The Impact of Malware on Healthcare Organizations and Patient Outcomes.

Thomas Juricek

Lewis University

Dr. Roncero-Bellido

4/20/2023

Abstract

The healthcare industry has become increasingly reliant on technology, leading to improved patient care and outcomes. However, this reliance has also made healthcare organizations vulnerable to cyber-attacks, including malware attacks. This research paper explores the impact of malware attacks on healthcare organizations and patient outcomes. The paper provides an overview of the types of malwares commonly used in attacks and the reasons why healthcare is a prime target for cyber criminals. Additionally, the paper discusses the various ways in which malware attacks can disrupt healthcare services, lead to loss of sensitive patient data, and negatively affect patient outcomes. The paper analyzes case studies of malware attacks on healthcare organizations, including the WannaCry and NotPetya ransomware attacks, and examines how healthcare organizations responded to these attacks. The paper concludes by discussing the importance of cybersecurity in healthcare and the need for healthcare organizations to develop comprehensive cybersecurity strategies to protect against malware attacks.

Keywords: cybersecurity, malware, healthcare, technology, ransomware

Introduction

As technology usage increases in society, so does the complexity of malicious code, or "malware". Malware is any code or program that has malicious intent, such as taking your money from your bank account, or damaging your computer. Malware comes in many different forms, such as viruses, worms, and ransomware. A virus attaches itself to a legitimate program or file and infects other files on the system when the infected program is run. Viruses are designed to replicate and spread to other computers. Once a virus infects a computer, it can cause damage by deleting files, corrupting data, and even stealing personal information. A computer worm is a self-replicating type of malware that spreads through a network, exploiting vulnerabilities in computer systems to infect other computers. Worms can cause significant damage by consuming bandwidth, slowing down computer systems, and spreading other types of malwares. Ransomware encrypts the victim's files, rendering them inaccessible, and demands a ransom payment in exchange for the decryption key to restore access to the files. Ransomware is typically spread through phishing emails, malicious websites, or vulnerabilities in computer systems. Ransomware will display a message on the victim's screen, often with a countdown timer, and demand payment in exchange for the decryption key. In many cases, the payment must be made in cryptocurrency to avoid detection by law enforcement.

With healthcare becoming more digitalized, it brings many benefits, such as improved efficiency with patient records, reduce costs associated with administrative tasks, such as paperwork and manual data entry, and enhanced patient outcomes due to helping providers make faster and more accurate diagnoses. Additionally, telemedicine can improve access to care for patients in remote or underserved areas, allowing them to receive care without having to travel long distances. The digitalization of healthcare has unfortunately opened the door to cyberattacks. Attacks have grown in frequency and complexity within the past few years, due to holding sensitive data, limited resources for cybersecurity, complex networks with endpoints including medical devices, computers, and mobile devices, and lots of opportunities for human error. Malware attacks pose a significant threat to healthcare organizations through compromising patient privacy, disrupting healthcare services, and negatively impacting patient outcomes. How do healthcare organizations and expert approach management of ransomware attacks, and what are the most effective strategies? How does malware affect the quality of care provided by healthcare organizations? How can healthcare systems prepare and respond to these attacks? This paper examines the impact of malware on healthcare organizations and patient outcomes and discusses the importance of implementing effective cybersecurity measures to prevent and mitigate the effects of malware attacks.

Background

The history of malware attacks on healthcare organizations can be traced back to the early 2000s. One of the most sudden known attacks occurred in 2003, when the SQL Slammer worm infected several healthcare organizations, causing widespread disruption to computer networks. In the years that followed, healthcare organizations continued to be targeted by malware attacks. In 2007, a Trojan horse virus known as "Storm" infected several healthcare organizations, causing significant damage and resulting in the theft of sensitive patient data. In 2010, the Stuxnet worm was discovered, specifically designed to target industrial control systems, including those used in healthcare facilities. In recent years, there has been a significant increase in malware attacks targeting healthcare organizations. In 2017, the WannaCry ransomware attack infected computer systems at numerous hospitals and healthcare facilities worldwide, causing widespread disruption to healthcare services. The COVID-19 pandemic has also created new opportunities for cybercriminals to target healthcare organizations, shown by the way Menaka Muthuppalaniappan (2020) stresses it in her article, “In April 2020, the International Criminal Police Organization (INTERPOL) published a report cautioning a global increase in the prevalence of cyber-attacks relating to the Coronavirus Disease 2019 (COVID-19) pandemic” (1). In 2020, numerous reports of cyber-attacks on healthcare organizations involved in COVID-19 research and vaccine development occurred. In response to the increase in COVID-19 related cyber-attacks, organizations worldwide have been increasing their cybersecurity measures, including implementing stronger authentication protocols, conducting regular vulnerability assessments, and providing cybersecurity training to their employees. However, despite these efforts, the threat of cyber-attacks remains a persistent challenge, requiring continued vigilance and adaptation to evolving threats.

Analysis of Case Studies

It is essential to look at cyberattack studies to learn how they started, how they were handled, and what issues they caused. In May 2017, the WannaCry ransomware attack infected computer systems at numerous hospitals and healthcare facilities worldwide, including the UK's National Health Service (NHS). The attack caused widespread disruption to healthcare services, with some hospitals forced to cancel surgeries and appointments. The episode also resulted in the theft of sensitive patient data, including medical records and personal information. The lack of proper updating of medical systems and servers heavily influenced this attack. Jessica Davis (2019) from the HealthITSecurity journal, tries to understand why WannaCry was so successful, “It is not a coincidence that these sectors are also the ones affected the most by ransomware like

WannaCry, which rely on unpatched devices for their successful operation" (pg. 11). Hospitals and healthcare organizations took several measures in the United States to protect themselves from the WannaCry attack. Many organizations updated their systems with the relevant patches and software updates, while others disconnected their systems from the internet altogether. Some hospitals also canceled non-emergency procedures and appointments to free up resources to deal with any potential impact of the attack. Hospitals and healthcare organizations in other countries also took steps to protect themselves from the WannaCry attack. In Spain, for example, the government declared a state of emergency and urged hospitals to take precautionary measures. In Japan, hospitals were advised to disconnect their systems from the internet and use pen and paper to record patient data.

Figure 1.1: WannaCry Attack Logistics. (NPJ Digital Medicine, 2019)

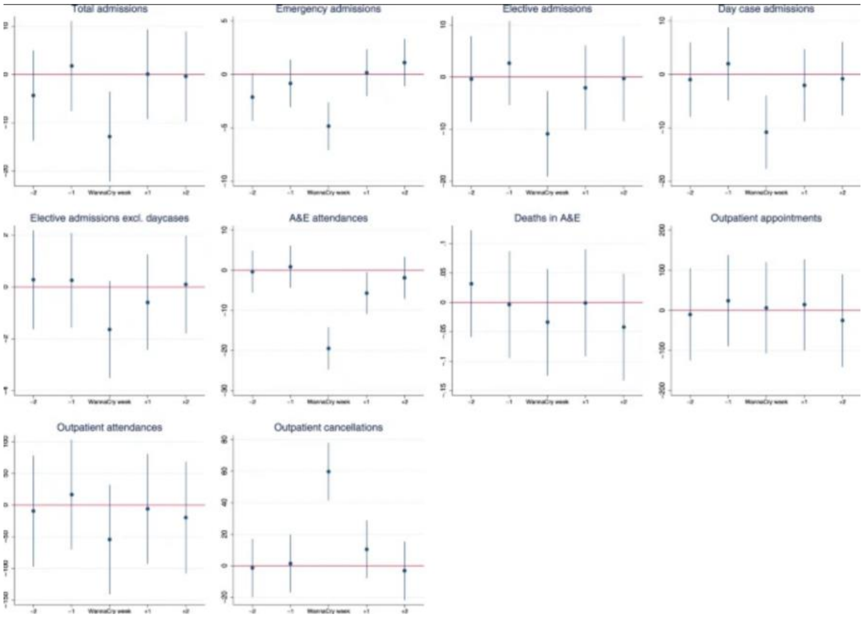
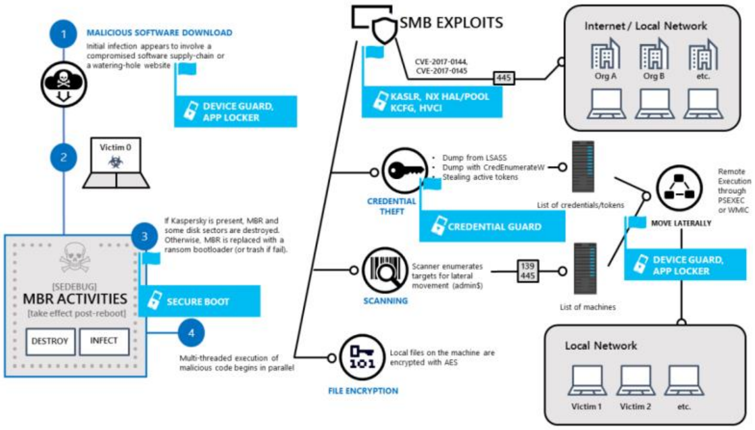


Figure 1.1 is a combination of several statistics from hospitals affected by WannaCry. During the WannaCry infection, there were notable differences in activity levels at infected institutions that were statistically and clinically significant. This also significantly affects outpatient services, as Ghafur (2019) explains, "During the WannaCry week, infected trusts had

on average 50% more cancellations than non-infected trusts per day (59.7 cancellations, 95% confidence interval 41.4 to 78.0). This resulted in 55 fewer outpatient attendances per day at infected trusts" (8). Of course, the full extent of damages or impact on patient care is hard to calculate due to how widespread and how each patient case varies. However, Ghafur shows that in the case of WannaCry, there was no difference in the number of deaths when comparing an infected trust and a non-infected trust, "Across all trusts, compared to the baseline week, there was no significant difference in the number of deaths in A&E. There was also no significant difference in deaths in A&E between infected and non-infected trust (0 deaths (−0.1 to 0.1)" (2019, para. 9).

Though there are no deaths in most cases, there have been instances where deaths can be traced back to cyberattacks. Ralston (2020) explains the story of a 78-year-old woman who suffered from an aortic aneurysm and could not be transported to the nearest hospital due to an emergency closure. The situation started off as a regular transportation of a patient, but things went awry when the ambulance crew contacted the nearby university hospital to notify them of their arrival. They were informed that the hospital's emergency department was not operational, and hence, the patient couldn't be admitted there. The crew was then instructed to go to Helios University Hospital, which was located 32 kilometers away, resulting in a delay of one hour before the patient could receive medical attention. Unfortunately, the patient passed away shortly after this delay (para. 1). The local university hospital was experiencing a ransomware attack, which compromised the digital infrastructure of the hospital. Ralston explains that stopping new admissions was vital to protect those inside. The hackers realized that they had infected a hospital and had even presented the encryption key to the authorities when they learned, but it was too late.

Figure 1.2: NotPetya Attack Phases (Microsoft Defender ATP Research Team, 2017)


1
MALICIOUS SOFTWARE DOWNLOAD
Initial infection appears to involve a compromised software supply-chain or a watering-hole website
DEVICE GUARD, APP LOCKER
2
Victim 0
3
If Kaspersky is present, MBR and some disk sectors are destroyed. Otherwise, MBR is replaced with a ransom bootloader (or trash if fail).
[SEDEBUG]
MBR ACTIVITIES
[take effect post-reboot]
DESTROY
INFECT
SECURE BOOT
4
Multi-threaded execution of malicious code begins in parallel
SMB EXPLOITS
CVE-2017-0144, CVE-2017-0145
445
KASLR, NX HAL/POOL KCFG, HVCI
Internet / Local Network
Org A
Org B
etc.
Dump from LSASS
Dump with CredEnumerateW
Stealing active tokens
CREDENTIAL THEFT
CREDENTIAL GUARD
List of credentials/tokens
Remote Execution through PSEXEC or WMIC
MOVE LATERALLY
DEVICE GUARD, APP LOCKER
Scanner enumerates targets for lateral movement (admin$)
139
445
SCANNING
List of machines
Local files on the machine are encrypted with AES
FILE ENCRYPTION
Local Network
Victim 1
Victim 2
etc.

In June 2017, NotPetya, which originated as a fraudulent tax software update in Ukraine, managed to infect hundreds of thousands of computers in over 100 countries in a matter of days. Unlike its predecessor, Petya, NotPetya incorporated the same exploit as WannaCry to execute the attack. The NotPetya attack is very similar to WannaCry, with one key difference. Instead of trying to make infected networks pay a ransom, NotPetya destroyed everything in its path. Unlike WannaCry, where it was directed at critical institutions that would be more likely to pay the ransom, NotPetya was engineered to do damage to the country’s infrastructure. David Dufour of PR Newswire (2017), stressed that there will be more just like NotPetya, “ This past year was unlike anything we've ever seen. Attacks such as NotPetya and WannaCry were hijacking computers worldwide and spreading new infections through tried-and-true methods. This list is further evidence that cybercriminals will continue to exploit the same vulnerabilities in increasingly malicious ways” (4). Figure 1.1 shows how the attack starts, and spreads to an uncontainable level. The attack caused significant damage, with some healthcare organizations reporting the loss of patient data and the disruption of critical healthcare services. One affected hospital reported that the attack caused a delay in cancer treatment for patients. The NotPetya attacks show that even if the attack is not aimed at healthcare, they are still easily caught in collateral damage due to lack of security.

Factors Contributing to Malware Attacks in Healthcare

Healthcare organizations have become an increasingly attractive target for cyber-attacks in recent years, with many high-profile attacks making headlines around the world. In this section, we will explore the factors that make hospitals a prime target for cyber-attacks. The first factor that makes hospitals vulnerable to cyber-attacks is the vast amount of valuable data they store. Hospitals collect and store a vast amount of sensitive patient data, financial information, and research data, all of which are valuable to cyber criminals. This data can be sold on the dark web or used for identity theft or ransomware attacks, making healthcare organizations an appealing target for attackers seeking to profit from stolen data. In addition to the value of the data they store, healthcare organizations are also vulnerable due to their limited resources. Many hospitals have limited budgets and staff dedicated to cybersecurity, making it easier for cyber criminals to exploit vulnerabilities in their systems. This is compounded by the fact that healthcare IT networks are often complex and interconnected, providing multiple entry points for attackers to gain access. Another factor that makes healthcare organizations a prime target for cyber-attacks is the high availability requirements of their services. Healthcare services need to be available 24/7, which means that hospitals cannot afford to have their systems down for an extended period. This makes hospitals more likely to pay ransomware demands to get their systems back up and running, as the cost of downtime can be far greater than the ransom demanded by attackers. For example, Muthuppalaniappan (2021) explains that Hackers targeted institutions working on COVID-19 vaccines, to increase the chances of them paying the ransom, “UK’s National Cyber-Security Centre announced a significant increase in cyber-attacks perpetrated by hostile states and cyber-criminals targeting British universities and institutions working on COVID-19 research” (2). As horrible as it sounds, it works and leaves institutions no choice. Furthermore, many healthcare professionals lack cybersecurity training, leaving them vulnerable to phishing attacks and other social engineering tactics used by cyber criminals. Finally, many healthcare organizations still use legacy systems that are no longer supported by vendors and are vulnerable to cyber-attacks, and do not upgrade due to cost. Overall, the combination of valuable data, limited resources, complex networks, high availability requirements, lack of cybersecurity training, and legacy systems make hospitals a prime target for cyber-attacks.

Prevention of Malware Attacks in Healthcare

The threat of malware attacks on healthcare organizations is a serious concern, as discussed in previous sections. Healthcare organizations must take proactive measures to prevent these attacks and protect patient data, ensure the continuity of care, and maintain the integrity of their operations. There are several measures that healthcare organizations can take to mitigate these security threats.

One of the biggest vulnerabilities can be fixed relatively easily, through ensuring that all software and systems are patched and up to date. This includes operating systems, applications, and firmware. Outdated software can contain vulnerabilities that can be exploited by malware attacks, which is clearly shown by WannaCry, which took advantage of out-of-date software. Lisa Pino, from the U.S department of health, stresses the importance of updating software, “Such unpatched vulnerabilities give hackers easy access to an organization’s computer server, and possible entry into other parts of a network. These reports underscore why it is so important for health care to be vigilant in their approach to cybersecurity" (2022, para. 2). Every update to any software typically patches known exploits, and not updating systems leave the door to attacks open. Though this sounds simple, hospital-wide updates could create downtime, and be expensive.

Another way these attacks can be prevented is the use of Endpoint protection software, such as antivirus and anti-malware software, can help prevent malware infections on individual devices. Endpoints include anything, from laptops, medical devices, to even smartwatches. Endpoint protection This software should be updated regularly to ensure it can detect and respond to the latest threats. This is extremely important if an organization has a lot of remote work done. McKeon (2022) explains how endpoint security can greatly improve organization and reliability, "Organizations are now looking to take a holistic, end-to-end stance on security to encompass all entry points to the network. By integrating network and endpoint security, organizations are afforded greater visibility over the entire range of security threats that they face, both in real time and for historical analysis" (para. 19). This seems like a very universal solution, though it still is not impenetrable, due to the inconsistency of healthcare systems, and varying budget for each organization.

Finally, one of the most cost-effective solutions to help ensure that cyberattacks are handled accordingly, is training. Healthcare staff should receive ongoing training on cybersecurity best practices, including how to identify phishing emails, how to create strong passwords, and how to report suspected security incidents. Staff training should also include regular updates on the latest cybersecurity threats and trends. McKeon explains how this is a threat, "the rapid shift to entirely remote work as one of the biggest cybersecurity threats to the healthcare sector. Most remote workers received minimal cybersecurity training, and operational needs caused organizations to overlook cybersecurity" (2022, para. 7). Mckeon goes on to also explain that employees bringing in their own devices such as laptops improves efficiency, but comes with several safety concerns that lead to patient data leakage (para. 8). Proper security training can significantly improve network security.

Conclusion

To conclude, healthcare organizations are prime targets for malware attacks due to the sensitive nature of patient data and the potential for financial gain. Malware attacks can have devastating effects on healthcare services, patient outcomes, and the reputation of the organization. However, prevention strategies such as employee education, regular software updates, and robust cybersecurity measures can greatly reduce the risk of attacks. As healthcare continues to become more digitalized, the threat of malware attacks will only increase. It is imperative for healthcare organizations to prioritize cybersecurity and take proactive steps to prevent attacks. Malware attacks pose a significant threat to healthcare organizations and patient outcomes, but with effective prevention strategies, these risks can be mitigated.

References

Cornish, T. C., & McClintock, D. S. (2022). Are You Prepared? Laboratory Downtime in the Ransomware Era. American Journal of Clinical Pathology, 157(4), 482–484. https://doi.org/10.1093/ajcp/aqac021

Davis, J. (2019, May 30). 40% of health organizations suffered wannacry attack in past 6 months. HealthITSecurity. Retrieved April 16, 2023, from https://healthitsecurity.com/news/40-of-health-organizations-suffered-wannacry-attack-in-past-6-months

Ghafur, S., Kristensen, S. R., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. Npj Digital Medicine, 2(1). https://doi.org/10.1038/s41746-019-0161-6

McKeon, J. (2022, September 7). Why Endpoint Security is Critical For Healthcare Cybersecurity. HealthITSecurity. https://www.healthitsecurity.com/features/why-endpoint-security-in-healthcare-is-critical-for-cybersecurity

Menaka Muthuppalaniappan (2021), LLB, Kerrie Stevenson, MBChB BMedSci (Hons) FHEA, Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health, International Journal for Quality in Health Care, Volume 33, Issue 1, mzaa117, https://doi.org/10.1093/intqhc/mzaa117

Ralston, W. (2020, November 11). The untold story of a cyberattack, a hospital and a dying woman. WIRED UK. https://www.wired.co.uk/article/ransomware-hospital-death-germany

Rights, O. F. C. (2022, April 8). Improving the Cybersecurity Posture of Healthcare in 2022. HHS.gov. https://www.hhs.gov/blog/2022/02/28/improving-cybersecurity-posture-healthcare-2022.html

Webroot Threat Research Reveals the Top 10 Nastiest Ransomware Attacks of 2017: NotPetya, WannaCry, and Other Ransomware Strains Caused Unprecedented Damage to Businesses, Infrastructure, and Users. (2017, Oct 31). PR Newswire https://go.openathens.net/redirector/lewisu.edu?url=https://www.proquest.com/wire-feeds/webroot-threat-research-reveals-top-10-nastiest/docview/1957708281/se-2