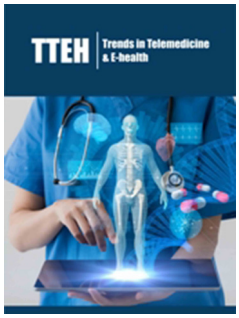
Crimson Publishers
Wings to the Research

Commentary

Ransomware: Taking Hospitals Hostage

ISSN: 2689-2707



***Corresponding author:** Jain Kanika, Assistant Professor, Department of Hospital Administration, All India Institute of Medical Sciences, Delhi, India

Submission: February 16, 2023
Published: June 02, 2023

Volume 4 - Issue 3

How to cite this article: Jain Kanika* and Mohindra Ritin. Ransomware: Taking Hospitals Hostage. Trends Telemed E-Health. 4(3). TTEH. 000586. 2023.
DOI: 10.31031/TTEH.2023.04.000586

Jain Kanika[1]* and Mohindra Ritin[2]

[1]Assistant Professor, Department of Hospital Administration, All India Institute of Medical Sciences, India

[2]Assistant Professor, Department of Emergency Medicine, All India Institute of Medical Sciences, India

Introduction

Ransomware refers to a type of malware used by attackers that first encrypts files and then the attackers attempt to extort money in return for the key to unlock the files by demanding a "ransom" [1]. Anonymity, irreversible nature of transactions, easy transfers made cryptocurrency the in-demand ransom [2]. Initially transmitted through emails, ransomware targeted individuals and/or Institutions. The emails may contain a link to an infected website or include an attachment such as a Word document that contains macros. Once a link is clicked or a document is opened, it downloads and infects the machine quickly [3-5]. Once infected, all the data in the infected system is encrypted and locked using a key, the key is provided only once the ransom demanded is paid [6]. Hospitals are organizations that never stop working and are always a hub of activity. Along with the healthcare boom, there is now an unprecedented dependance on technology in the execution of a number of its functions. From the time a patient decides to visit a healthcare provider or a hospital till the patient avails the services and even after that, imprints of technology can be seen everywhere. In the past decade, a number of incidents of ransomware have been reported from different healthcare organizations across the world. Ransomware attacks have crippled the victim organization because these days no data is preserved manually. The nature of the healthcare industry means that it relies on an extensive network of suppliers, vendors and partners for day-to-day operations [7].

What Makes Healthcare an Attractive Target

Healthcare facilities are an alternate target for attackers to visit for three reasons. First, a crippled system equals to lives lost. Secondly, healthcare has valuable data to steal. Thirdly, it is seen that healthcare has the weakest defenses built within their systems. The very fact that healthcare provides critical, lifesaving services makes it an attractive target because there is always an increased pressure to normalize the crippled system not only to ensure continuity of services but to also uphold the trust enjoyed by healthcare providers. It is because of this increased pressure and the fact that healthcare is a warehouse of the most sensitive and personal data that it is felt that healthcare organizations are more likely to pay ransom. More sensitive data equals easier sale of the same across the dark web or third parties for illegal reasons. At one end, healthcare organizations are the places where the most technical work is being executed on the human body. On the other end, healthcare organizations possess an extremely lackadaisical attitude in updating their IT systems. More often than not healthcare organizations are seen relying on legacy and end of life systems. It was reported by an Australian organization HIS in its Healthcare Cybersecurity report published in June 2018 that over 22 percent of healthcare organizations continue to use legacy and end-of-life systems without vendor support and a further 26 percent which are unaware of any support [8]. Low

investments in IT network security, poor cyber controls, absence of a Security Operations Centre (SOC), non-existent knowledge and competence in cyber security make healthcare organizations a lucrative target for attackers. It's predicted that a new organization will fall victim to ransomware every 11 seconds by the end of 2023, according to Cybersecurity Ventures [9].

Cost of Recovery from an Ransomware Attack

Ransomware costs to the global economy were estimated to be around 92 billion dollars in the year 2021-22 [10]. The average cost to an organization to rectify the impacts of recent ransomware attacks (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.) is over AU$900,000 [11]. Ransom demanded from healthcare organizations is found to range between $900 and $20 million. Ransomware attacks have the potential of causing widespread disruption in the target organization. The cost of disruption is estimated at $92 billion [10].

Recommended Measures to Protect Healthcare Organizations Against Ransomware Attacks

Healthcare have prioritized data security only after being attacked. It is imperative for organizations to secure their data right from the start. In order to avert cyber-attacks, healthcare organizations need to build a highly robust, adaptive and secure IT environment. Enumerated below are a few steps which the authors recommend.

Enforce IT hygiene

IT hygiene should be implemented and maintained across all IT and medical devices that are connected to the network. IT Hygiene can be achieved with real-time monitoring of all IT systems logged on to the network. Vulnerabilities can appear in different elements of the IT stack-in servers, the database, the network, the endpoints, etc. Software patches are to be applied to close those vulnerabilities [12].

This can be achieved with the following steps:

a) Adherence to Standard Operating procedures.

b) Use of only latest IT infrastructure and constant upgradation of the existing infrastructure.

c) High-risk systems should be hardened as per industry best practices.

d) Adoption of the Zero Trust model [12].

e) Network segmentation for separating mission-critical systems (such as life support systems) from other systems will help in preventing lateral spreading of malware or attacker access [12].

f) Reduction of the threat surface by provision of "least privileged access" [12].

g) Prevention of unauthorized access.

h) Use secure web gateways for remote access instead of traditional VPNs.

i) Implementation of automated systems for data identification and classification, data encryption, and data masking.

j) Use of DLP (Data Loss Prevention) systems for email, network, and endpoints for real-time loss monitoring [12].

k) Periodic network security reviews [12].

Secure by design

The IT system in the healthcare organization should be securely designed. All stakeholders in the organization should be considered a potential source and need to be made aware about the importance of cybersecurity. They need to be educated about security risks, it's impact and mitigation strategies. A security buy-in needs to be created in the organization. It is important to establish secure coding guidelines and embrace email security and dev-sec-ops for all development programs [12]. It is imperative for organizations to develop a Security operations centre, which will be the hub for continuous real-time monitoring and applying patches to all detected threats, identifying vulnerabilities and reducing surface threat pro-actively.

Managed detection and response

Healthcare organizations need to plan for early detection and prompt IT recovery to improve resilience in case of a breach. They should consider use of behaviour-based anomaly detection and sandboxing for those threats, which cannot be detected using signature-based systems [12].

References

1. Bridges L (2008) The changing face of malware. Network Security 2008(1): 17-20.
2. Angel JJ, McCabe D (2015) The ethics of payments: Paper, plastic, or bitcoin? Journal of Business Ethics 132(3): 603-611.
3. Fruhlinger J (2020) Ransomware explained: How it works and how to remove it. CSO Online.
4. Correa R (2008) How fast does ransomware encrypt files? Faster than you think. Barkly.
5. (2017) NFF ransomware: Understand the threat. Know the Risks. Protect the Enterprise. NFF: Delivering Net Results.
6. Mustaca S (2014) Are your IT professionals prepared for the challenges to come? Computer Fraud & Security 2014(3): 18-20.
7. Dimkin D, Aggarwal A, Jayasekere R, Narain J (2021) How cyber criminals are holding health to ransom. PwC, UK.
8. Cybersecurity across the final report of a National Survey.
9. Combat ransomware in healthcare brief. Pure Storage, USA.
10. Guru's (2022) Ransomware on healthcare organizations cost global economy $92 bn. IT Security Guru.
11. Reports and statistics. Cyber.gov.au.
12. Salvi V, Ananth V, Bari YD (2020) Being resilient: Overcoming healthcare's cybersecurity challenge. Infosys Knowledge Institute.