CYBLE

The Medical Industry Is at Risk

Navigating the Cyber Threat Landscape of the Indian Healthcare Sector

TABLE OF CONTENTS

Introduction

India is an emerging medical tourism destination, and Healthcare is one of the largest sectors of the Indian economy in terms of revenue generation and employment. In addition, the nation's 140 billion population and diverse healthcare needs propel India's public care sector to a fast-growing industry of over USD350 billion.

India's significant measures to digitize Healthcare over the last five years have enhanced India's position in the world's Healthcare ecosystem, be it dealing with the pandemic, developing the COVID-19 vaccines, lowering healthcare costs, improving healthcare facilities, and extending public healthcare benefits to rural citizens. It has also elevated the Indian Pharmaceutical & Biotechnology industry to dominate the global value chain.

This economic rise of the Indian Healthcare and Pharmaceutical industry, coupled with the healthcare data of billions of citizens being added to the internet, has led to new cybersecurity challenges grappling the country.

In the second half of 2022, a series of high-profile cyberattacks became a cause of concern for India, emphasizing the need for strong cybersecurity measures to secure sensitive patient data and the growing need to combat security threats to the entire value chain involving Healthcare, Pharma, and Insurance sectors.

Cyble Research & Intelligence Labs (CRIL) is closely monitoring the changing dynamics of cybersecurity and threats faced by the Indian Healthcare sector.

Ransomware Attacks

In March 2023, the Indian Healthcare industry was in the crosshairs of ransomware groups, as we witnessed industry stalwarts like Sun Pharmaceutical Industries and Piramal Group affected due to the cyberattacks.

Subsequently, a healthcare technology company – TharWorx, was compromised in a recent attack by the LOCKBIT ransomware group, making public 3 GB of the company's sensitive data from allegedly 20 GB of data.

Previously, Laxmi Organic Industries Ltd., a manufacturing intermediary for a wide array of pharmaceuticals applications, including lifesaving drugs, was targeted by the LOCKBIT ransomware group in January 2023, leaking over 41 GB of data.

The widespread and one of the fiercest cyberattacks on India's premier hospital, All India Medical Institute of Medical Sciences (AIIMS), in November 2022, forced the hospital to move to manual operations.

As per reports, the ransomware attack, possibly perpetrated by Chinese actors, affected all 100 servers of the hospital and kept AIIMS offline for about two weeks. In the same month, the second most prominent government hospital in Delhi, Safdarjung Hospital, and the top medical body, the Indian Council of Medical Research (ICMR), also suffered severe cyberattacks.

While Aarti Drugs Ltd. and Ipca Laboratories Limited were hit by cyberattacks on September 9, 2022, and September 10, 2022, respectively, by the BianLian ransomware group and RansomHouse extortion groups., BianLian claimed to compromise the internal documents of Aarti Drugs, including financial documents, employee data, and the company's internal secrets on their leaked site.

Ipca Laboratories suffered a 500 GB data breach during the attack that affected employee records, formulation data, and financial and audit reports. RansomHouse leaked 140 GB of the company's files claiming that the negotiations had failed.

Underground Forums Adding to Foray

Threat Actors (TAs) leverage the anonymity of underground forums for buying and selling unauthorized accesses and data, which are then used as initial vectors for large-scale cyberattacks. In the first quarter of 2023, CRIL observed and investigated the following noteworthy leads from underground forums:

- A TA leaked an Indian hospital database containing patient and doctor information. The TA has been consistently leaking Healthcare data from other countries too.

Figure 1: Compromised dataset of an Indian hospital leaked

- A TA offered to sell unauthorized access and a database dumped from the India-based Healthcare company Lloyd Healthcare Pvt. Ltd. The TA posted a sample of the 423,326 records, which included names and addresses of business leads (pharmacies), along with names and phone numbers of the point of contact (stockist).

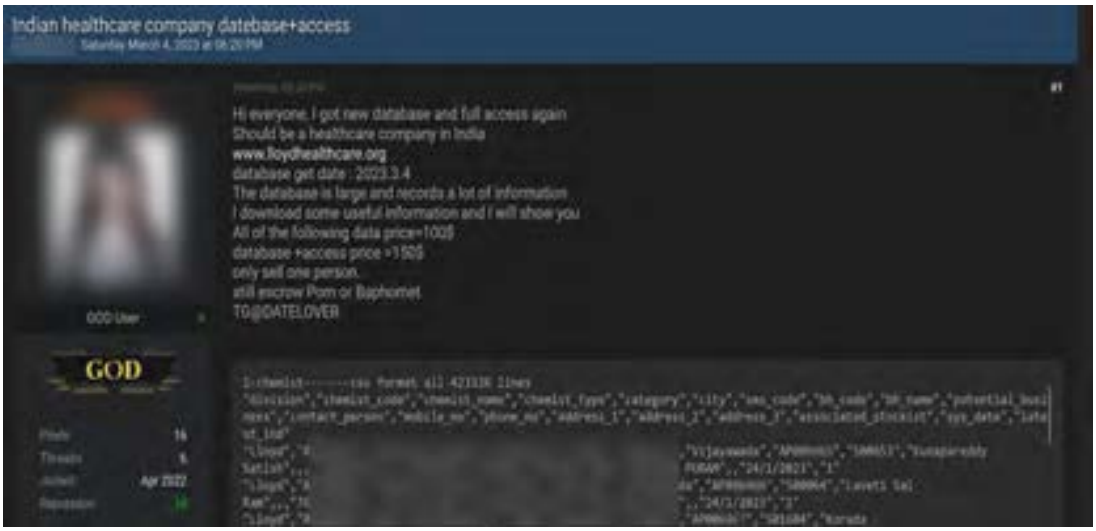


Figure 2: Unauthorized access to an Indian Healthcare company on sale

- A TA offered to sell database information allegedly belonging to covid19.ap.gov.in and claimed to have exfiltrated more than 500k records of users from the affected domain. After analyzing the sample, we observed that the data relates to citizens diagnosed with COVID-19. The data records contain Name, Patient ID, COVID-19 Sample ID, Locality, Mobile number, test result date, etc. We also observed that the latest timestamp on that data was from December 2022.

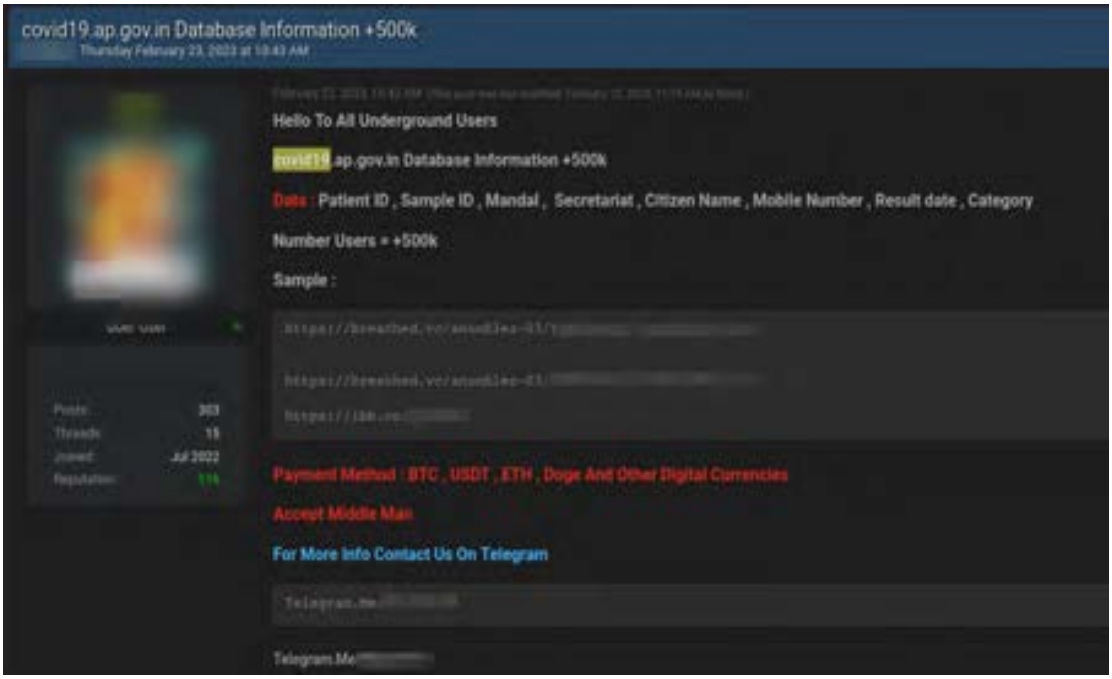


Figure 3: COVID patient data on sale

- In December 2022, a TA offered to sell Indian patient data allegedly stolen from Wockhardt. The TA claimed the data of 178066 patients under the headers Aadhar_no, age, comments, contact, current location, date, time, district, DOB, doctor-id, email, examination date, gender ID, patient ID, patient name, state, van-ID, and voter-ID.

  We investigated the samples and assessed that the data belonged to Wockhardt Hospitals, while the TA seems to have misattributed this data to Wockhardt's pharmaceutical business. It is evident from the post that the database was stolen from the company's backup servers. The samples reflected the timestamp of breached data from December 2021 to January 2022.

Figure 4: Wockhardt Hospital data on sale

- Alleged administrative access to the panel of the COVID-19 registration application, CoWIN (cowin.gov.in), operated by the Ministry of Health and Family Welfare of the Government of India, was put on sale by a TA on cybercrime forum in December 2022.

  According to the TA, the portal consisted of the name, address, and mobile information of about 5k staff users. TA also shared screenshots of the dashboard revealing name, mobile, job role, and last login details of the supervisors, vaccinators, and site managers associated with the COVID-19 vaccination drives.

Figure 5: Admin access to CoWIN panel on sale

- In November 2022, a TA was observed selling sensitive, Protected Health Information (PHI) from the Hospital Management System (HMS), allegedly stolen from Three Cube IT Lab Private Limited, a Chennai-based software solution company. The compromised database contained user records with login credentials and registered patients' details.

Figure 6: PHI was stolen from servers of an HMS provider on sale

- We observed a compromised database of Apollo Pharmacy PVT Ltd containing email, hashed password, and order date claimed associated with 600k users being sold on a cybercrime forum in September 2022.

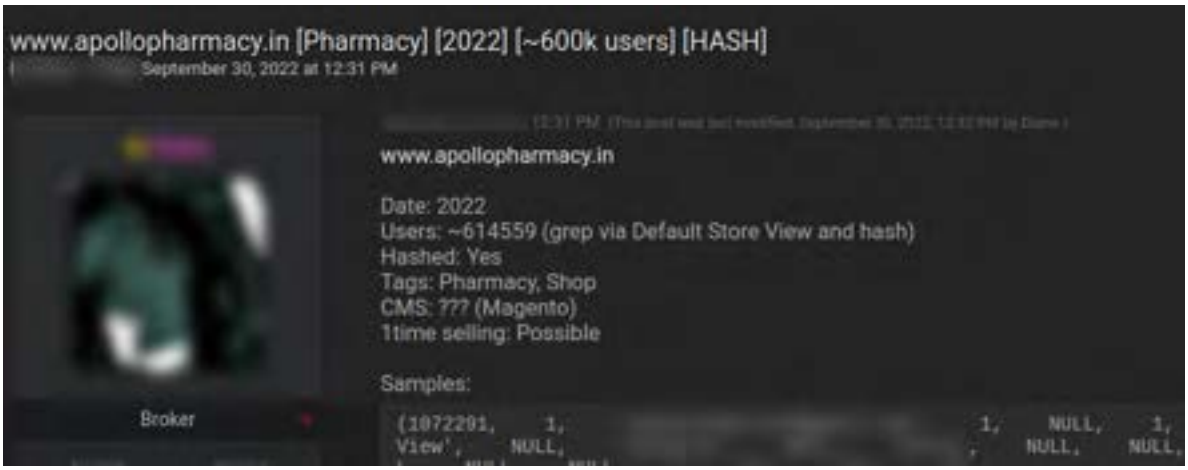


Figure 7: Apollo Pharmacy data on sale

- A thread advertising the sale of 6 databases allegedly from hospitals in West Bengal was observed in an underground forum in August 2022. The TA claimed access to Personally Identifiable Information (PII) of 329,000 patients, consisting of name, date of referral, referring hospital or medical center, age, sex, diagnosis, etc.

- An Indian Insurance provider, Mallapuram Insurance & Allied Services, suffered a data breach in August 2022 that resulted in over 7.5 GB of the data leak, including COVID-19 vaccine testing reports and documents of Sputnik V, among 28,000 other files.

Figure 8: Health Insurer's data leaked on the Telegram channel

Hacktivist Campaigns

The Russian hacktivist group PHOENIX, a known affiliate of KILLNET, claimed to target the Health Management Information System of the Indian Ministry of Health and Family Welfare in March 2023. The hacktivist group claimed the attack was in retaliation to India's neutral stand over the price cap coalition and sanctions by G7 countries on Russian oil imports.

The Mysterious Team Bangladesh is another prominent hacktivist group that has been observed to be targeting Indian hospitals.

Internet Exposure to Medical Devices and Applications

Exposing Medical devices and related applications over the internet is a significant concern in the Healthcare Sector as TAs usually target these applications to collect PHI data.

Especially when left exposed over the internet, widely used applications like OpenEMR and PACS systems can become an easy target of cyberattacks. These applications, combined with vulnerabilities and exploits available in the public domain, render an easy target for TAs to steal PHI and PII. Similarly, other web applications that offer Medical related services for storing PHI and PII data are vulnerable to attacks like injection, local file inclusion, authentication bypass, CSRF, etc.

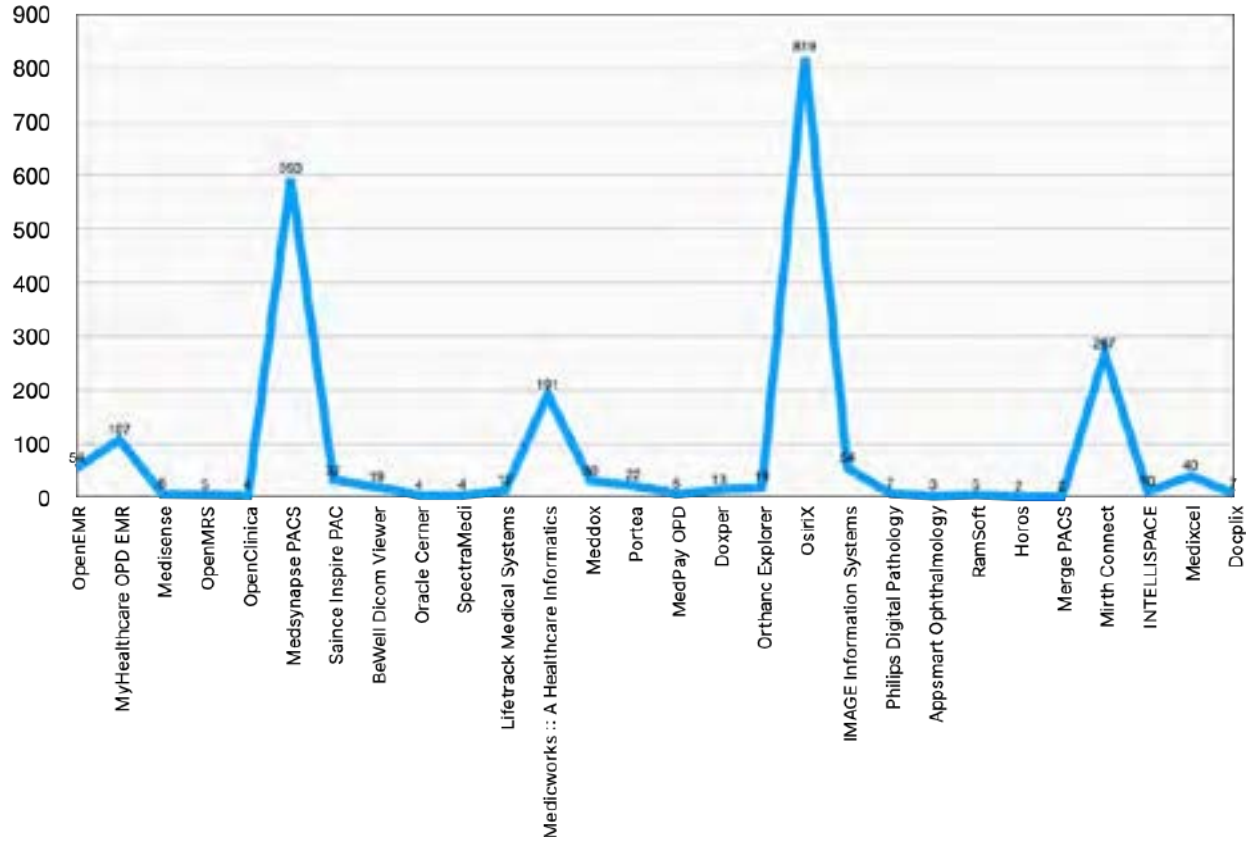
In most cases, the operators of medical applications generally lack cybersecurity domain knowledge and expertise, the applications used are outdated, and the patch management process is lackadaisical. These factors lead to further security weaknesses within the network.

Medical applications and devices are provided with factory default settings that need to be changed as per security protocols within the organization. However, on several occasions, these applications run on default or weak passwords, which can be quickly brute-forced by TAs.

CRIL investigated various medical devices and applications widely used within the Indian region and found nearly 2500 internet-exposed instances.

Note: Exposed instances do not indicate vulnerable products. Instead, they highlight the extensive attack surface within the Indian Public Health sector.

Internet Exposure Of Medical Devices And Application



PHI leaks via Misconfigurations

During the investigation, CRIL researchers observed multiple open directories leaking the PHI data of Indian citizens. The highly sensitive data found within these directories contain the following:

- Personal identifiers include name, address, date of birth, social security number, and phone number.
- Medical histories such as diagnoses, treatments, prescriptions, and test results.
- Payment information such as insurance information, billing records, and payment history.
- Genetic information such as DNA samples or results of genetic tests.
- Mental health information includes mental health diagnoses, counseling records, and psychiatric evaluations.
- Substance abuse information, such as records of drug or alcohol abuse treatment.

Attackers gaining access to such confidential PHI data are prone to sell it in the darkweb marketplaces and cybercrime forums. The data collected from these leaks is further vulnerable to being utilized by TAs for launching social engineering attacks and medical frauds. The figure below shows some instances of data leaked from exposed open directories.

Figure 9: Leaked PHI data of Indian citizens from an exposed open directory

Malicious Domains Impersonating Indian Health Entities

The prevalence of phishing campaigns targeting top hospitals and organizations within the Indian healthcare sector is a severe issue that cannot be ignored. Cybercriminals create targeted phishing campaigns to trick individuals into disclosing sensitive information such as PHI and PII.

Moreover, malicious domains in the garb of providing guides to download mobile applications also contain stealthy malware and stealers, making them a significant threat to individuals' mobile devices, which are used to store and access sensitive information. Upon entering an unsuspecting individual's mobile device, this malware and stealers can steal data, damage devices, and compromise sensitive information.

CRIL continuously monitors malicious campaigns targeting Indian critical infrastructure, including Healthcare and Pharmaceutical industries, to understand changes and developments and their associated risks. We observed several unsafe domains of impersonating Indian hospitals to trick patients into stealing their sensitive information.

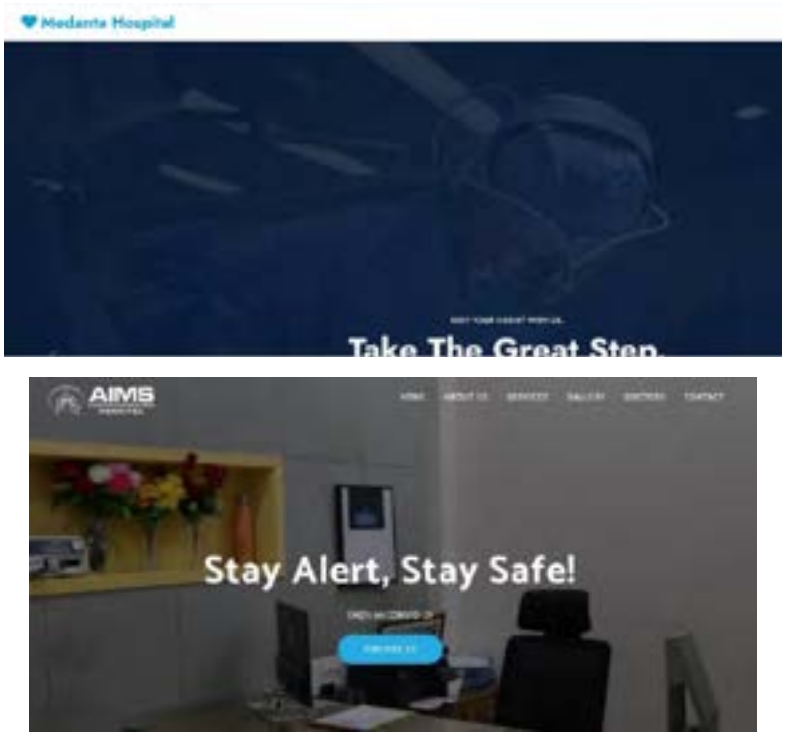


Figure 10: Malicious domains of prominent Indian hospitals

APT Groups Aiming at Indian Healthcare Sector

APT10

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

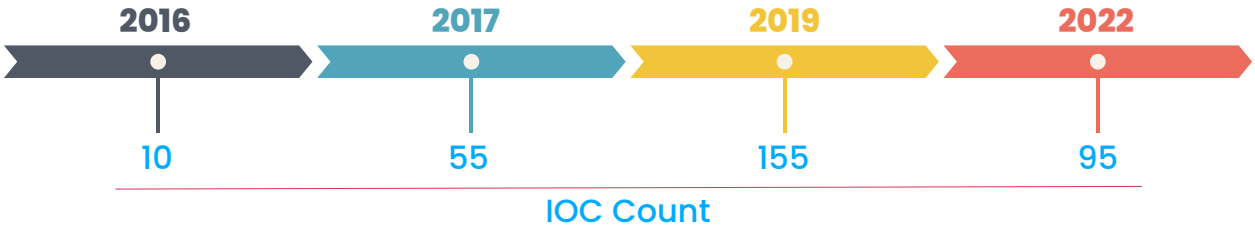


Figure 11: Activity timeline of APT10

APT29

APT29, aka CozyBear, is a highly dedicated and organized cyberespionage group reported to be working for the Russian Federation since at least 2008. The APT group is known to employ large-scale spear-phishing campaigns and use a vast arsenal of malware toolsets, like MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke, and GeminiDuke.

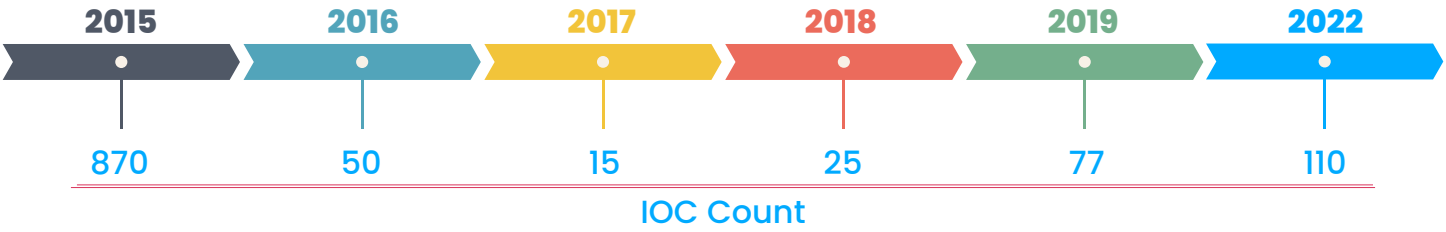


Figure 12: Activity Timeline of APT29

APT 37

APT37, aka Reaper, is reported to have North Korean government links. The group employs Social Engineering as an Initial vector against their targets and is also known to weaponize zero-day and existing vulnerabilities alongside a diverse suite of malware.

Figure 13: APT37 activity timeline

APT41

APT41, aka Wicked Panda, is reported to be a Chinese state-sponsored threat group that has been active since 2012. APT41 conducted primarily financially motivated operations focused on the video game industry before expanding into likely state-sponsored activities. Reports suggest the use of HIGHNOON malware that is used by other Chinese cyber espionage groups like Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon, and Mana.

The group is known to target the Healthcare and Pharmaceutical sectors in India, along with various other countries in Asia.

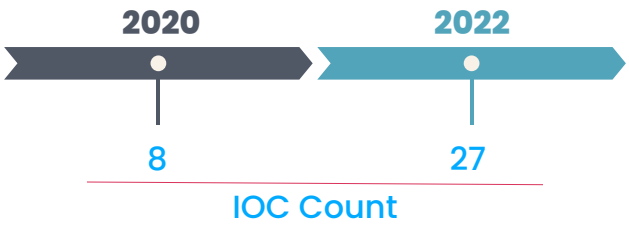


Figure 14: APT41 activity timeline

Fake Applications Targeting The Medical Industry:

Several medical brands have developed mobile applications for their consumers to access medicines easily, schedule doctor appointments, obtain online prescriptions, and more. However, malicious individuals are taking advantage of the popularity of these applications by creating fake apps.

CRIL detected multiple fake mobile applications of healthcare applications directed at deceiving Indian consumers into believing they are legitimate. These fraudulent apps include adware created by TAs to generate revenue by displaying advertisements to users. Additionally, some of these apps are modified versions of legitimate apps, classified as potentially unwanted programs (PUPs).

Figure 15: Fake applications impersonating an Indian Healthcare App

Furthermore, CRIL also discovered an Android Banking Trojan malware (4ccd949df507f9e13d621edb8164591b04f92318466b4669ffa0e8988cdbf9ce) using the identical package name "com.medscape.android" as the legitimate MedScape application.

Figure 16: Application Metadata Information

The Banking Trojan has the following advanced features:

- VNC
- Overlay injection for targeted applications
- Disabling play protect
- Granting auto-permissions
- Preventing uninstallation
- Stealing incoming SMSes with other sensitive details

The figure below shows the class names performing malicious activities and the code which creates an overlay by loading the HTML injection page into a WebView.

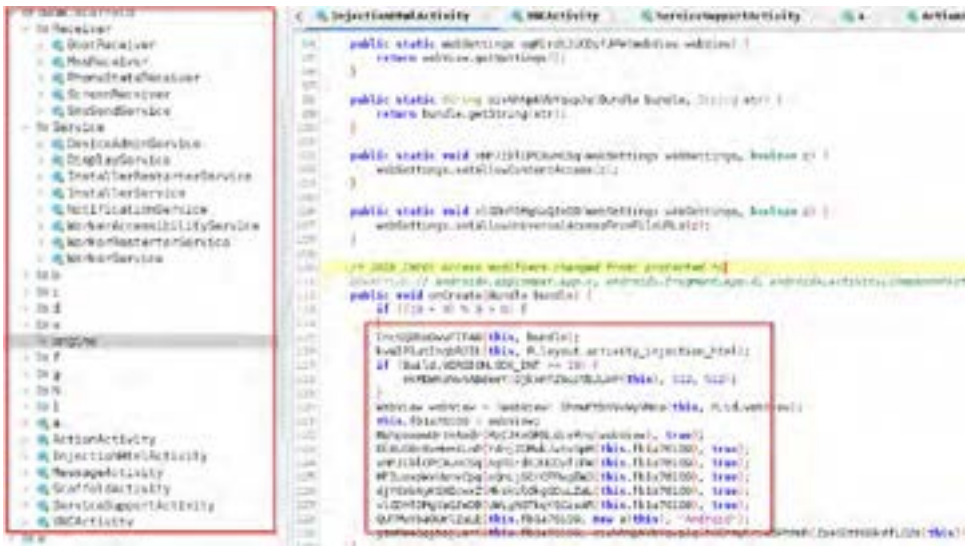


Figure 17: Overlay injection activity code and classes present in malware

Conclusion

The Indian Healthcare sector is one of the largest in the world, with a vast network of public and private hospitals, clinics, and medical centers. However, despite the significant progress made in recent years, the sector still faces numerous challenges, including a shortage of healthcare professionals, inadequate infrastructure, and limited access to healthcare services in rural areas.

The sector's vulnerability to cyberattacks has added another layer of complexity to these challenges. The increasing use of digital technologies and the internet of things (IoT) in Healthcare has led to an exponential increase in sensitive patient data being generated and transmitted across networks. It makes the sector an attractive target for cybercriminals seeking to exploit vulnerabilities and steal sensitive patient data for financial gain.

In recent years, several high-profile cyberattacks have been observed on healthcare organizations globally, highlighting the critical need for robust cybersecurity measures to protect against these threats.

Therefore, the Indian healthcare sector must prioritize cybersecurity and take a proactive approach to mitigate these risks to ensure the confidentiality, integrity, and availability of patient data and critical healthcare services.

Recommendations

Enterprises may implement the following measures to counter such cyberattacks:

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

About Us

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

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