The State of Ransomware in Hospitals:
Current Threats and How Healthcare Facilities Can Defend Against Them

Dana Grotenstein
Tufts University
December 13, 2019

I. Abstract

The healthcare industry has long been a target for cyberattacks. Patient data is some of the most sensitive and valuable information stored on computers to date, which makes healthcare facilities prime victims for cyberattackers to extort these facilities for profit. In recent years, ransomware has become an extremely common threat. Ransomware is a type of malware that disables a device or system of devices through encryption. Cyberattackers disable hospital networks and demand money in exchange for releasing the devices from the malware. With lives on the line and time-sensitive issues to be addressed such as medication and lab work records, hospitals have particularly been hit hard by the intensification of the ransomware problem. Without a plan of backup and strong infrastructure in place, hospitals are forced to pay attackers the ransom or suffer the often larger financial burden of rebuilding their system from the ground up. Hospitals can mitigate the risk of ransomware attacks through preparedness, reducing the amount of online patient data, implementing early threat detection systems, and much more.

II. Introduction

Ransomware is one type of malware, or malicious software, that infects a computer system and encrypts data on the computer, rendering the system inaccessible, until a ransom is paid to the attacker. Ransomware is often spread through emails with malicious attachments or visiting a website that is infected[1]. With the emergence of bitcoin and online currency, cyber-attackers now have an anonymous avenue for obtaining huge sums of money in exchange for the (sometimes) safe return of data to hacked systems. This means that ransomware has only risen in prevalence over the past few year. And, hackers have discovered that there is nobody better to demand money from than from organizations where data is sensitive and time is of the essence. This includes government systems, law enforcement systems, other critical infrastructure systems, and, of course, hospitals[1]. Hospitals are a prime target for ransomware attacks because they are often behind the curve in the security of their systems and store extremely valuable information electronically[2]. Downtime in a hospital can be a difference between life and death, meaning that healthcare organizations are more likely to pay off a ransom in exchange for the fast and safe return of patient data. With ransomware attacks on the rise, hospitals must raise their defenses. A major shift in the culture of security in the healthcare sector is required, and national standards of security in healthcare facilities must be set.

III. To the Community

The rise of ransomware in hospitals is a life or death concern, and there is data now to prove it. According to a recent study from Vanderbilt University examining the effect of data breaches in hospitals on mortality rates, "on average, a data breach at a nonfederal acute-care inpatient hospital was associated with an additional 23-36 deaths per 10,000 [acute event] discharges per year", where acute events relate to events requiring immediate action, such as cardiac arrest[3]. Other instances have been reported of nurses distributing medication with serious side effects to patients that should have been discontinued hours earlier because the lab results were delayed[2]. In an after-the-fact analysis of the 2017 WannaCry ransomware attack, the United Kingdom found that approximately 19,000 appointments nationwide, including operations, were cancelled due to disrupted function[4]. Mortality rates for the U.K. WannaCry outbreak have yet to be reported[4]. In the current state, the future is bleak. In the past 6 months, 40% of healthcare organizations have fallen victim to WannaCry, just one of many ransomware strains out there[5]. The number of ransomware attacks increased by 350% in 2017 and will likely continue to grow[6]. We must take action now. Lives are at stake.

IV. Background

Why hospitals?

Hospitals and healthcare organizations are a prime target for ransomware attacks for many reasons. First, hospitals are often technologically behind other industries. When systems need to be up and running at all times, it is difficult to commit time and money to update technology on devices. Thus hospital systems carry on operating on their current technology with system vulnerabilities wide open for hackers to exploit. Second, the healthcare industry as a whole has very rapidly moved to adopting the use of electronic health records (EHRs) in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Although HIPAA was passed as an attempt to increase security and privacy for patients, support from the government mandating these compliances have not provided smaller hospitals and healthcare organizations with enough continued assistance to maintain secure systems in the digital age[2]. Many smaller healthcare organizations do not see system security as an essential part of medical care and instead consider it to be a mandate forced on them by the government, and thus do not prioritize security technologies in their allocation of resources, making them particularly

susceptible to breaches[7]. Thirdly, hospitals are a prime target for ransomware attacks specifically because of the importance of patient data to function. Without access to all of the online records required to treat a patient, hospitals cannot function properly. Thus, hospitals are the most likely to give in to paying off a ransom. All of these factors together make hospitals a perfect ecosystem for a ransomware attack, and attackers know that.

How does crypto ransomware work?

Crypto ransomware, the type of malware that encrypts files and most commonly used to attack hospitals, is usually spread through phishing emails with malicious attachments or what is called drive-by downloading. Drive-by downloading is the term used for when someone visits an infected website and unknowingly, malware is downloaded and installed on their computer[8]. Newer include social media hooks such as online messaging applications which allow attackers to gain access to an organizations entire network. Once the malware gains access to a system, it will run an encryption algorithm to render files on the system unreadable. The only way to regain access to files is to pay a ransom based on instructions provided by the attacker, and then the attacker *may* send the private key necessary to decrypt the files[9]. This tactic has been very successful over the past decade, and the following examples are only some of the many strains of ransomware that have wreaked havoc to healthcare facilities in recent years.

Locky Ransomware

Locky, one strain of crypto ransomware, takes advantage of email attachments containing Microsoft Office documents with dangerous macros containing malicious Visual Basic Script code. Using social engineering, attackers trick users into enabling the running of these Microsoft macros, which automatically then run the Visual Basic Script upon opening the Word or Excel document[10]. The Visual Basic Script with download and run the Locky malware binary, which has the capability to encrypt over 160 different kinds of files such as source code, databases, and virtual disks[10]. Files are encrypted using RSA-2048 and AES-128 ciphers and renamed with .locky file extensions. Locky also adds instructions for recovering data in every directory with encrypted files, and often will set desktop wallpaper to be the instructions as well. The Locky ransom can only be paid through BitCoin[10].

Locky successfully brought down two U.S. hospitals in 2016. Hollywood Presbyterian Medical Center in Los Angeles, California was attacked through what was likely an email phishing scam with malicious Microsoft Word Documents as mentioned above. On February 5th, 2016, members of the hospital staff began noticing that they were unable to access the network. Doctors were unable to access patient medical histories, nor could they share medical tests. Some departments could not even turn on their computers[11]. The hospital was in a state of crisis for 10 days, when they decided to pay off their ransom of 40 Bitcoin, approximately $17,000. Just weeks later, Methodist Hospital in Henderson, Kentucky was hit with Locky, preventing hospital staff from accessing any patient files[12]. Luckily for them, Methodist Hospital was able to recover all of the hospital's data from file backups and did not need to pay the ransomware[12]. According to MalwareBytes, Locky has since been put out of commission but has been one of the most significant strains of ransomware to date[13].

In the news now: Ryuk Ransomware

Ransomware wasn't just an issue of 2016. On November 18th of this year, a ransomware attack on a technology services provider called Virtual Care Provider (VCPI) has resulted in the disruption of about 110 nursing homes and acute care facilities[14]. The attackers are demanding $14 million worth of bitcoin in order to decrypt patient records. Until then, patient records are on hold. Some nursing homes, with inability to submit billing document to Medicaid, will have to close their doors[14].

Ryuk is a ransomware strain used to attack large organizations and systems, often demanding large sums of money in return. Ryuk, introduced to a system through phishing or other covert methods like drive-by downloads, can lurk on a system for months before actually encrypting a system. Ryuk usually piggybacks onto systems through other malware, such as TrickBot and Emotet, which are malware strains that often result from phishing scams claiming to be a banking site[15]. These Trojans can then run tasks such as propogating through a network and installing other malware, which is where Ryuk gets introduced and gains access to entire networks at a time[16, 17]. At this point, VCPI has yet to resolve this situation, leaving thousands of patients across the United States at risk.

V. What can we do?

Precautionary Measures

Ransomware in the healthcare industry is a serious problem. To make matters worse, unless a hospital already has backups of electronic health records in place before an attack occurs, there is not much one can do once a system gets encrypted. There are, however, plenty of steps that can and should be taken by organizations to prevent ransomware attacks in the future.

Hospitals should be backing up systems and data regularly, and ensuring that backups are being stored off-site as many attacks can access on-site backup storage such as Volume Shadow Copies and other on-device snapshots[18]. Organizations should assess how necessary it is to have Server Message Block ports and Remote Desktop Protocol ports open, which allow for easy file sharing to and from potentially malicious third parties. If this is necessary, steps should be taken to make sure connections are only allowed for verified and trusted hosts[18]. Filters should be implemented to filter emails that are evidently phishing emails and block emails from these suspicious sites in the future[18]. Most importantly, however, is to enforce continued education among all staff. Barring ransomware that attacks known software vulnerabilities, the largest contributor to ransomware attacks is ignorance.

A Massive Shift is Needed

Although defense mechanisms and taking precautionary measures is certainly a step in the right direction, ransomware tactics are getting smarter every day and there will always be new vulnerabilities to take advantage of. The situation at hand calls for a fundamental change in the culture around security in the healthcare community. HIPAA at this point is antiquated. HIPAA was passed with the intention of preventing healthcare providers from disclosing patient information without their consent, but the danger of infiltration from third parties was never considered[2]. With EHRs being stolen and encrypted all over the country, government regulations must be put in place to address threats from outside attackers. Lawmakers should be working towards aggressive legislation to enforce best practices. Hospitals cannot and likely will not implement high-security measures without pressure. High standards of backups, firewalls, endpoint detection, and other precautions must be put in place.

VI. Conclusion

Ransomware incidents in the healthcare space continue to rise, and now we have proof that it is impacting human lives. With so much valuable data and not enough security to protect it, the healthcare industry is a prime target for ransomware attacks. There are many defenses that can be taken, but at the end of the day, a great cultural shift is needed. Not nearly enough attention is being paid to malware in an age where it growing more detrimental by the day. Healthcare is only one industry being impacting by this issue, but this is a global problem that needs immediate attention. We need to start raising our defenses, or attackers will continue on their path of havoc.

VII. Supporting Material

Accompanying this paper is a presentation summarizing the content for an audience of healthcare and government officials

References:

1. "Ransomware." *CISA*, https://www.us-cert.gov/Ransomware.
2. Deborah R. Farringer, *Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals*, 40 SEATTLE U. L. REV. 937 (2017).
3. Choi, Sung J., et al. "Data Breach Remediation Efforts and Their Implications for Hospital Quality." *Wiley Online Library*, John Wiley & Sons, Ltd (10.1111), 10 Sept. 2019, https://onlinelibrary.wiley.com/doi/pdf/10.1111/1475-6773.13203.
4. "Krebs on Security." *Brian Krebs*, https://krebsonsecurity.com/2019/11/study-ransomware-data-breaches-at-hospitals-tied-to-uptick-in-fatal-heart-attacks/.
5. Landi, Heather. "Report: 40% of Healthcare Organizations Hit by WannaCry in Past 6 Months." *FierceHealthcare*, 29 May 2019, https://www.fiercehealthcare.com/tech/lingering-impacts-from-wannacry-40-healthcare-organizations-suffered-from-attack-past-6-months.
6. "The Evolution of Ransomware: 2019 Brings the 30 Year Anniversary." *Kraft Business Systems*, 7 Jan. 2019, https://kraftbusiness.com/cyber-security/evolution-of-ransomware-2019-brings-30-year-anniversary/.
7. "A Health Hack Wake-Up Call." *U.S. News & World Report*, U.S. News & World Report, https://www.usnews.com/opinion/blogs/policy-dose/articles/2016-04-01/ransomware-hacks-are-a-hospital-health-it-wake-up-call.
8. "What Is Ransomware?" *Information Security Office*, https://security.berkeley.edu/faq/ransomware/.
9. Ubaid. "Ransomware - A CryptoViral Extortion Attack." *TO THE NEW BLOG*, https://www.tothenew.com/blog/ransomware-a-cryptoviral-extortion-attack/#.
10. "A Closer Look at the Locky Ransomware." *Avast Blog*, https://blog.avast.com/a-closer-look-at-the-locky-ransomware.
11. "Ransomware Case Studies: Hollywood Presbyterian and The Ottawa Hospital." *Infosec Resources*, https://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-attack-statistics-and-case-studies/ransomware-case-studies-hollywood-presbyterian-and-the-ottawa-hospital/#gref.
12. Zetter, Kim. "Why Hospitals Are the Perfect Targets for Ransomware." *Wired*, Conde Nast, 3 June 2017, https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/.
13. "Ransom.Locky." *Malwarebytes Labs*, https://blog.malwarebytes.com/detections/ransom-locky/.
14. Davis, Jessica. "Ransomware Attack on IT Vendor Disrupts Care at 110 Nursing Homes." *HealthITSecurity*, HealthITSecurity, 25 Nov. 2019, https://healthitsecurity.com/news/ransomware-attack-on-it-vendor-disrupts-care-at-110-nursing-homes.
15. "What You Should Know about Ryuk Ransomware." *Infosec Resources*, 23 Sept. 2019, https://resources.infosecinstitute.com/what-you-should-know-about-ryuk-ransomware/#gref.
16. "Emotet Malware – An Introduction to the Banking Trojan." *Malwarebytes*, https://www.malwarebytes.com/emotet/.
17. "Trojan.TrickBot." *Malwarebytes Labs*, https://blog.malwarebytes.com/detections/trojan-trickbot/.
18. "MS-ISAC Security Primer - Ransomware." *CIS*, https://www.cisecurity.org/white-papers/security-primer-ransomware/.