

Increased Cyber Attacks on the Global Healthcare Sector

Data from CloudSEK DRM reveals that the number of cyberattacks against the healthcare industry has increased by 95.34% in the first 4 months of 2022 as compared to the number of cyberattacks in 2021 during the same period. A total of 34.14% of this increase can be attributed to the USA alone.

Authors: Aastha Mittal and Hansika Saxena

Co-Author: Isha Tripathi

CloudSEK TRIAD

(Threat Research & Information Analytics)

Table of Contents

| | |
|--|-----------|
| Synopsis of Cyber Threats to the Global Healthcare Industry | 2 |
| Advancements in the Healthcare Industry | 3 |
| RPM (Remote Patient Monitoring) | 3 |
| EHR (Electronic Health Records) | 3 |
| IoT (Internet of Things) | 4 |
| Cyber Attacks on Healthcare Institutions in 2021 | 5 |
| Most Targeted Regions | 6 |
| USA Emerges as a Prime Target for Threat Actors* | 8 |
| Major Threat Actors | 8 |
| Kristina | 9 |
| Master data | 10 |
| LockBIT 2.0 | 10 |
| Commonly Sought After Data Types | 11 |
| Database | 12 |
| Access | 12 |
| Increase in Dark Web Activity Related to the Healthcare Industry | 13 |
| Why Healthcare Industry is a Desirable Target for Cybercriminals? | 21 |
| Common Attack Vectors | 22 |
| Phishing & BEC (Business Email Compromise) | 22 |
| Ransomware | 22 |
| DDoS (Distributed Denial of Service) Attacks | 22 |
| Insider Threats | 23 |
| Critical Infrastructure & Medjacking | 23 |
| Vulnerabilities & Exploits | 23 |
| Mitigation Measures | 24 |
| Impact of Cyberattacks on the Healthcare Industry | 25 |
| Create a Cyber Resilient Healthcare Ecosystem | 26 |
| Resources | 27 |
| About CloudSEK | 28 |

Synopsis of Cyber Threats to the Global Healthcare Industry

Healthcare accounts for over 10% of the GDP of most developed countries. The global healthcare industry was valued at USD 359.2 billion in 2021 and is expected to reach USD 665.37 billion by 2028, according to Verified Market Research. According to the Centers for Medicare and Medicaid Services, the US national healthcare expenditure alone has surpassed USD 4.1 trillion in 2020 and is expected to reach USD 6.2 trillion by 2028.




XVigil data shows that ~4% of threats identified in 2021 targeted healthcare institutions. This can be attributed to the advancements in technology and infrastructure of the healthcare

industry along with the mass digitization of systems brought about by the growing market and catalyzed by the COVID-19 pandemic.

In this report, we delve into:

- Advancements in the healthcare sector
- Major cyber attacks on prominent entities in the healthcare sector
- Breakdown of the attacks by region and types.
- Why healthcare is a major target for cybercriminals
- Common attack vectors
- Long-term impact of the attacks
- Preventive measures

Top 5 Targeted Countries

| | |
|--|------|
|  USA | 28% |
|  India | 7.7% |
|  France | 7.0% |
|  China | 5.6% |
|  Italy | 4.2% |

Most Targeted Data Types

-  Vaccination Records
-  PII of Healthcare Workers
-  PII of Patients
-  Administrative Login Credentials
-  Financial Records

Common Attack Vectors

-  Phishing & BEC
-  DDoS
-  Ransomware
-  Insider Threats
-  Critical Infrastructure
-  Vulnerabilities/Exploits

Advances in the Healthcare Industry

Healthcare Information Technology (IT) is a branch of IT that helps in developing, designing, creating, and maintaining information systems in hospitals, clinics, and other healthcare facilities. In 2021, the global healthcare IT market was valued at USD 135.6 billion, with a predicted CAGR (Compound annual growth rate) of 29.3% during the forecast period of 2020 to 2030, according to Allied Market Research. The exponential growth of the global healthcare IT market brought about due to the outbreak of the 2020 global pandemic has led to a significant rise in cyberattacks targeting the sector globally. Safeguarding the medical and financial information of patients emerged as a new challenge for healthcare companies.

The following advancements caused by the healthcare IT have provided cybercriminals with more opportunities to the attack this sector:



RPM
(Remote Patient Monitoring)

Remote Patient Monitoring is the monitoring and capture of a patient's medical and health data outside of the conventional clinical settings such as home and remote areas. It allows smooth transmission of health data between patients and their doctors. Experts have shown their concerns regarding the security risks associated with the usage of this technology. Dr. Tuvia Ben Gal, a leading expert on the subject, has pointed out that manufacturers of such devices frequently overlook cybersecurity guidelines, and healthcare providers are often uneducated about security threats and inexperienced with methods for assessing those risks.



EHR
(Electronic Health Records)

Electronic Health Records are digital representations of a patient's medical history that have been collected over time. These hold a lot of private information regarding a patient's identification, medical condition, and medical history. Although EHRs make it simple to store and distribute a patient's information in a digital format, their sensitive patient-care-centered content makes them a prime target for phishing, spyware, ransomware, and other vulnerabilities.

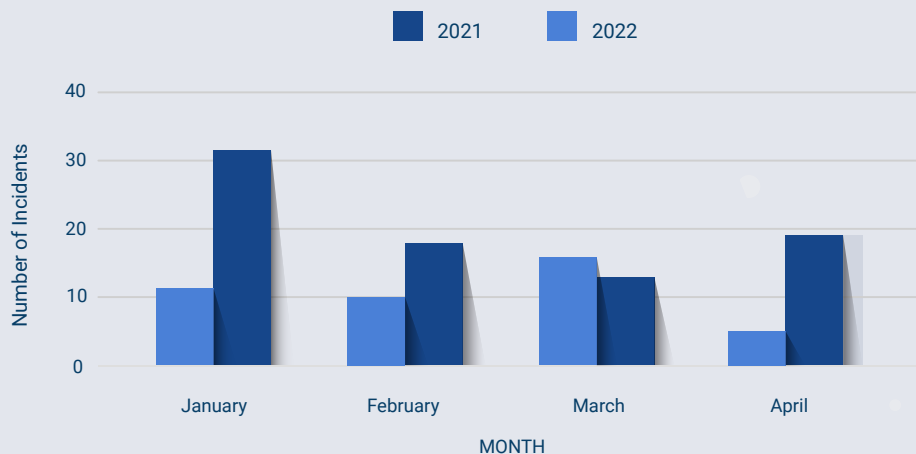


IoT
(Internet of
Things)

The Internet of Things (IoT) is a network of physical objects with sensors, software, processing ability, and other technologies which connect and share data with other devices and systems on the communication network or the internet. This sudden digitalization of the healthcare industry has left a lot of sensitive information and systems vulnerable to various cyberattacks. With the increasing attacks on the healthcare industry, 75% of the healthcare facilities such as hospitals and clinics were found unprepared in case of a cyberattack.



Cyber Attacks on Healthcare Institutions in 2021



Monthly distribution of cyber attacks on healthcare institutions in first four months of 2021 & 2022

Monthly distribution of cyber attacks on healthcare institutions in 2021



In 2021, cyber attacks on Healthcare institutions peaked in

October

Least number of cyber attack incidents in 2021 were in

August



Most Targeted Regions

Data gathered by XVigil shows that the following three regions were primary targets of cyberattacks targeting the healthcare sector:

North America

USA showed the highest number of attacks, accounting for 28% of all the attacks on the healthcare industry in 2021.

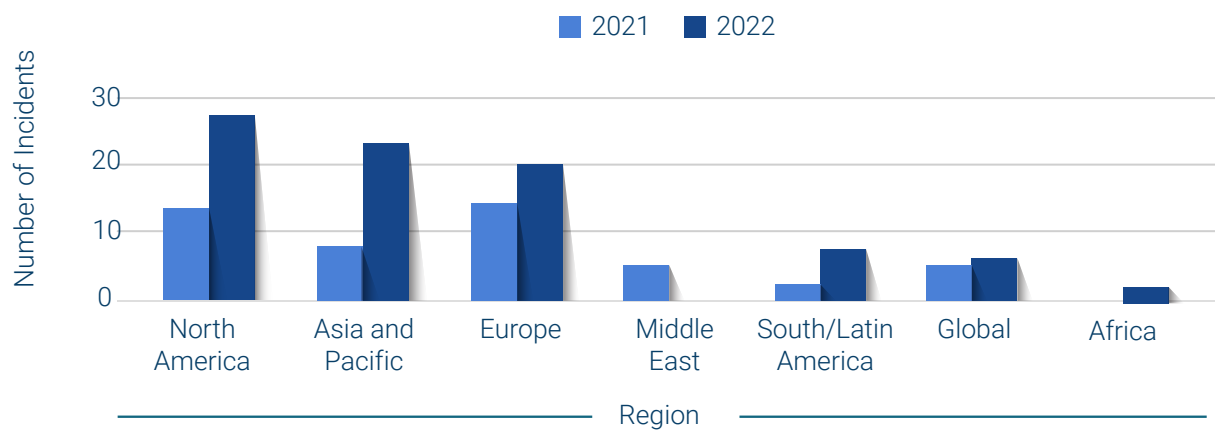
Asia & Pacific

India recorded the second highest number of attacks, with a total of 7.7% of the total attacks on the healthcare industry in 2021. (29.7% of all attacks in Asia & Pacific region). China was the second most targeted country in the Asia & Pacific region with 21.6% recorded attacks in 2021 (5% of worldwide total).

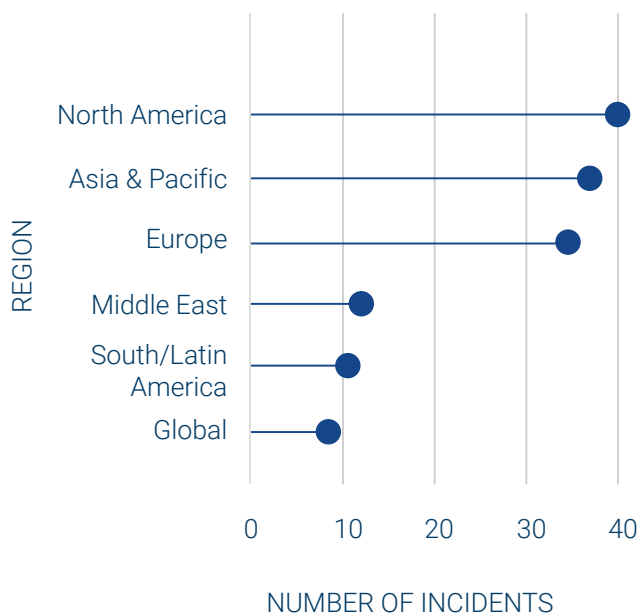
Europe

France ranked third in the world for the number of attacks on the healthcare industry, accounting for 7.0% of all attacks in 2021 (28.8% of all attacks in Europe). Italy was the second most targeted country in the Europe region with 17.1% of recorded attacks in 2021 (4.2% of total worldwide).





Region wise number of recorded cyberattacks targeting the healthcare sector in first four months of 2021 and 2022



Region wise number of recorded cyberattacks targeting the healthcare sector in 2021

32.1%

of total attacks recorded worldwide in 2022 occurred in the USA.

7.1%

India, China, and Italy tied for the second place, with each having 7.1% of total attacks.

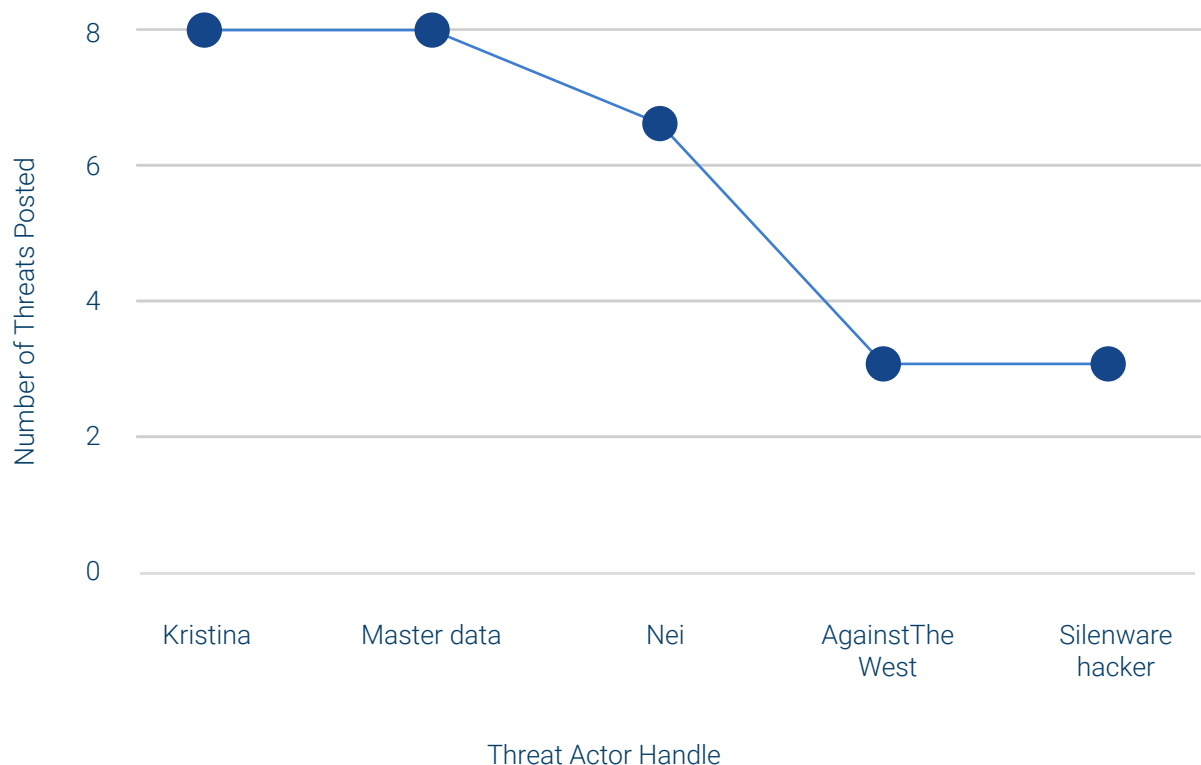




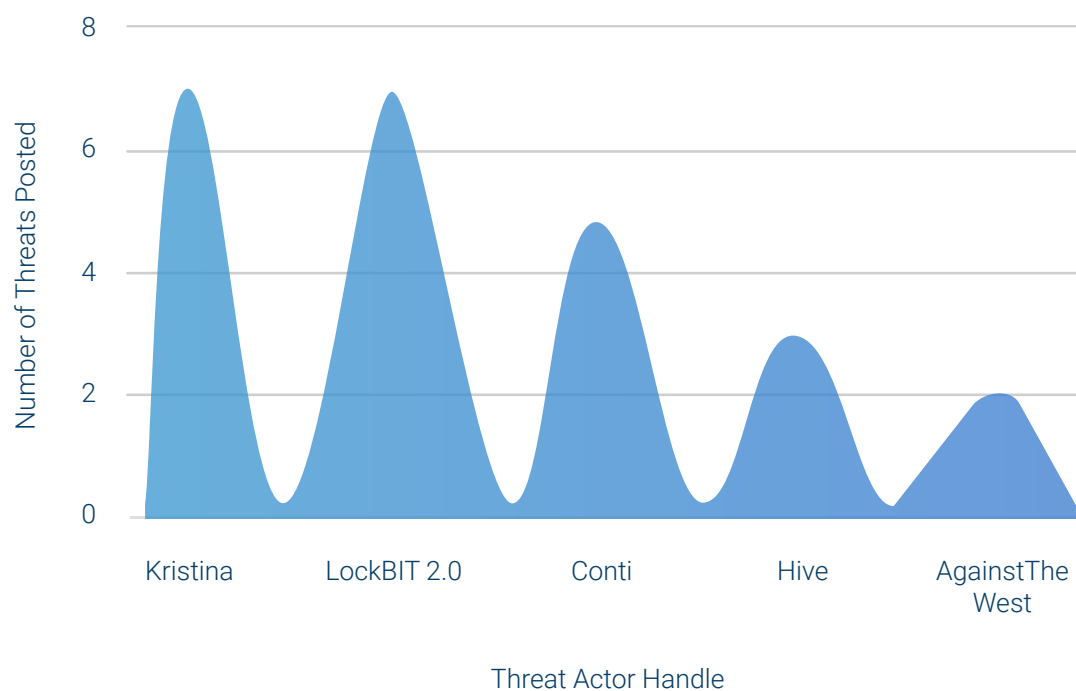
USA Emerges as a prime Target for Threat Actors

In the year 2021, North America dominated healthcare IT by recording a total revenue share of 47.1% and is expected to grow at the fastest rate in the coming years. The North American healthcare industry is starting to rapidly rely on IT services to improve patient care and reduce medical costs. The presence of various renowned medical care facilities in this region is another reason for the prominent market growth in the area. Given the healthcare industry's growth, expenditure, and digitalization in the USA, it is easy to see why it is the most targeted country when it comes to cyberattacks on the healthcare industry.

Major Threat Actors



Top 5 threat actors targeting the Healthcare sector in 2021



Top 5 Threat actors targeting the Healthcare sector in 2022

Kristina

- Kristina is a handle used by a threat group that was previously known as Kelvin Security team.
- The group uses targeted fuzzing and exploits common vulnerabilities to target victims. Being highly skilled in the use of tools and having a wide knowledge of various exploits, they share their list of tools and payloads for free.
- They typically target victims with common underlying technologies or infrastructure at any given time.
- The group doesn't shy away from attention and publicly shares information such as new exploits, targets, and databases on cybercrime forums and communication channels such as Telegram.
- Recently, they started their data leak websites where other threat actors can share databases.

Master data

- Master data is a threat actor who actively operated on a now-dead English speaking cybercrime forum. They actively post data that targets various sectors and regions.
- Since most of their advertisements contained samples as proof to substantiate his claims, it was concluded that the actor did possess the data.
- On multiple occasions, the threat actor was found accessing and downloading databases from open databases, databases present in open web directories, or exploiting vulnerabilities on third-party vendors associated with an organization.
- The actor has been consistent in selling data and has been primarily data that contains PII such as phone numbers, email addresses, and passwords

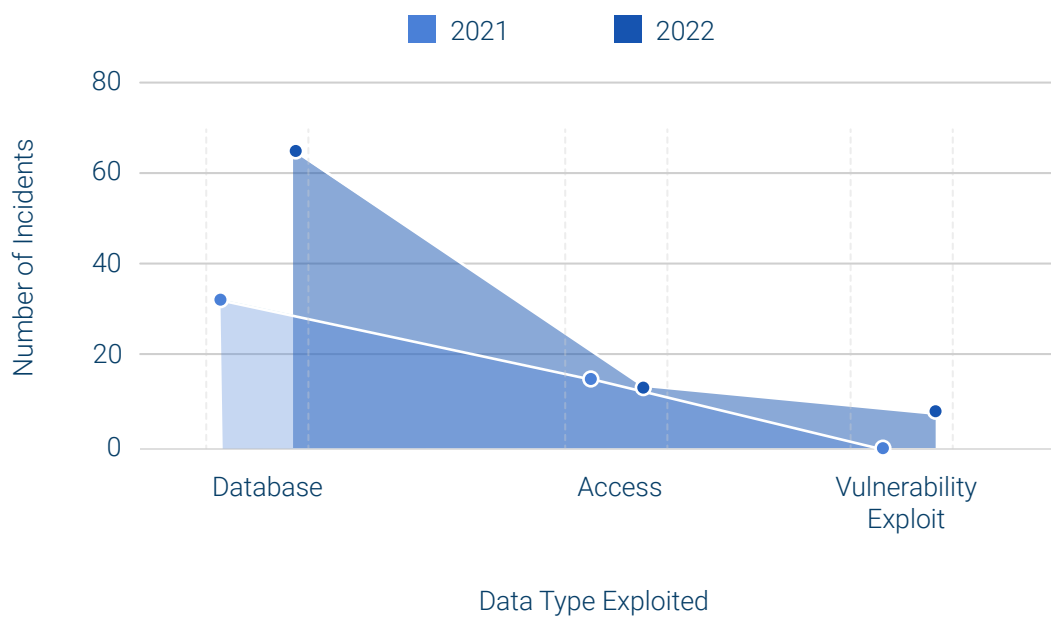
LockBIT 2.0

- LockBit 2.0 is an affiliate-based Ransomware-as-a-Service (RaaS) threat group, which employs a wide variety of tactics, techniques, and procedures (TTPs)
- The group is known for compromising victim networks by leveraging compromised access, unpatched vulnerabilities, insider access, and zero-day exploits.
- LockBit first appeared in September 2019, when it was dubbed as the “.abcd virus.”
- The group is known for using double extortion to pressure victims into paying the ransom.
- The group’s targets include organizations in the United States, China, India, Indonesia, Ukraine, and European countries.

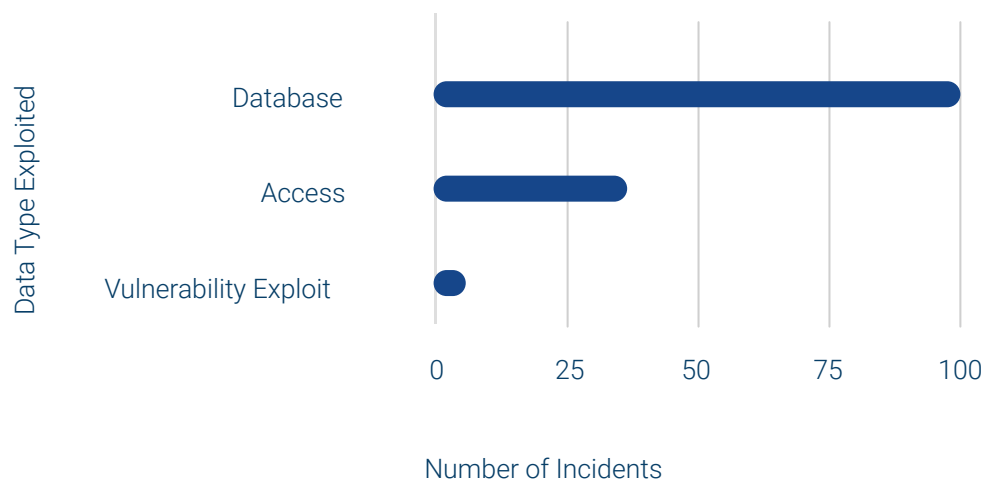


Commonly Sought After Data Types

Type of data posted on underground forums in posts related to the healthcare industry in first four months of 2021 and 2022



Type of data posted on underground forums in posts related to the healthcare industry in 2021



Database

- In both 2021 and 2022, databases were the most generally sought-after data type, with 69.2% of reported cases involving the leak or sale of databases in the healthcare industry in 2021. This figure increased to 78.6% in the first four months of 2022.
- The exploited databases include Personally Identifiable Information (PII) of patients and healthcare workers from various medical institutions, along with administrative information such as blood donor records, ambulance records, vaccination records, caregiver records, login credentials, etc.

The PII data fields leaked include:



Access

- Threat actors were found selling access to medical websites, equipment, and internal networks. The major types of accesses sold were:



- In 2021, accesses were involved in 27.3% of the cyber attacks on the healthcare industry. This figure reduced to 13.1% in the first four months of 2022.

Increase in Dark Web Activity Related to the Healthcare Industry

Bishop Eye Center Breach, USA

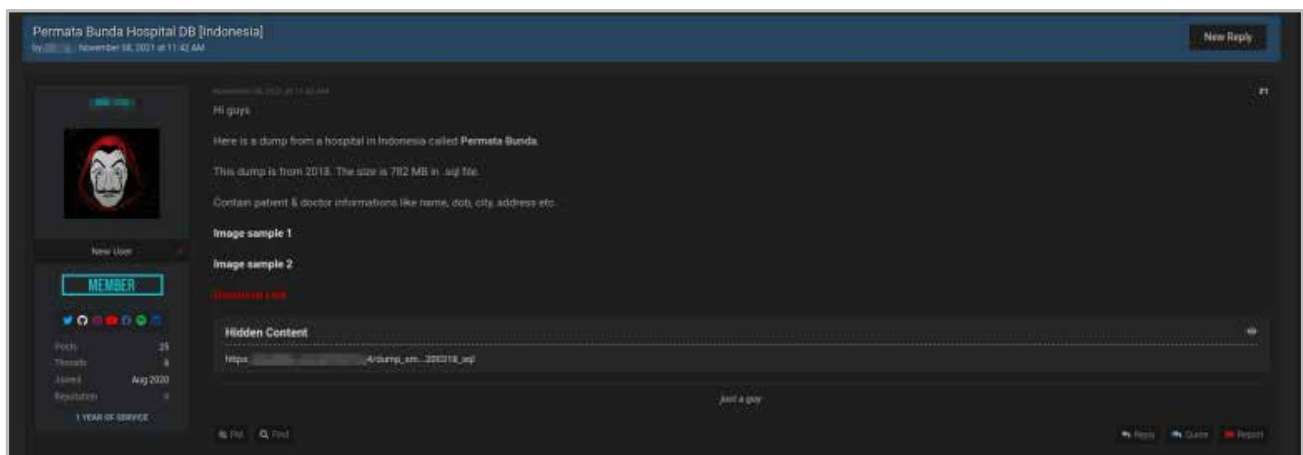
- On 06 February 2022, the BlackCat ransomware group announced that they have breached Bishop Eye Center through a post on their PR site.
- Bishop Eye Center is a leader in refractive cataract surgery, based out of South Carolina, USA.
- The breach compromised the database of Bishop Eye Center, along with their patients' confidential information.
- The sample images shared as proof of the breach showed that the group had access to patient data such as name, address, and date of birth, along with details related to their passports, credit cards, their medical records, etc.
- BlackCat is a ransomware written in the Rust language, which first appeared in late November 2021. It is one of the most sophisticated malware programs that can allegedly infect various Windows and Linux operating system versions.



Bishop Eye Center data breach post on the BlackCat PR site

Permata Bunda Database Leak, Indonesia

- On 10 November 2021, a threat actor published a post on a cybercrime forum advertising the database files of an Indonesian hospital named Permata Bunda, Bekasi.
- The database files were from 2018 and contained sensitive medical information of patients and doctors.
- Screenshots of the code snippets as well as a link to download a sample dataset was provided in the post as proof.



Threat actor's post on the cybercrime forum

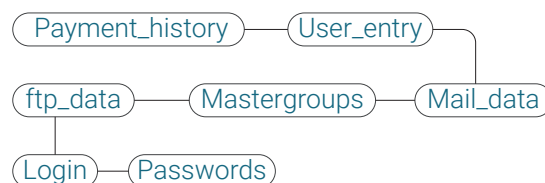
```
M_PatientID,  
M_PatientName,  
M_PatientAddress,  
M_PatientPhone,  
M_PatientHP,  
M_PatientEmail,  
M_PatientFax,  
M_PatientPinBB,  
M_PatientPostCode,  
M_PatientDOB,  
M_PatientHospitalNoReg,  
M_SexName,  
M_CityName,  
M_ProvinceName,  
d1.M_DoctorName,  
d2.M_DoctorName,  
M_PatientTypeName,  
M_PatientNoReg,  
T_ResultTypeName,  
S_SystemsID,  
S_SystemsLogo,  
S_SystemsLogoUrl,  
S_SystemsServerName,  
S_SystemsCompanyLogo,  
if(S_SystemsCompanyLogoUrl like '%server%', S_SystemsServerName, '') as cobacobi,  
Replace(S_SystemsCompanyLogoUrl, '%server%', S_SystemsServerName) as S_SystemsCompanyLogoUrl,  
S_SystemsCompanyName,  
S_SystemsCompanyAddress,  
S_SystemsCompanyCity,  
S_SystemsCompanyPhone,
```

Leaked database fields

Insight Product Development Initial Access, USA

- On 20 September 2021, a threat actor published a post on a cybercrime forum advertising the initial access to Insight Product Development.
- SQL infrastructure of the website displaying different schemes, tables, and columns was shared as proof of access. The actor further claimed to have access to the information of the root users.
- Screenshots of the code snippets as well as a link to download a sample dataset was provided in the post as proof.

- The columns of the database tables shared include:



- The sample shared also contained the technologies along with their versions that were exploited.



Threat actor's post on the cybercrime forum

VPN Access to Angelini Pharma, Italy

- On 22 September 2021, a threat actor published a post on a cybercrime forum advertising internal VPN access to a healthcare firm with annual revenue of USD 1 billion.
- CloudSEK researchers believe that the affected institution is most likely Angelini Pharma.
- Angelini Pharma is a pharmaceutical company based in Italy that markets its products across 70 countries.
- The internal access was sold in an online auction for a price range of USD 3,000 to USD 5,000.

VPN Access to Al Borg Medical Labs, Saudi Arabia

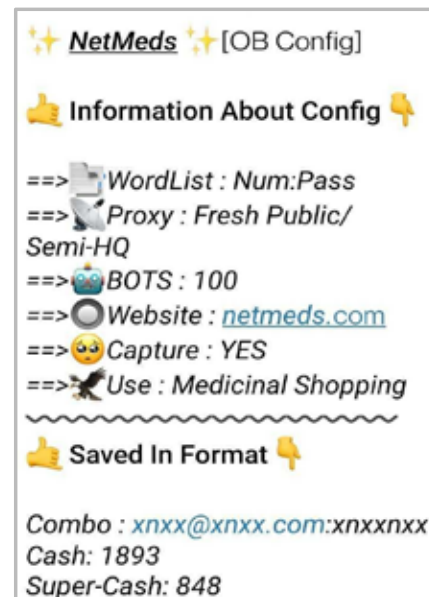
- On 27 September 2021, a threat actor published a post on a cybercrime forum, advertising the internal VPN access to a medical laboratory that has an annual revenue of USD 150 million.
- CloudSEK researchers believe that the affected institution is most likely Al Borg Medical Labs.
- Al Borg Medical Labs is a medical laboratory that provides health testing services in Saudi Arabia.
- The internal access was sold in an online auction for a price range of USD 1000 to USD 2500.



Threat actor's post on the cybercrime forum

Netmeds OpenBullet Configuration, India

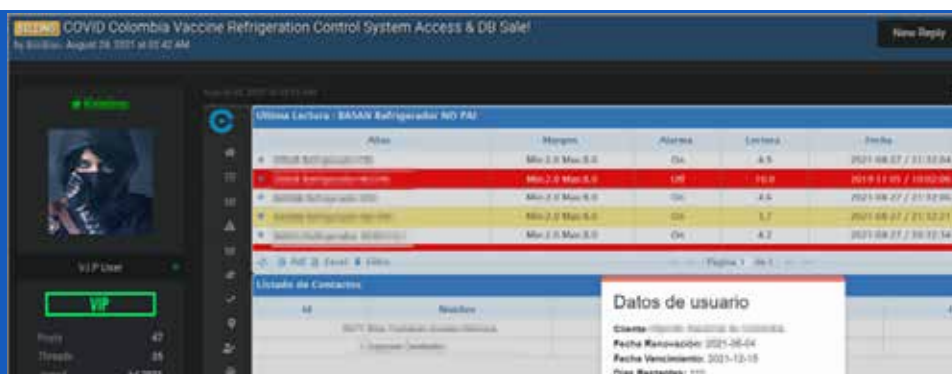
- On 31 August 2021, a threat actor published a post on a Telegram channel advertising the OpenBullet (OB) configurations to a pharma website called Netmeds.
- Netmeds is an Indian e-pharma portal that provides authenticated prescription and over-the-counter (OTC) medicines along with other health products.
- The configuration was shared for free and the compromised user accounts were shared as proof of the breach.



Threat actor's post on the Telegram Channel

MiCentinela Application User Database Leak, Colombia

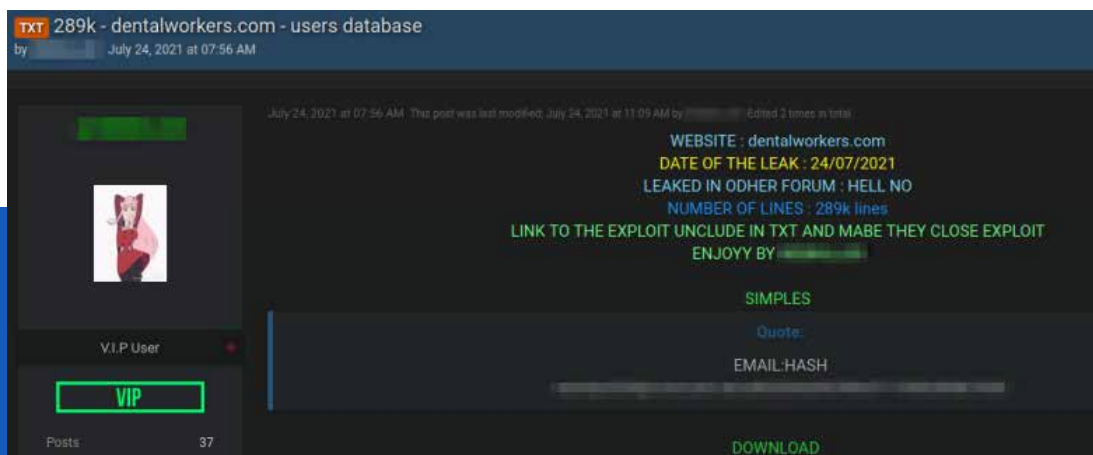
- On 28 August 2021, a threat actor published a post on a cybercrime forum advertising the user database and system access of Colombia Vaccine Refrigeration Control through the MiCentinela application.
- MiCentinela is an application that provides real-time temperature monitoring services, catering to corporate clients through a series of cold chains.
- As proof of the breach, a sample screenshot containing client information and database of the application's users was also shared.
- The data allegedly contained the information of 2000 clients including the Colombian army, institutions, laboratories, and vaccination centers.



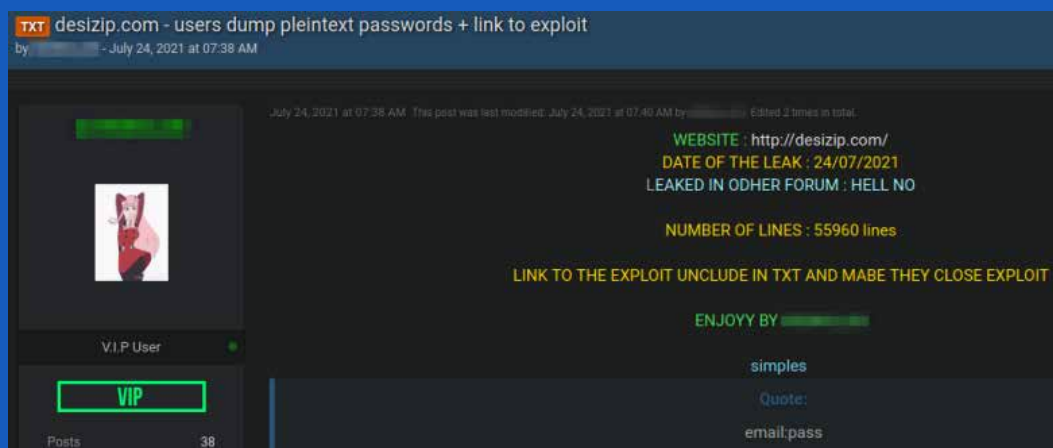
Threat actor's post on the cybercrime forum

Dental Workers, USA, and Desi Zip, India, Multiple Databases Leaked

- On 24 July 2021, a threat actor published multiple posts on a cybercrime forum advertising databases of two different organizations, Dental Works and Desi Zip.
- Dental Workers, founded in 2000, is a USA-based online staff recruitment platform exclusively for dentists.
- Desi Zip is an Indian online classifieds website for businesses, products, and services.
- The data provided in the posts could be downloaded with a few forum credits. These databases contain 289,000 records from Dental Workers and 55,960 records from Desi Zip.



Threat actor's post on the cybercrime forum advertising the database of Dental Workers



Threat actor's post on the cybercrime forum advertising the database of Desi Zip

150 Million COVID 19 Vaccination Records, India

- A threat actor published a post on a cybercrime forum advertising the records of 150 million Indians who have received the COVID 19 vaccination and selling them for USD 800.
- On 27 May 2021, another threat actor advertised a database containing 150 million records of vaccinated Indian citizens over a private Telegram channel. This database was being sold for USD 1,000.
- Many members of the cybersecurity community believed this to be a scam.

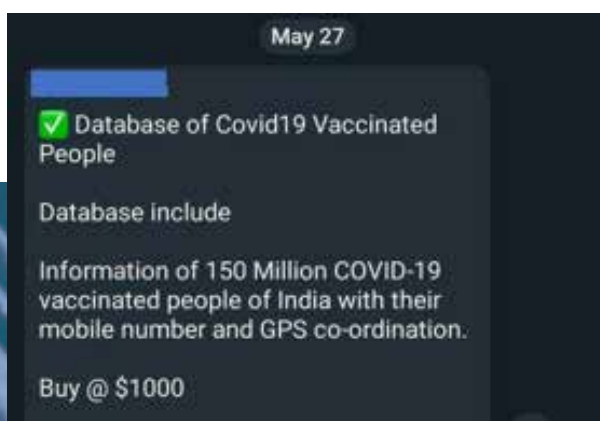
Database of Covid19 Vaccination INDIA

June, 2021 / Leak / Price: \$800

Information of 150 Million COVID19 Vaccinated People of India with their Name, Mobile Number, Aadhaar ID, GPS (Pin Point) Location, State etc. (PLEASE NOTE: WE ARE NOT THE ORIGINAL LEAKER OF THIS DATA. WE ARE RESELLER)



Threat actor's post on the dark web forum



Post on the private Telegram channel



Why is the Healthcare Industry a Desirable Target for Cybercriminals?

The numerous attacks on the healthcare industry turn up the question of why it has become such a popular target for criminals all across the world. Here are a few reasons why healthcare is one of the most targeted industries worldwide.

Patient Information

Medical industry has a plethora of patient records containing personal and sensitive information such as name, address, contact details, social security number, and financial information. This confidential data can be sold easily for a huge sum of money.

Insecure Medical Devices

With increasing advancements in technology, the number of medical devices in healthcare institutions has risen rapidly. With the primary focus of such devices being healthcare, more often than not they aren't equipped with proper security algorithms. Although most of these devices don't store patient information, they can be leveraged by attackers to access the

network of servers these devices are connected to, which store valuable information.

Unprepared Medical Professionals

Medical staff working for long erratic hours on tight schedules do not have the time or resources to gain expertise in cybersecurity practices. Thus, due to the complexity of cybersecurity solutions and the unavailability of proper security teams in medical institutes, no one on the front lines can detect vulnerabilities or compromised systems.

Remote Access to Data

Confidential patient data needs to be available to multiple medical professionals, on-site and remote for proper examination. Especially after the pandemic, remote access to data has become an important element of the healthcare industry. In such a time-sensitive environment, data is shared instantly without consideration for the security of the devices on which it is shared.



Common Attack Vectors

Our analysis shows that the following are immediate challenges to the healthcare sector:

Phishing & BEC (Business Email Compromise)

- Phishing is the most common cyber threat in healthcare, where malicious links are embedded in an otherwise innocent email.
- Business Email Compromise or BEC, referred to as the “Billion Dollar Scam” by the Federal Bureau of Investigation (FBI) is where scammers use a spoofed email or compromised account to trick employees into initiating a money transfer to an alternate (fraudulent) account.
- Several phishing campaigns were uncovered during the global pandemic, in which attackers posed as the WHO (World Health Organization) and sent malicious links to people claiming to be the most recently issued safety guidelines.

Ransomware

- Ransomware is one of the most popular attack vectors used by cybercriminals to target and compromise the healthcare industry.

- Malware is injected into a network during a ransomware attack to infect and encrypt sensitive data until a ransom amount is paid.
- Inspired by the ease of implementation of the Business as a Service (BaaS) model, cybercriminals have developed their variant known as Ransomware-as-a-Service (Raas).
- According to XVigil data, the most common ransomware variant used in healthcare sector attacks in 2021 is LockBIT 2.0, closely followed by Conti and Hive.

DDoS Attacks (Distributed Denial of Service)

- DDoS attacks are a commonly used by hackers and cybercriminals to overwhelm a network to the point of inoperability.
- The increased global digitization in the healthcare sector has provided attackers new opportunities to launch DDoS attacks on vulnerable devices and make a quick buck.
- Although these attacks do not pose the same risks of data exfiltration as ransomware attacks, they do cause the same operational disruptions.

- In September 2020, German authorities reported that an apparently misdirected ransomware attack caused the failure of IT systems at a major hospital in Düsseldorf, which resulted in the death of a woman who required immediate admission, after being transferred to another city for treatment.

Insider Threats

- Insider threats are employees or individuals with authorized access who may disrupt, reveal, or alter sensitive information in an information management system.
- Individuals working in healthcare institutions have access to a massive amount of patient information, which they need from time to time for treatment and diagnosis. As a result, it is common in the healthcare industry for an employee to be an insider threat, either knowingly or unknowingly.
- According to the 2021 Data Breach Investigations Report published by Verizon, insiders are responsible for almost 22% of security issues in the healthcare industry.

Critical Infrastructure & Medjacking

- Cyber attacks on critical infrastructure can target key technologies, processes, networks, services, systems, and facilities that are crucial to public safety.
- The attacks specifically aimed at hijacking

the medical devices are termed as “medjacking”.

- To provide effective services, healthcare institutions rely on critical infrastructure (equipments such as ventilators, CT scans, pacemakers, and so on). As a result, cyber-attacks on critical infrastructure might have disastrous repercussions.
- According to Kim Zetter of The Washington Post, Israhers have developed a computer virus that can infuse tumors into CT and MRI scans. Such malware can lead to misdiagnoses and the implementation of wrong treatment procedures.
- Old physical infrastructure, increasing energy prices, natural disasters, ever-changing regulatory requirements, and a shortage of experienced staff have an impact on healthcare critical infrastructure.

Vulnerabilities & Exploits

- Many threat actor groups begin their attack on any target organization by exploiting publically known software or web vulnerabilities.
- The Covid-19-assisted digitization has resulted in greater cloud storage as well as additional endpoints for threat actors to exploit.

Mitigation Measures

Given the scale and significance of the healthcare industry, it is vital for institutions, employees, and healthcare professionals to ensure that the data they gather and store is not leaked or exploited by cybercriminals. To ensure this, we recommend that:

- Healthcare institutions and related government entities should:
 - Follow the HIPAA (Health Insurance Portability and Accountability Act) compliance
 - Create awareness among users regarding cyber-attacks, online scams, and phishing campaigns
 - Enact strong password policies and enable multi-factor authentication (MFA)
 - Update and patch software, systems, and networks regularly
 - Maintain multiple backups, both online and offline, in separate and secure locations
 - Monitor logs for unusual traffic and activity to websites and other applications
 - Block illegitimate IP addresses and deactivate port forwarding using network firewalls
 - Perform real-time monitoring of the internet to identify and mitigate low-hanging threats, such as misconfigured apps, exposed data, and leaked accesses, that are leveraged by cybercriminals to carry out large scale attacks
- Healthcare professionals, including the hospital faculty and staff should:
 - Avoid clicking on suspicious emails, messages, and links
 - Not download or install unverified apps
 - Use strong passwords and enable multi-factor authentication (MFA) across accounts



Impact of Cyberattacks on the Healthcare Industry

The cyberattacks on the healthcare industry impact everyone including healthcare organizations, staff, and patients. The impact is often threefold:



Financial

Cyber Attacks cause significant damage to healthcare institutions' funds. Cyberattacks such as wire fraud and extortion cause monetary loss. Healthcare institutions may also have to pay for the damage caused to the individuals. If the data was handled carelessly, the institutions can also face legal ramifications.



Organizational

If customer data is compromised, companies can suffer reputational damage, resulting in a decrease in the trust of customers. Cyberattacks can also lead to a decrease in productivity. Ransomware attacks and data breaches can force medical organizations to halt all business operations. This can lead to a potential threat to many patients' lives.



Personal

If the PII records of individuals are compromised they can become vulnerable to cybercrimes such as identity theft, financial fraud, and tax fraud. The termination of medical procedures leads to a delay in the diagnosis and treatment of patients. Obstruction in the working of critical medical equipment can lead to life-threatening situations for some patients.

Create a Cyber Resilient Healthcare Ecosystem

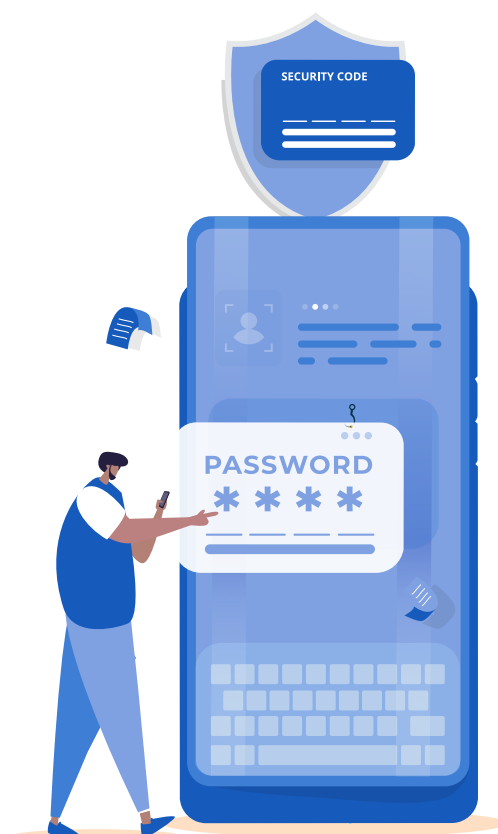
Cyberattacks on the healthcare industry impacts everyone including healthcare organizations, staff, and patients. To minimize these, it is important to create a resilient healthcare ecosystem.

The COVID-19 pandemic forced the healthcare industry to adopt various new technologies which they weren't fully equipped to handle. The transition wasn't smooth and left multiple gaps in cybersecurity for the attackers to exploit. Along with this, the rapid digitalization done by the healthcare companies to keep up with the growing market and competition has given cybercriminals new opportunities to exploit the industry.

Budget constraints also add to the cybersecurity troubles faced by the healthcare industry. It is expensive to replace legacy software and when these aren't kept up to date with important updates and vulnerability patches the consequences are faced in the form of cyberattacks. Besides this, medical care providers are not aware of the increasing cybersecurity threats to the industry.

Thus, it is important to realize the severity of the issue and try our best to equip the healthcare staff against cybersecurity attacks. This can be achieved by educating them to

identify common cyber threats such as phishing attacks by conducting various seminars, conferences, and cyber awareness training sessions. Having a well-funded and widely supported cybersecurity strategy would protect healthcare organizations and consumers from financial and reputational losses.



Resources

- US Healthcare Industry in 2022: Analysis of the health sector, healthcare trends, & future of digital health : <https://csek.me/nl66>
- Consumer Healthcare Market Size | Share | Trends | Analysis | Forecast : <https://csek.me/al7H>
- NHE Fact Sheet | CMS : <https://csek.me/ql4P>
- The State of Healthcare Industry – Statistics for 2022 : <https://csek.me/FI56>
- The \$11.9 Trillion Global Healthcare Market: Key Opportunities & Strategies (2014-2022) : <https://csek.me/tzqg>
- Healthcare IT Market Size and Share | Industry Growth By, 2030 : <https://csek.me/MzwN>
- Healthcare IT Market Size & Share Report, 2022 - 2030 : <https://csek.me/czeK>
- Home Healthcare Market Size & Share Report, 2030 : <https://csek.me/ozrv>
- 30 Healthcare Statistics 2021: Industry, US Market Size, Tech : <https://csek.me/Rzt3>
- A Comprehensive Guide to Remote Patient Monitoring : <https://csek.me/LzyQ>
- Remote patient monitoring - Wikipedia : <https://csek.me/Zzup>
- Internet of things - Wikipedia : <https://csek.me/4ziD>
- What Is the Internet of Things (IoT)? | Oracle India : <https://csek.me/hzoD>
- Cybersecurity in Healthcare | HIMSS : <https://csek.me/Dzpm>
- Cybersecurity threat to remote monitoring devices • healthcare-in-europe.com : <https://csek.me/mza2>
- Top 5 Cybersecurity Threats to Electronic Medical Records | Integracon : <https://csek.me/Nzs6>
- Cyber Attacks: In the Healthcare Sector : <https://csek.me/Lzdm>
- Top 5 cyberattacks against the health care industry | Stormshield : <https://csek.me/gzfi>
- German hospital hacked, patient taken to another city dies - ABC News : <https://csek.me/yzgD>
- Biggest Cyber Threats in Healthcare (Updated for 2022) | UpGuard : <https://csek.me/jzhW>
- Healthcare Critical Infrastructure Solutions : <https://csek.me/uzjr>
- 8 Cyberattacks on Critical Infrastructure : <https://csek.me/yzk4>
- The 5 Major Cybersecurity Threats Against the Healthcare Industry in 2021 : <https://csek.me/ezl8>
- Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists - The Washington Post : <https://csek.me/8zzL>
- 9 Reasons Healthcare is the Biggest Target for Cyberattacks : <https://csek.me/szxq>
- Cybersecurity in the healthcare industry : <https://csek.me/mzcl>
- Increased Cyberattacks On Healthcare Institutions Shows the Need For Greater Cybersecurity : <https://csek.me/xzvm>

Note : The links have been shortened for brevity.



About CloudSEK

CloudSEK is a contextual AI company that predicts Cyber Threats even before they occur. We combine the power of Cyber Crime monitoring, Brand Monitoring, Attack Surface monitoring, and Supply chain intelligence to provide context to our customer's digital risks. Our unified dashboard allows customers to triage and visualize all digital threats in one place. We also offer workflows and integrations to manage and remediate the identified threats.

To learn more about CloudSEK, visit cloudsek.com.