KELA DATASHEET

CYBERCRIME THREATS TO THE

HEALTHCARE SECTOR

In 2023, the healthcare sector is a prime target for cybercriminals. Despite some threat actors avoiding attacking healthcare targets, various health related facilities, including hospitals, clinics, mental health organizations and pharmaceutical companies, remain vulnerable to cyberattacks.

The healthcare sector faces a distinct risk to its data compared to other industries. While personal information like names, email addresses, Social Security Numbers, and financial details can be compromised in various sectors, the healthcare sector deals with even more sensitive data, including medical reports, private body images for medical purposes, medical scans, psychological assessments, and other highly personal information that could be compromised. In addition, this sector delivers critical and at times life-saving services, that can be jeopardized by such incidents.

In addition to attacks directly on healthcare institutions, third-party vendors, commonly used by healthcare institutions, are also under attack, for example, an attack on a shared IT supplier has recently affected daily work in 5 Canadian hospitals.

Towards the end of 2023, KELA delves deep into the persistent threats against the healthcare sector from the past year, including ransomware attacks, network access offers, data breaches and hacktivist groups' attacks.

RANSOMWARE ATTACKS

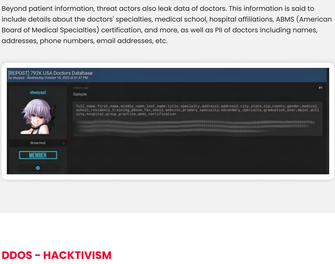
Ransomware attacks on healthcare have led to various consequences, such as diverting patients to other hospitals, disruptions in accessing lab results and electronic medical records (1),(2), delays in treatment, and even the permanent closure when smaller and rural facilities are targeted.

Healthcare institutions face a significant risk from ransomware, as cybercriminals recognize the likelihood of these institutions negotiating or paying a ransom to prevent disruptions to patient care. According to KELA's analysis of ransomware incidents and data leaks, ransomware and extortion actors have persistently targeted the healthcare sector, impacting over 800 victims since 2021. In 2023, this sector ranked among the top 3 most targeted, with over 40 victims. The United States is the most targeted country in this sector, and in overall targeting as well, accounting for approximately 63% of ransomware attacks in the healthcare sector in the past year. The prominent ransomware groups targeting healthcare in 2023 include LockBit, Clop, Alphv, and BianLian, collectively responsible for about 50% of the ransomware attacks in the past year. BianLian, unlike the other actors, is not usually in the top, but it appears that the healthcare sector is one of the two the most targeted sectors for the group this year.

NETWORK ACCESS OFFERS

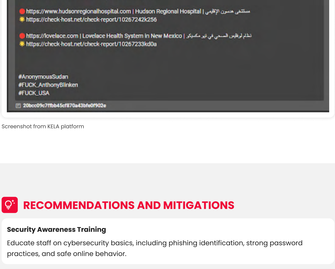
Initial Access Brokers (IABs) play an important role in a ransomware-as-a-service supply chain by supplying access to compromised networks. In 2023, KELA identified around 85 instances of healthcare network access being offered for sale, with the United States being the primary target, accounting for over half of these cases.

The entities targeted for access include public and governmental organizations, as well as private companies and hospitals, which can allow actors to search, and edit patetins' data.

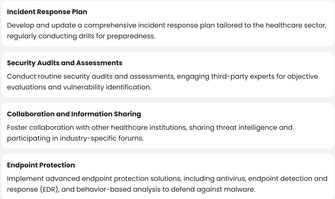


DATA LEAKS

Healthcare organizations house sensitive and confidential information that can be highly valuable for threat actors, and can be further leveraged for phishing, spear-phishing, social engineering, and extortion attacks targeting patients whose personal data has been compromised. Cyber chatter indicates a substantial supply of healthcare-related data, accompanied by actors' demand. KELA has observed threat actors leaking for free and offering for sale Personal Identifying Information (PII) and private medical information from health entities. This includes patient details such as name, sex, age, address, medical reports, and patient lab samples, along with pharmacy-related data, encompassing credit card information and emails with clean passwords.



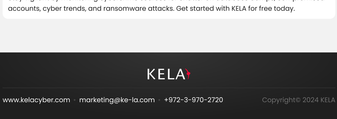
Beyond patient information, threat actors also leak data of doctors. This information is said to include details about the doctors' specialties, medical school, hospital affiliations, AIMG (American Board of Medical Specialties) certification, and more, as well as PII of doctors including names, addresses, phone numbers, email addresses, etc.



DDOS - HACKTIVISM

Distributed Denial of Service (DDoS) attacks pose a significant threat to the healthcare sector, potentially resulting in damage to online services, reputation, as well as financial loss. Some attacks are performed by financially motivated threat actors, and some by hacktivist groups driven by ideological motives, launching attacks against specific countries or companies, such as hacktivists involved in the Israel-Palestine or the Russia-Ukraine conflict.

For example, during the Israel-Hamas war (since October 7, 2023), Israeli hospital websites, including Sheba Medical Center, Rambam Hospital, and Herzog Medical, were targeted in DDoS attacks. Moreover, amid the ongoing Russia-Ukraine war, pro-Russian hacking groups have directed attacks towards institutions in countries supporting Ukraine, including Anonymous Russia and Anonymous Sudan, who targeted various websites of US-based hospitals.



Screenshot from KELA platform

RECOMMENDATIONS AND MITIGATIONS

Security Awareness Training

Educate staff on cybersecurity basics, including phishing identification, strong password practices, and safe online behavior.

Regular Backups

Maintain secure offline backups of critical data and systems to mitigate the impact of ransomware attacks.

Multi-Factor Authentication (MFA)

Implement MFA for accessing sensitive data and systems to add an extra layer of security against credential reuse.

Incident Response Plan

Develop and update a comprehensive incident response plan tailored to the healthcare sector, regularly conducting drills for preparedness.

Security Audits and Assessments

Conduct routine security audits and assessments, engaging third-party experts for objective evaluations and vulnerability identification.

Collaboration and Information Sharing

Foster collaboration with other healthcare institutions, sharing threat intelligence and participating in industry-specific forums.

Endpoint Protection

Implement advanced endpoint protection solutions, including antivirus, endpoint detection and response (EDR), and behavior-based analysis to defend against malware.

Monitor Cybercrime Platforms

Stay vigilant by monitoring cybercrime sources for chatter on database dumps, compromised accounts, cyber trends, and ransomware attacks. Get started with KELA for free today.