Michael Seleman
COMP 116 - Final Project
05/07/2018

Ransomware Ravages Healthcare: Cryptoviral Extortion in the Healthcare Sector

Abstract:

The past decade has ushered in countless high-impact technological upgrades in the healthcare industry, the most prominent of which being the digitalization of patient health records. Since its passing in 1996, the Health Insurance Portability and Accountability Act (HIPAA) has mandated the rigorous safekeeping of patient information by healthcare organizations across the United States. [1] Yet, despite HIPAA's efforts to establish exhaustive security provisions, the introduction of electronic health records (EHRs), as well as the subsequent storage of such records in the cloud, has created new vulnerabilities in the protection of patient data that neither industry professionals nor HIPAA regulators were prepared to defend against. Among the most pertinent of these vulnerabilities was exposed in 2016, when cyber criminals demanded $3.6 million from the Hollywood Presbyterian Medical Center in exchange for the return of hospital files that the criminals had seized.[2] Popularly referred to as "ransomware", the malware used to execute this attack has ravaged the healthcare industry in recent years, as cyber criminals have identified hospitals as particularly sensitive to attacks compromising the immediate accessibility of EHRs.[3] In this paper, we will discuss the healthcare industry's particular susceptibility to ransomware attacks, and propose viable defense mechanisms against such attacks.

Introduction:

Healthcare Takes a Hit:

In 2016, the healthcare industry found itself face to face with the blunt end of what now appears to be a worldwide ransomware epidemic. Unsuspecting hospitals and clinics, such as Hollywood Presbyterian Medical Center (HPMC), found themselves under a global spotlight, being the first high profile victims of this hard hitting cyber attack in the industry, or at least the first to publicly disclose the event.[2] With rumors lurking that HPMC had been successfully extorted for roughly $3.6 million, ransomware was dubbed a legitimate threat to the industry.[2]

Yet in a matter of months, similar attacks would claim several other unsuspecting victims, taking down 10 hospitals and 250 outpatient centers in Washington D.C. with the attack of MedStar health, and another 16 hospitals across the United Kingdom at the hands of the renowned WannaCry attacks.[4,5] In doing so, these attacks, while endangering millions of lives and compromising the confidentiality of terabytes of patient information, brought to light the healthcare industry's particular susceptibility to ransomware and a need for the prompt reform of healthcare information security.

What is Ransomware?:

Ransomware is a type of malware that denies a victim access to any/all files stored on an infected system. Although ransomware comes in many different sizes, most instances of the malicious software have been found to deny access to data by encrypting all files on a given host machine.[6,7] Desperate to retrieve precious documents, presentations, etc., victims are then given an opportunity to regain access to encrypted files for a ransom, most often demanded in bitcoin to preserve the anonymity of the attackers.

Not unlike most other forms of malware, ransomware has several different methods by which it can infect a host, and propagate thereafter. Among the most common of these methods is known as "drive-by-download", during which web traffic to a given site is redirected to another site hosting an exploit kit.[6] Victims of this method of infection are often redirected from untrusted, adult content-related websites, naively exposing themselves to these malicious exploit kits, that will then attempt to download/install the ransomware. Arguably an even more rampant form of infection features the use of spam email. Aided by surprisingly effective social engineering tactics, spam email has been known to be a major source of infection, as recipients are often tricked into downloading malicious attachments containing the ransomware.[8]

Once installed on a victim's machine, crypto ransomware will make use of either symmetric or asymmetric encryption to complete its undertaking. More often than not, ransomware will employ symmetric encryption techniques, generating a new public key on each machine it infects.[6,8] This key is then used to encrypt all data on the host machine, and is then sent back to the attacker, only to be returned to the victim for a ransom. Robust ransomware likely favors such symmetric encryption techniques for the speed of symmetric algorithms relative asymmetric ones, an important consideration for attackers hoping to seize control of all files before a victim realizes that their machine has been compromised. The use of symmetric

encryption does however require the attacker to adequately hide their encryption key on the host machine, lest the victim get a hold of it.

An Inside Look at WannaCry:

Although not limited in impact to this particular industry, the WannaCry ransomware was among the first to make a name for itself in the healthcare industry. As mentioned above, the ransomware was particularly devastating to the UK's healthcare infrastructure, resulting in the abrupt shutdown of hospitals/clinics across the nation.[9] Since these happenings, WannaCry has become a trademark example of this brand of malware, shedding great insight into the inner workings of the classic ransomware attack.

The attack targets machines running an unpatched version of the Windows operating system, specifically those without the MS17-010 patch, which was ironically released just a few months prior to the 2017 WannaCry attacks.[10] Vulnerable versions of the operating system included Windows 7, Windows Server 2008, and Windows 10 among several others. Interestingly enough, the exploit employed by the WannaCry attacks was not an original, but rather an exploit rumored to have been developed by the National Security Agency (NSA).[11] Commonly referred to by the name "EternalBlue", the exploit takes advantage of a flaw in the Windows' server message block (SMB) protocol, allowing attackers to send malicious packets to the SMB server and gain remote access to the targeted machines.[12] The exploit since been documented thoroughly (CVE-2017-0143), but is still used to wreak havoc on unpatched versions of Windows worldwide.[11,12] Please see the attached supplementary material for an interactive demo of the EternalBlue exploit, used to gain remote access to a vulnerable Windows VM (Metasploitable3).

To The Community:

With ransomware attacks on the rise, the healthcare industry is particularly vulnerable. Harboring billions of electronic health records (EHRs), the industry is positioned among both the most enticing and the easiest of targets. There are two primary reasons for the industry's particularly vulnerable position: (1) the sensitivity of the data collected and stored by the industry, and (2) the fact that medical personnel require constant access to this data to administer adequate care. With respect to the former of these points, healthcare data is most often compromised in the form of stolen electronic health records, which contain an abundance of

HIPAA protected personal information.[3,13] This in mind, the sensitivity of this kind of data ensures attackers that healthcare organizations will be willing to go to great lengths to retrieve any stolen records, and are therefore less likely to rule out paying the demanded ransom amount. Arguably paramount to sensitivity of the stolen data is a healthcare organization's inability to access the stolen data. Compromising the accessibility of patient files renders hospital personnel unable to provide the highest quality of care to their patients, therefore compromising patient safety.[14] With lives at stake, a hospital is least likely, relative to other target organizations, to delay in paying the requested ransom if an alternate solution is not immediately apparent.

Furthermore, as touched upon by Kevin Sacco at DEF CON 25, the healthcare industry is also uniquely susceptible to social engineering tactics, allowing for easy infection.[15] Such tactics generally feature the impersonation of healthcare personnel requiring account information for an urgent matter (which could mean life or death in a hospital setting). Sacco found that recipients of these artificial communications (who tend to be IT professionals) are much more likely to comply with the senders' requests and unsuspectingly provide attackers with passwords and/or other sensitive credentials.[15]

To make matters worse, healthcare is popularly perceived as the least "tech savvy" of the world's largest industries, lagging behind in its adoption of the latest information security provisions. In fact, the Healthcare Information and Management Systems Society reported in 2016 that only 31% of healthcare organizations regularly encrypt EHRs, and that 20% do not encrypt any data.[16] If such trends continue unaddressed, the impact of ransomware attacks alone could prove catastrophic to the healthcare industry on a global scale.

Defense Mechanisms:

As in any industry, the response to cyber crime begins with a long list of potential defense mechanisms, most of which are intended to mitigate risk. In this context, such mechanisms include frequent audits of systems/infrastructure and the training of employees to spot and avoid common forms of infection.[17]

While these defenses are undoubtedly worthwhile, I advocate for a more robust defense mechanism, one that requires an organization to address its two most glaring weaknesses, mentioned above and restated as follows: (1) the sensitivity of HIPAA protected patient information stolen in the form of EHRs, and (2) the inability of medical professionals to provide the highest quality care without access to patient's medical history.

Staggered Storage:

Addressing the latter of these two issues is as simple as storing regularly updated, offline backups of all EHRs and other crucial information required for a given organization's day-to-day operations. In settings where frequent hospital-wide updates to an offline backup are not feasible, I suggest a staggered approach: daily backups of all recently modified documentation, coupled with more comprehensive monthly backups.[18,19] Daily backups ensure a healthcare organization that the most pertinent data to an organization's day-to-day operations is always accessible. Conversely, monthly backups reduce the risk of extensive data loss in the event of a breach.

By implementing this or another comparable backup protocol, healthcare organizations will not only be well prepared to defend against ransomware attacks, but will also have made themselves much less appealing targets to attackers, who can no longer count on a hasty payment from an organization looking to restore its ability to provide adequate patient care.

Data Encryption:

While having a comprehensive backup of all stolen data is a giant step in the right direction, it does not change the fact that sensitive patient information has been compromised in the event of an attack. According to HIPAA, the encryption of protected healthcare information falls within the category of a data breach, simply because the attacker has control of the information, and can view or distribute it if they so choose.[1,20] Herein lies the need for a second component of defense. Ironically, the most effective and most feasible solution for this issue features a technique used by the ransomware itself: data encryption. Encrypting all patient data, such that it can be viewed only by individuals given a key, makes this data invisible to cyber criminals, even in the event of an attack.[21] In fact, the theft of records that are sufficiently encrypted according to standards established by the U.S. Department of Health and Human Services is not considered a breach, as the records are considered "indecipherable to unauthorized personnel".[1,20] Thus, paired with a staggered backup protocol, the encryption of all sensitive patient data promises to be an effective method of defense against ransomware infections.

Conclusion:

As more ransomware-related incidents begin to surface in the healthcare sector, it is increasingly likely that future ransomware attacks will only grow stronger, and that the ransoms demanded will rise correspondingly. That said, the healthcare industry is quite unfortunately

positioned, having so much at stake with the sensitivity HIPAA protected information and the reliance of healthcare personnel on accurate and update EHRs. To date, the industry as a whole has been slow to adopt information security provisions. Yet, with several organizations reeling from the crippling ransomware attacks of 2016/17, the need for robust security provisions is quite evident. Fortunately, as outlined above, an adequate defense against ransomware requires a simple two-part approach, featuring frequent, offline backups to maintain availability of patient data, as well as the regular encryption of patient data to maintain its confidentiality. This approach provides healthcare organizations with a proper defense not only against ransomware, but also against any other cyber threats specifically targeting the confidentiality, integrity, or availability of patient information. Only time will tell, however, if these or similar provisions will be adopted in time to prevent the industry from falling victim to yet another catastrophic ransomware attack.

Supplementary Material

My supplementary material is a live demo of the EternalBlue DoubePulsar exploit used to attack a vulnerable Windows Server 2008 machine (Metasploitable 3). The live demo is too large to upload to Trunk, so I have uploaded it to YouTube. It can be accessed at https://youtu.be/M0WuC_VyIvM. References for this demo are also shown below.

References

1. FACT SHEET: Ransomware and HIPAA. :8.
2. Ragan S. Ransomware takes Hollywood hospital offline, $3.6M demanded by attackers. CSO Online. https://www.csoonline.com/article/3033160/security/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.html. Published February 14, 2016. Accessed May 7, 2018.
3. HealthITSecurity. How Ransomware Affects Hospital Data Security. HealthITSecurity. https://healthitsecurity.com/features/how-ransomware-affects-hospital-data-security. Published June 3, 2016. Accessed April 2, 2018.
4. Washington's MedStar Health shuts down computers after virus. *Reuters*. https://www.reuters.com/article/us-usa-cyber-medstar/washingtons-medstar-health-shuts-down-network-after-computer-virus-idUSKCN0WU1O9. Published March 28, 2016. Accessed May 7, 2018.

5. Do You WannaCry? A Taste of SMB Exploitation. Dionach. https://www.dionach.com/blog/do-you-wannacry-a-taste-of-smb-exploitation. Published September 8, 2017. Accessed May 7, 2018.

6. Savage K, Coogan P, Lau H. The evolution of ransomware. :57.

7. Ransomware - A CryptoViral Extortion Attack. *TO THE NEW BLOG*. http://www.tothenew.com/blog/ransomware-a-cryptoviral-extortion-attack/. Accessed May 7, 2018.

8. Young A. *Abstract Cryptovirology: Extortion-Based Security Threats and Countermeasures*.

9. Brandom R. UK hospitals hit with massive ransomware attack. The Verge. https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin. Published May 12, 2017. Accessed April 2, 2018.

10. CVE-2017-0143 MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption | Rapid7. https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue. Accessed May 7, 2018.

11. Burgess M. Everything you need to know about EternalBlue – the NSA exploit linked to Petya. WIRED UK. http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch. Accessed May 7, 2018.

12. CVE-2017-0143 : The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows. https://www.cvedetails.com/cve/cve-2017-0143. Accessed May 7, 2018.

13. Ransomware attack exposes data of nearly 18,000 Metropolitan Urology patients. Healthcare IT News. http://www.healthcareitnews.com/news/ransomware-attack-exposes-data-nearly-18000-metropolitan-urology-patients. Published March 20, 2017. Accessed May 7, 2018.

14. Hospital Declares 'Internal State of Emergency' After Ransomware Infection — Krebs on Security. https://krebsonsecurity.com/2016/03/hospital-declares-internet-state-of-emergency-after-ransomware-infection/. Accessed May 7, 2018.

15. DEFCONConference. *DEF CON 25 BioHacking Village - Kevin Sacco - Tales of A Healthcare Hacker*. https://www.youtube.com/watch?v=ij7uuY-3eXk. Accessed May 7, 2018.

16. Hacking health care: Inside scoop to the most vulnerable vertical. http://www.healthcarebusinesstech.com/healthcare-vulnerable-hacking/. Accessed May 8, 2018.

17. 4 ways hospitals can prevent a ransomware attack | FierceHealthcare. /privacy-security/4-simple-ways-hospitals-can-prevent-a-ransomware-attack. Accessed April 2, 2018.

18. Korolov M. Will your backups protect you against ransomware? CSO Online. https://www.csoonline.com/article/3075385/backup-recovery/will-your-backups-protect-you-against-ransomware.html. Published May 31, 2016. Accessed May 7, 2018.

19. How Has Information Security Changed in Healthcare? *CynergisTek, Inc*. October 2017. https://cynergistek.com/information-security-changed-healthcare/. Accessed May 7, 2018.

20. HHS: Ransomware Infections are (Probably) Reportable Under HIPAA. Digital Guardian. https://digitalguardian.com/blog/hhs-ransomware-infections-are-probably-reportable-under-hipaa. Published July 14, 2016. Accessed May 7, 2018.

21. Why healthcare organizations should encrypt everything. https://www.beckershospitalreview.com/healthcare-information-technology/why-healthcare-organizations-should-encrypt-everything.html. Accessed May 7, 2018.

References (Supplementary Material)

1. Burgess M. Everything you need to know about EternalBlue – the NSA exploit linked to Petya. WIRED UK. http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch. Accessed May 7, 2018.

2. S G. Exploit Windows with EternalBlue & DoublePulsar through Metasploit. *GBHackers On Security*. March 2018. https://gbhackers.com/windows-eternalblue-doublepulsar/. Accessed April 2, 2018.

3. Introducing the Metasploit Vulnerable Service Emulator. Rapid7 Blog. https://blog.rapid7.com/2017/03/02/vulnerable-service-emulator/. Published March 2, 2017. Accessed May 7, 2018.

4. webpwnized. *Introduction to Using Metasploit Modules*. https://www.youtube.com/watch?v=7gQP82lzsPc&index=6&list=PLZOToVAK85MpnjpcVtNMwmCxMZRFaY6mT. Accessed May 7, 2018.

5. *Metasploitable3: Metasploitable3 Is a VM That Is Built from the Ground up with a Large Amount of Security Vulnerabilities*. Rapid7; 2018. https://github.com/rapid7/metasploitable3. Accessed May 7, 2018.

6. Coter S. Oracle VM VirtualBox: Networking options and how-to manage them. https://blogs.oracle.com/scoter/networking-in-virtualbox-v2. Accessed May 7, 2018.

7. Dieterle AD. Using the "NSA" EternalBlue exploit on Metasploitable 3. *CYBER ARMS - Computer Security*. June 2017. https://cyberarms.wordpress.com/2017/06/12/using-the-nsa-eternalblue-exploit-on-metasploitable-3/. Accessed May 7, 2018.