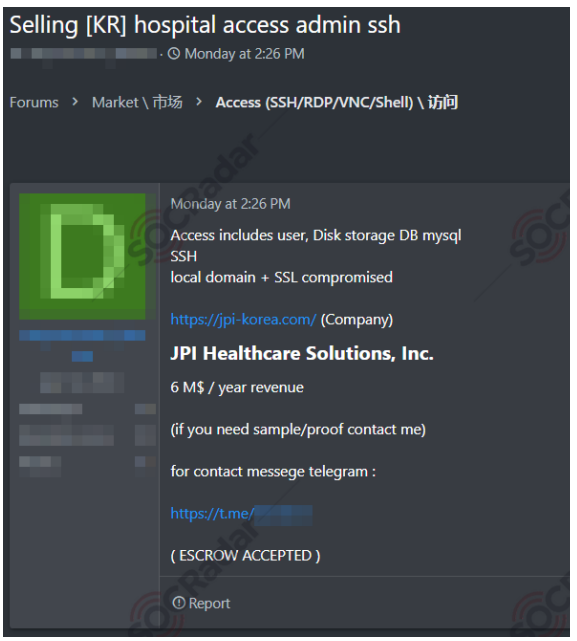


Healthcare Cyber Incidents: Recent Events and Trends

April 23 2023

An unauthorized Admin Access Sale was Detected for JPI Healthcare Solutions

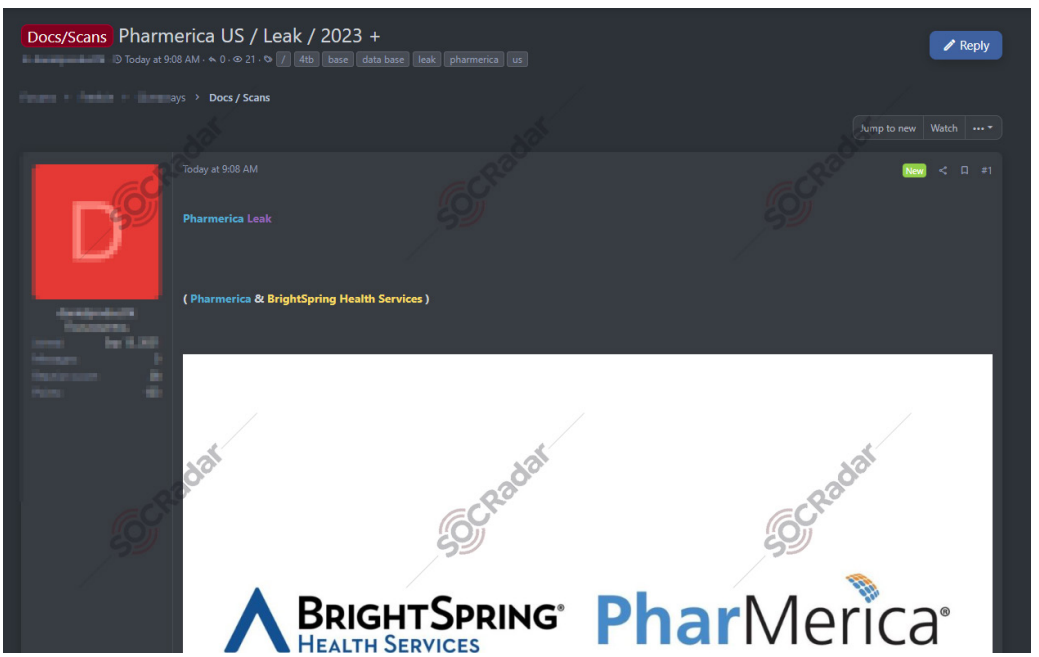
In a monitored hacker forum, SOCRadar detected the alleged sale of unauthorized admin access to JPI Healthcare Solutions. The access being sold allegedly includes user, disk storage, MySQL database, SSH to the local domain, and SSL.



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, MoneyMessage, the 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).



Healthcare Cyber Incidents: Recent Events and Trends

April 17
2023

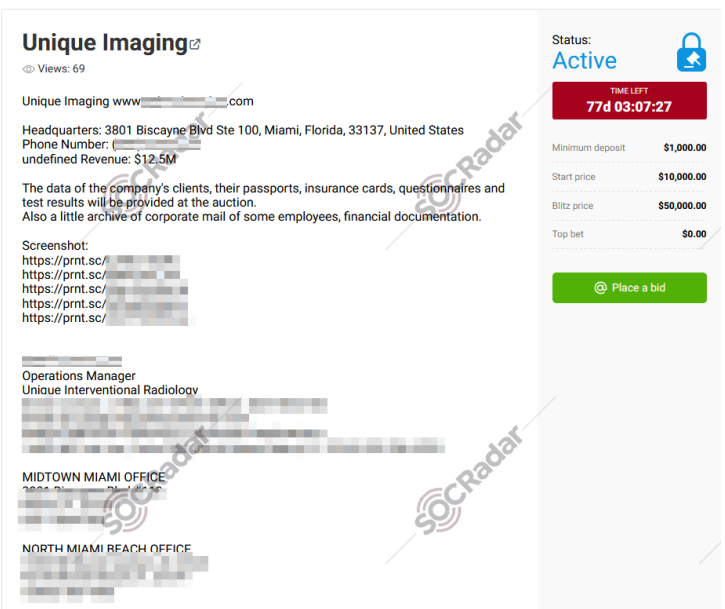
Unauthorized Admin Access Sale was Detected for Spanish Unicorn Pharmaceutical Industry

An unauthorized admin access sale allegedly belonging to a Spanish Unicorn company in the Pharmaceutical Industry is detected in a hacker forum monitored by SOCRadar researchers.

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.

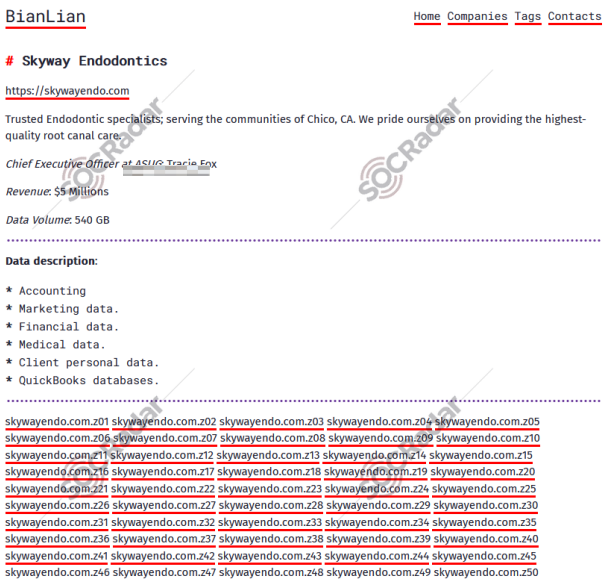


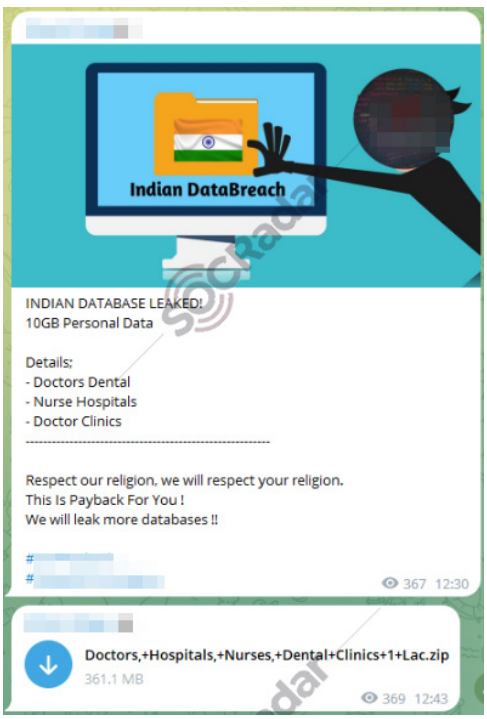
Healthcare Cyber Incidents: Recent Events and Trends

BianLian Ransomware Group LeakedThe 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.





A Database of Indian Healthcare Workers was Leaked

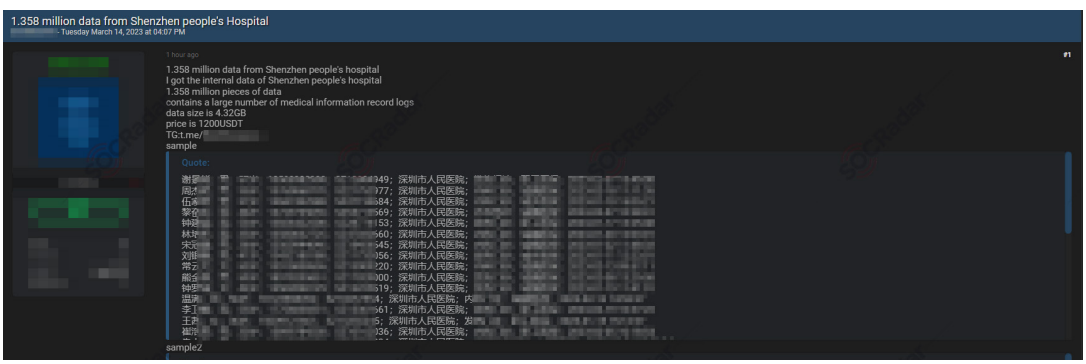
March 26 2023

SOCRadar researchers monitoring a hacker Telegram channel discovered an alleged data leak involving 10 GB of personal information belonging to healthcare workers in India.

Data of Shenzhen People's Hospital were on Sale

March 13 2023

SOCRadar researchers detected a new alleged data sale in a hacker forum for Shenzhen People's Hospital. The deal reportedly includes 1.358 million data containing many medical information record logs.

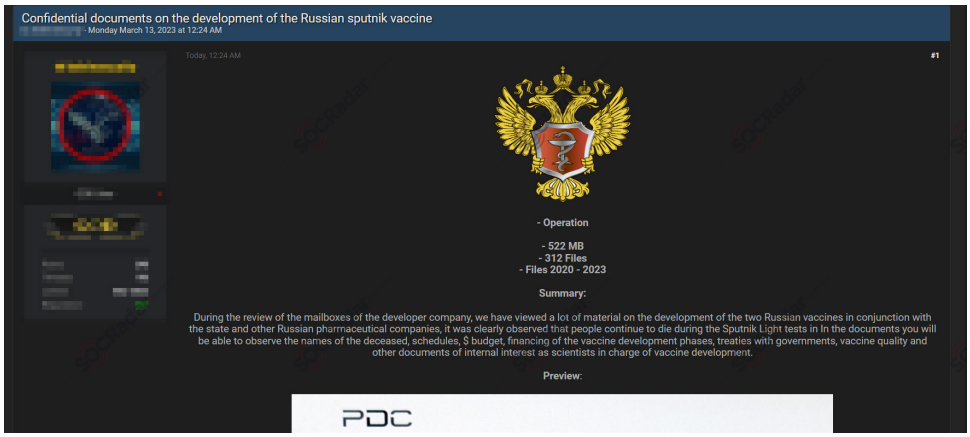


Healthcare Cyber Incidents: Recent Events and Trends

March 12 2023

Sensitive Documents of Sputnik V COVID-19 Vaccine were Leaked

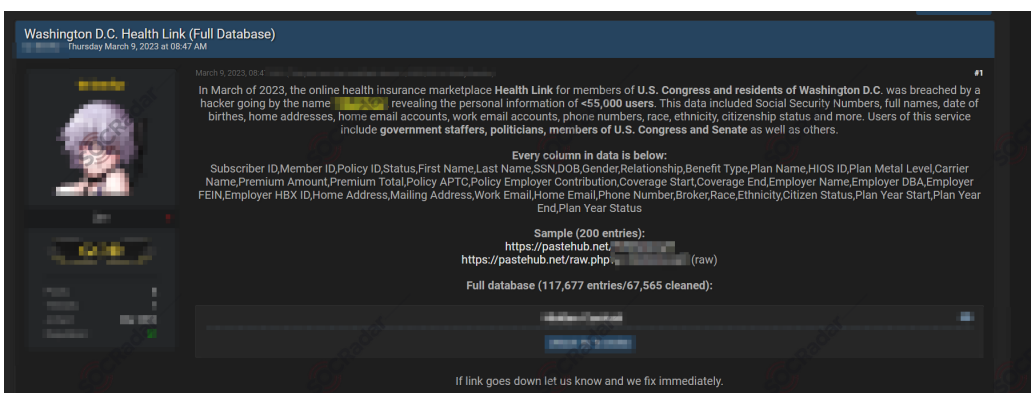
In a hacker forum, SOCRadar researchers detected an alleged leak of sensitive documents for the Sputnik V COVID-19 vaccine. The leaked documents, amounting to 522 MB across 312 files, included schedules, budgets, financing information for vaccine development phases, government treaties, vaccine quality information, and other internal documents related to the vaccine's development. The files were dated from 2020 to 2023.



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.



Healthcare Cyber Incidents: Recent Events and Trends

The Medibank Ransomware Incident

The Medibank ransomware incident involved a cyber attack on one of Australia's largest private health insurance companies, Medibank, by a ransomware group known to have ties to the now defunct REvil gang. The attackers gained access to approximately 9.7 million customer details, including sensitive information such as names, addresses, birthdates, and sometimes Medicare numbers. This information was stolen to extort a ransom payment from Medibank in exchange for not publicly releasing the data.

Medibank responded quickly to the incident and implemented measures to prevent further data breaches. They also investigated the incident and worked closely with law enforcement agencies to track down those responsible.

The Advocate Aurora Health Breach

Advocate Aurora Health, a significant healthcare provider in the Midwest with 26 hospitals, exposed the data of 3 million patients in July 2022 due to the improper use of Meta Pixel, a website tracking tool. The tool was used on patient portals, leading to the disclosure of PHI, especially if patients were logged into Facebook or Google simultaneously. A third-party vendor caused this incident and affects patients in Wisconsin and Illinois. The use of Meta Pixel by many healthcare providers across the country has raised concerns about patient privacy and led to class action lawsuits against the vendor and healthcare providers.

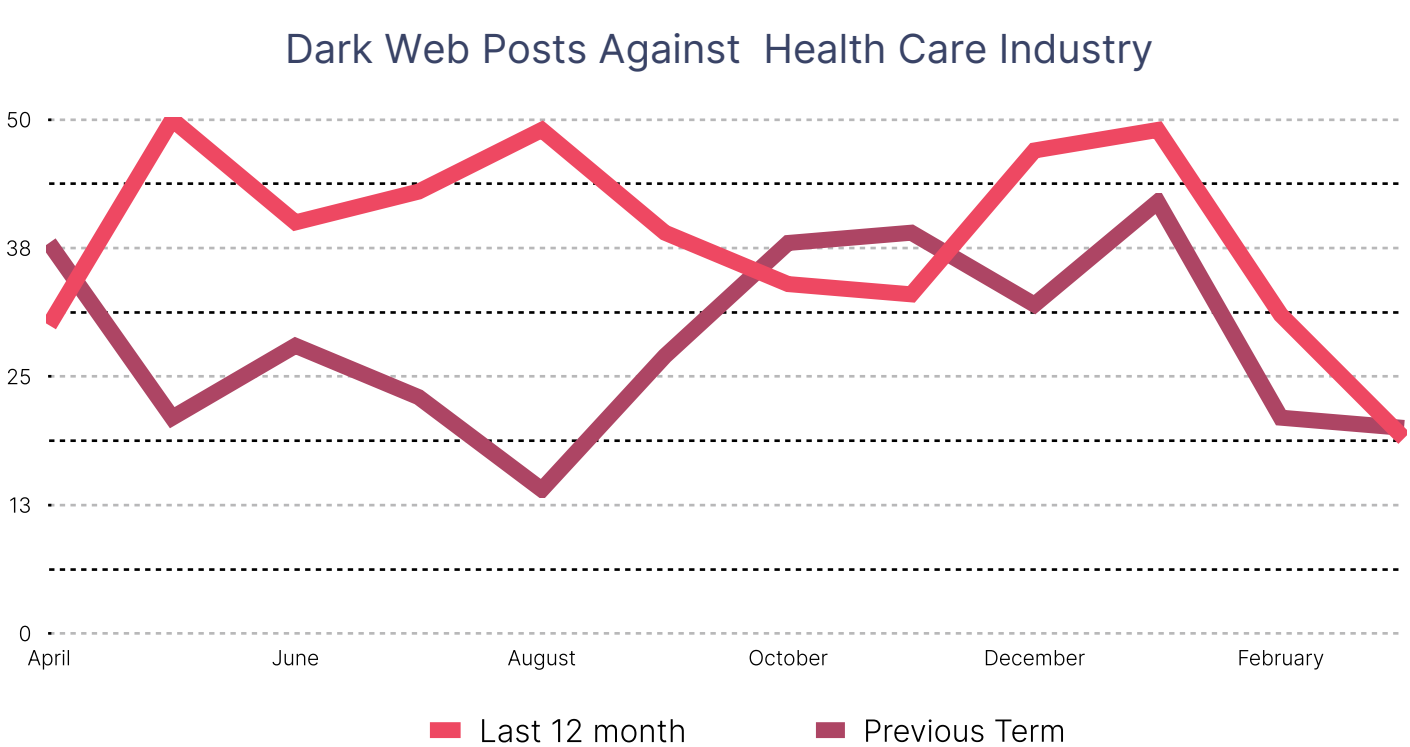
Healthcare Industry Remains a Primary Target for Cyber Attacks

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 means literally endangering 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.

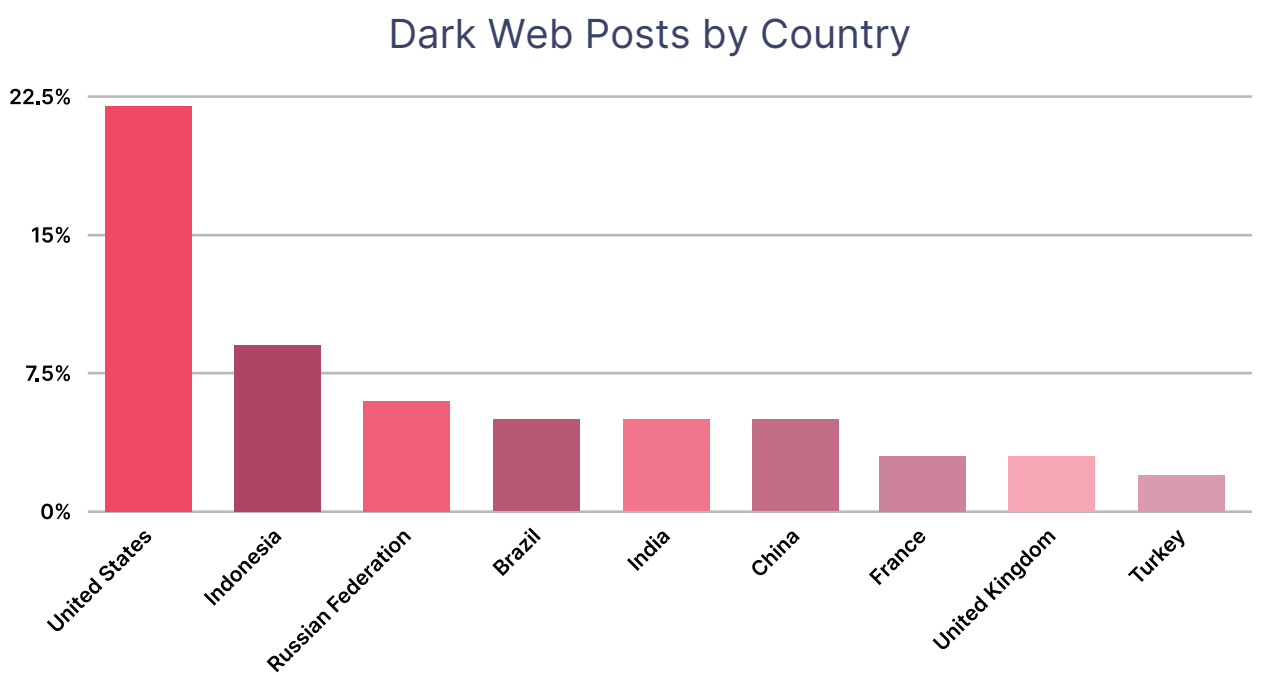
SOCRadar has reported a 35% rise in dark web posts regarding healthcare in the past year, with over 450 documented posts. Additionally, the IBM Cost of a Data Breach Report from 2022 shows that the healthcare sector has the highest average cost for a breach, averaging $10.1 million, representing a 10%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

In the last 12 months, 464 healthcare industry-related posts were reported in SOCRadar's Dark Web News Module. The number of healthcare industry-related postings shared on underground forums increased by 35% in the last 12 months compared to the previous term.

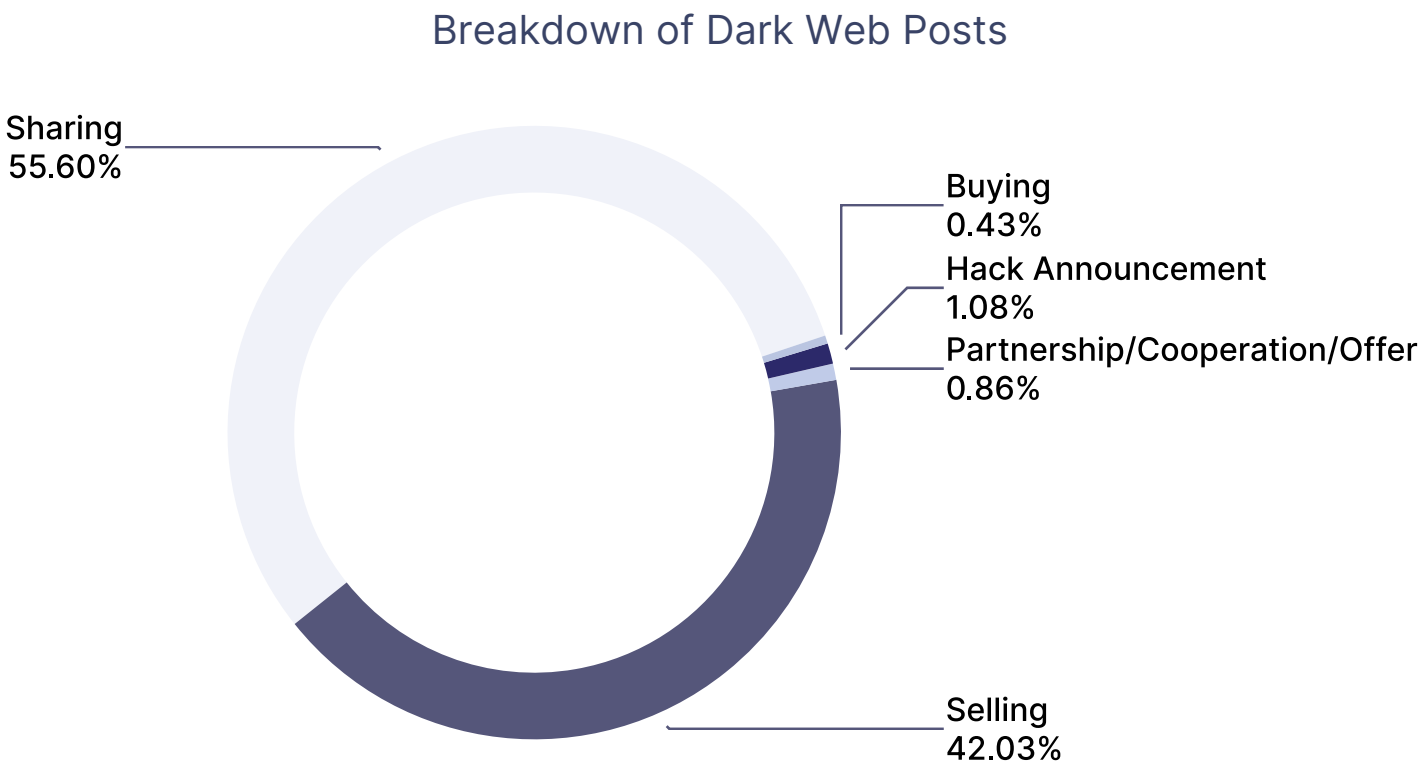


Healthcare Industry Remains a Primary Target for Cyber Attacks

SOCRadar research team analysis also revealed that dark web posts in the healthcare industry are primarily focused in the United States, Indonesia, and Russian Federation.



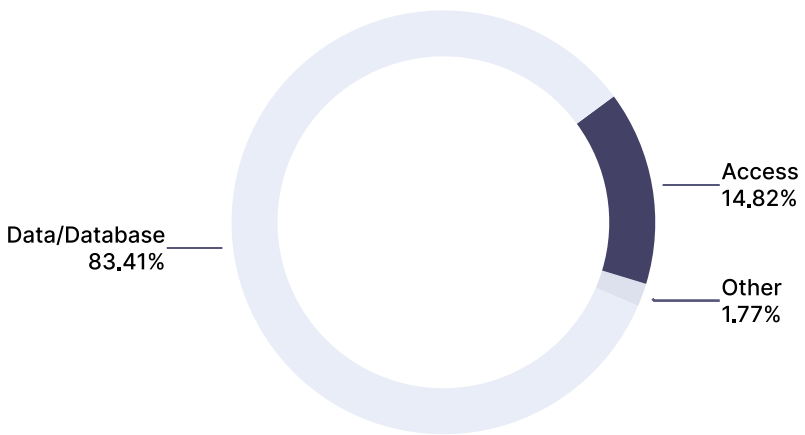
More than 97% of the topics in these dark web posts related to the healthcare industry revolved around selling and sharing information and discussing methods to compromise healthcare systems.



Healthcare Industry Remains a Primary Target for Cyber Attacks

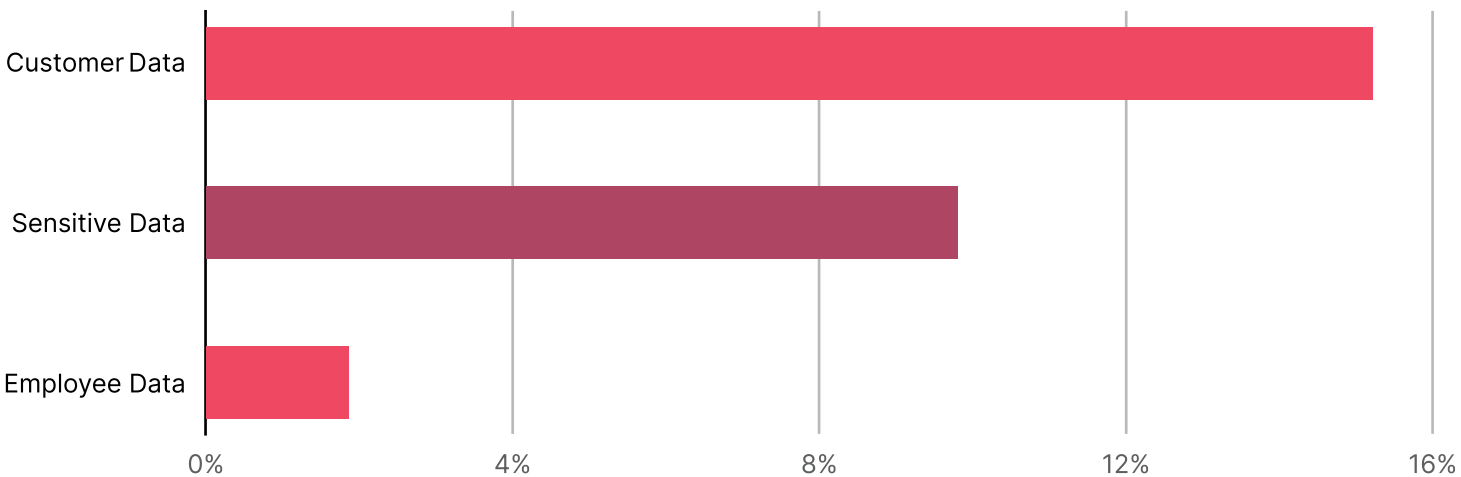
A closer look at the dark web post with selling, sharing, and buying topics revealed that threat actors in healthcare are interested in already compromised data, with more than 83.4%. This situation makes sense because the PHI (Protected Health Information) data is more valuable in the dark market and healthcare industry where you get it. Then around 15% were about unauthorized access to the health systems.

Breakdown of Sharing, Selling, and Buying Posts



When the post has enough information, SOCRadar analysts use secondary tags for what was shared. About 15% of bought, sold, and shared data was about the customers.

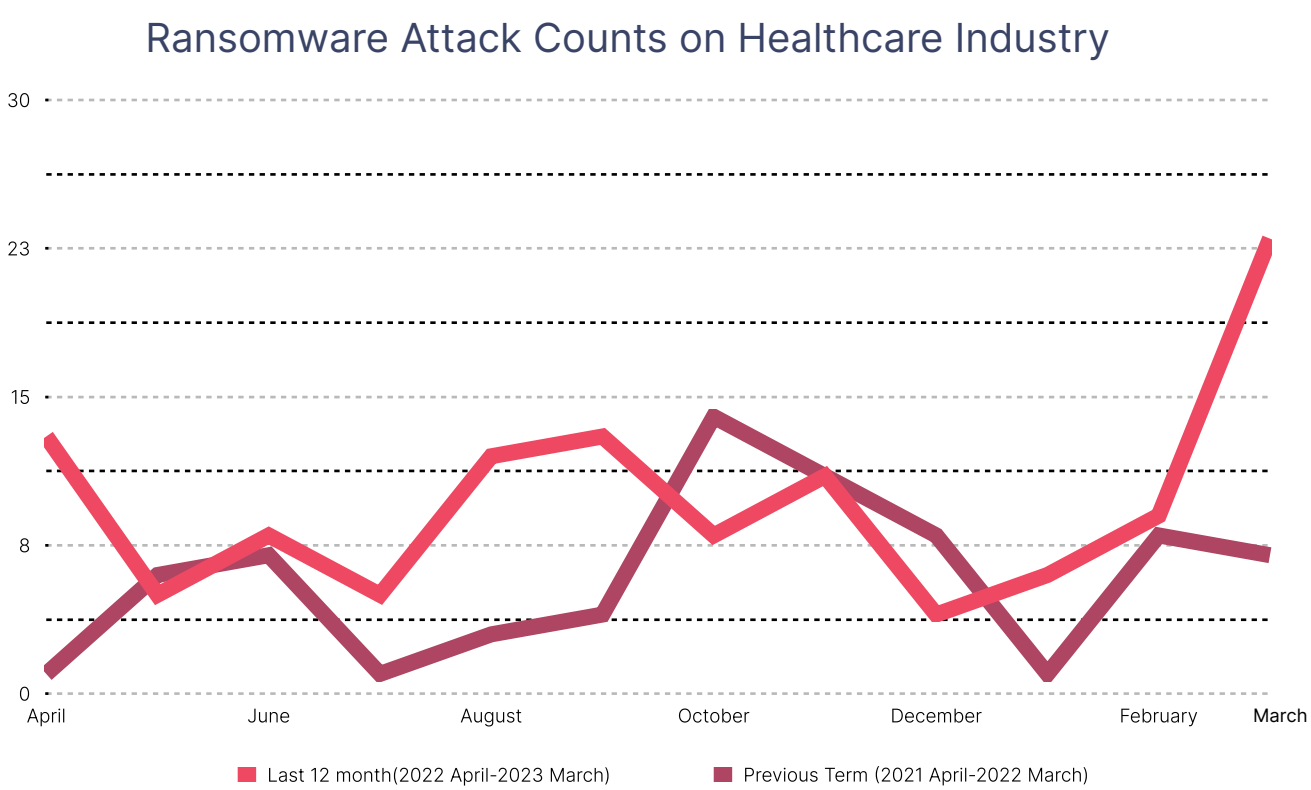
Breakdown of Access Sale Posts



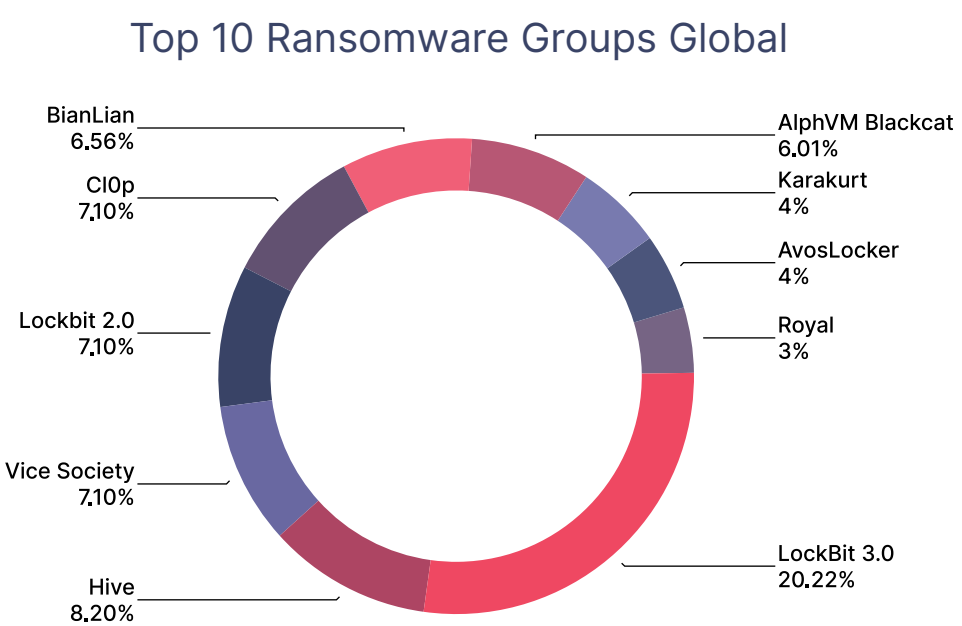
Again, when we looked at the secondary tags, RDP (Remote Desktop Protocol) access was found to be the most commonly offered or discussed.

Ransomware Attacks

In the last 12 months, 190 ransomware attacks against the healthcare industry have been reported. The number of ransomware attacks on the healthcare industry detected by SOCRadar dark web analysts increased by 58.3% in the last 12 months compared to the previous term.



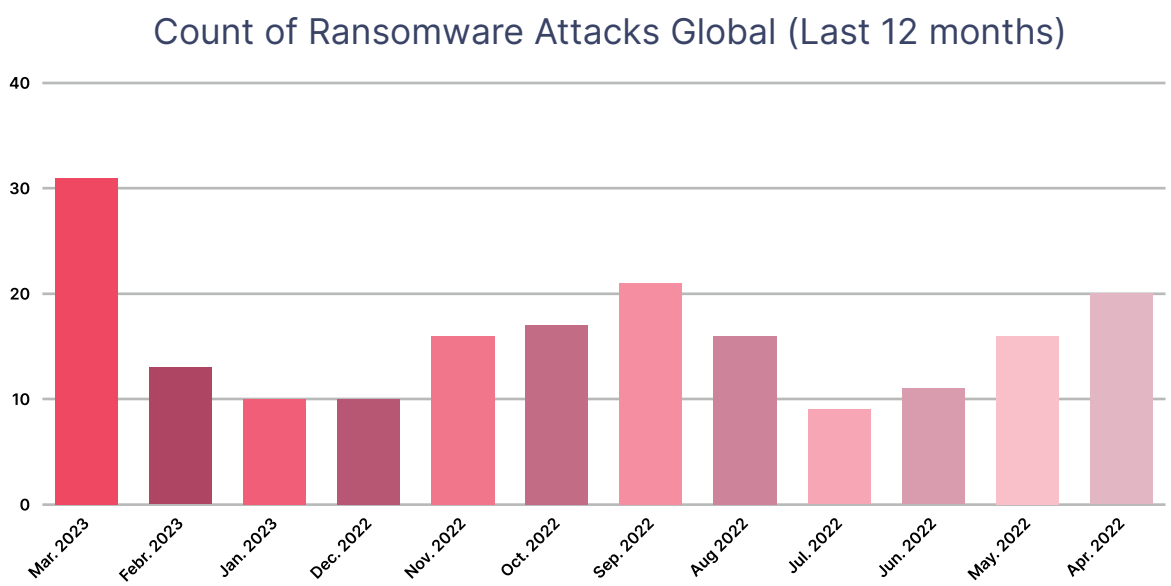
Within the last 12 months, SOCRadar's DarkMirror module has detected **190 ransomware incidents** targeting healthcare organizations. **33 unique ransomware gangs** perpetrated these attacks, and LockBit (3.0) was the most active one. The top ransomware groups that have targeted the healthcare system are **LockBit 3.0, HiveLeaks, and Vice Society.**



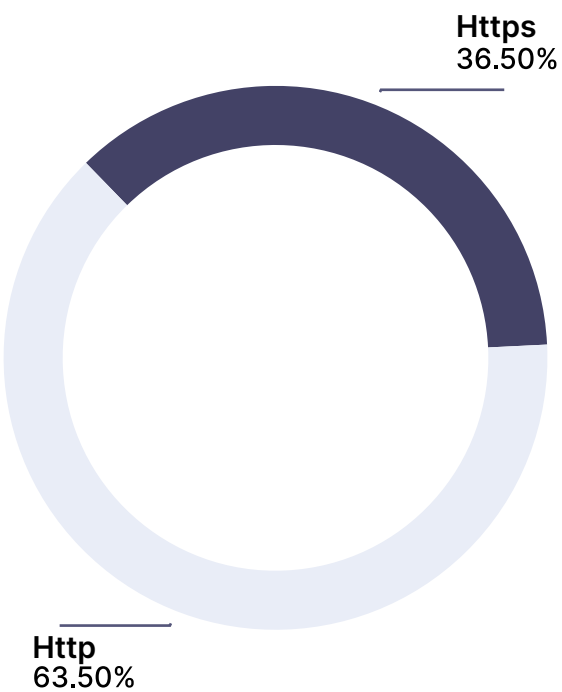
Phishing Attacks Against the Healthcare Industry

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

SOCRadar's monitoring revealed **nearly 1.200 phishing attempts** targeting healthcare entities from April 2022 to March 2023, highlighting the substantial risk of phishing in the healthcare sector. Interestingly, there appears to be a surge in phishing attempts during the summer months, possibly linked to the vacation period in the education system.



Based on SOCRadar's phishing data, an **alarming 63.5% 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.

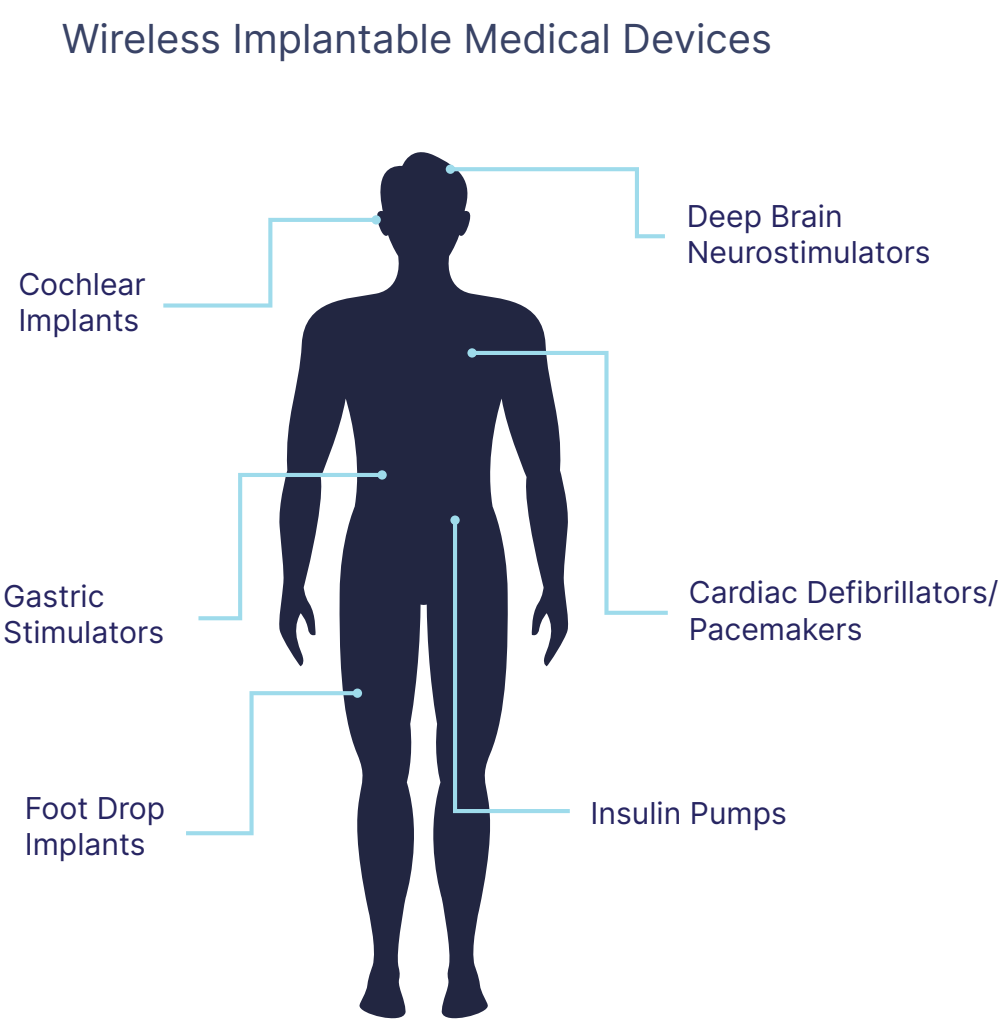


By employing HTTPS, commonly associated with legitimate and secure websites, attackers aim to trick individuals into clicking on malicious URLs, potentially compromising sensitive information. This emphasizes the need for individuals to exercise caution and employ additional layers of security measures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

Medical IoT Devices Carry the Biggest Security Risks

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 it, and take appropriate actions. This data can be utilized for various purposes, including monitoring systems, optimizing processes, and enhancing user experiences.



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 is especially critical, rather lethal, for medical IoT devices such as insulin pumps or pacemakers.

Medical IoT Devices Carry the Biggest Security Risks

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 like pacemakers and ventilators, ensuring the security of these devices becomes crucial.

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.

The issue arises 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.

FBI released a white notification (20220912-001) highlighting the growing concerns regarding the vulnerabilities presented by unpatched medical devices operating on outdated software and lacking sufficient security features on September 12, 2022.

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 one was about 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

Lesson 1:
Small hospitals and clinics are targeted since they are considered more accessible targets for attackers. Most minor medical institutions need more human resources and resources to implement the latest 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 security 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 attacks. People are vulnerable to attacks such as phishing and social engineering. 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 Cybersecurity and Infrastructure Security Agency (CISA) advised

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.

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 companies 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

Darknet and Deep 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 web, deep web, and darknet 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 resiliency 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