Prescribing Protection: A Comprehensive Approach to Malware Mitigation in Healthcare

Karch Forward, Ariana Ciaschini, Finn Rhoads, Jacie Orr, Neha Gopinathan

CSEC 468.01.2231

Introduction

Today, roughly 30% of the world's data belongs to the healthcare industry. And as healthcare data exponentially increases, so do the security and privacy threats to consumer's personal and medical information. (Hoffman, A. E. (2020, July 29))

Given the relevance of cybersecurity in multiple facets of healthcare such as, healthcare data, medical equipment, and patients' personal information, it comes as no surprise that healthcare institutions have long been one of the most popular targets of cyber-attacks. With the ever-growing integration of technology with healthcare, the impact of losing access to medical equipment and leaking of Personal Identification Information (PII) is significantly high, emphasizing the need for stringent mitigation strategies (Javaid et al., 2023).

Knowing this, it is necessary to consider how malware may be deployed against our infrastructure, and what mitigation strategies might be used both at the system or organizational level to reduce these risks. This paper will show the precedent of malware impacting similar companies surrounding the healthcare industry. Following this, the paper will dive into the methods used in researching solutions for malware attacks, followed by our findings of relevant risks and their corresponding mitigations. Lastly, included is emerging work in the field.

Keywords: Malware, Ransomware, Healthcare, PHI, Risk Mitigation

Background

What is malware and what is ransomware?

Software that is designed specifically to harm or prevent users from accessing services, files, etc., on their systems is referred to as malware or malicious software. It comes in many forms, including viruses, spyware, ransomware, and more.

Ransomware is a type of malware that restricts user access to their system by locking it, by encrypting the user's files or system, until a ransom is paid. It is a highly disruptive form of malware as it impacts both the customer and the business hierarchy (Permana et al., 2022).

How have healthcare organizations historically been attacked with malware?

Healthcare organizations have been targeted by malware through various means. Some prominent incidents include:

1. WannaCry Ransomware (2017): The WannaCry ransomware attack affected the UK's National Health Service (NHS) and other organizations globally. It exploited a vulnerability in Microsoft Windows systems, causing widespread disruptions.

2. Hollywood Presbyterian Medical Center (2016): Los Angeles hospital fell victim to a ransomware attack, leading to a $17,000 bitcoin ransom to restore access to its systems.

3. Hancock Regional Hospital (2018): A hospital in Indiana experienced a ransomware attack where hackers used Microsoft Remote Desktop Protocol (RDP) as an entry point. The attack disrupted hospital operations until a ransom was paid.

Why are healthcare organizations increasingly targeted?

Healthcare organizations are increasingly targeted for several reasons.

1. They store a vast amount of sensitive and valuable data, including personal and medical details, making them attractive targets for cybercriminals aiming to steal this data.
2. Healthcare facilities heavily rely on computer systems for patient care, record-keeping, and other critical functions. Disrupting these systems can have severe consequences, making them appealing targets.
3. Some healthcare organizations may have outdated or inadequately protected systems, creating vulnerabilities that can be exploited by attackers.
4. Cybercriminals see the potential for significant ransom payments from healthcare institutions that may be more willing to pay to restore critical services and protect patient data (Argaw et al., 2020).

Methodology

Infrastructure Considered

We considered the risk of malware to a hospital as it would generally operate in the US, following all applicable laws and compliance standards. The specific resources owned and operated on-premises include:

- SQL Servers 2008-2016 for Finance, HR, and IT databases
- Windows Servers 2003-2012
- Windows Server 2012 with CA Service Desk Manager r7.0

External technologies owned and supported by vendors include:

- EHR Cloud Application
- Microsoft Office 365
- One Drive
- CA Identity Manager 14.1
- Amazon Web Services (AWS) to move physical servers to Virtual Machines (VMs)

Additionally, we consider the following third-party relationships of the hospital:

- Health Information Exchange agreement with the states of Michigan, Illinois, and Ohio.
- Access agreements to share health information via EDI, as required by the state, including public health, mental health, immunology, and cancer.
- (25) business vendors, (12) of which are without Business Associate Agreements, among them: transcription service, medical records, food service, and medical supplies vendors.

Additional Concerns

In addition to researching the above hardware and software's susceptibility to malware, we researched; historical exploits in the healthcare industry, mitigations employed and their effectiveness, controls considered industry standards, as well as legal requirements. Our attack surface extends to the hospital's personnel, thus our mitigations may span across network security, personnel security, issue/system-specific policy, enterprise-level policy, and more.

Search Criteria & Evaluating Sources

To ensure coverage of current malware technologies, the scope was refined to academic publications within the last (5) years and the most recent version of any applicable reference material. Sources were limited to English publications freely available through public databases (e.g. Google Scholar), accessible through our university (e.g. RIT libraries), as well as product/service specific primary and authoritative references (e.g. Microsoft.) Quality of sources were cross-referenced and assessed before data could be added to preliminary findings. Scholarly publications included information technology-focused publications as well as healthcare publications relevant to malware impacting healthcare organizations and corresponding mitigations.

Findings

Outdated & Vulnerable Systems

A system's defense is only as strong as its weakest link. Out-of-date software and unpatched systems create the opportunity for an attacker to penetrate a security perimeter before moving laterally throughout. While segmenting the network can limit the mobility of the attacker once in a system, securing machines with outdated components protects the data those machines hold, as well as removes the foothold for which adversaries may attempt to leverage.

Of the Microsoft products utilized, several are beyond their extended support date but are still covered for Extended Security Updates for critical vulnerabilities only including SQL Server 2012 and Windows Server 2012. (Microsoft, "Extended Security Updates") Windows SQL Server 2008 and Windows Server 2008 can receive these security updates only if they are migrated to Azure using Microsoft's VM IaaS, and no such coverage is supported for Windows Server 2003. (Microsoft "Windows Server 2003")

Need for Incident Response Planning & BCDR

Crucial to reducing the impact of malware attacks, is a clear understanding of the organization. What systems are used, what normal operations look like, and how they may be expected to change in response to a security incident, all members of the organization should comprehend their role in promoting business continuity and supporting recovery efforts. For example, in 2017 Erie Country Medical Center was attacked with ransomware, SamSam. (Millard, 2017) While sensitive data was inaccessible from the ransomware, and systems were

taken offline to prevent its spread, the level 1 trauma center continued to serve the community without needing to divert patients delaying their care. Success was largely attributed to BCDR plans and staff practicing procedures necessary for navigating various incidents. Staff regularly rehearsed providing care during technical outages including blackouts, using paper records, and prescription pads, and following communication plans. (e.g. notifying pharmacies e-scripts could not be sent and paper scripts needed to be honored.) Health data was able to be accessed from regional EDI on machines provided by a sister facility, while cybersecurity experts supported the forensic investigation and wiping infected workstations & servers, and recent backups were restored by the EHR vendor. Planning to respond and recover requires perspective about the organization, alternate procedures to be developed and rehearsed, and for all stakeholders including third-party vendors to understand their roles and responsibilities. We can examine the variation in policy at the intersection of IR and BCDR with privacy, data protection, and information security policies from a survey of Michigan health sector information security practitioners. Of those surveyed who reported their organizations experienced a security incident in the past year, the majority identified the incident type as ransomware or web-borne malware attacks. (2021 MiHCC Cybersecurity Study, n.d.) Findings also revealed that 30% of respondents said their organizations lack cybersecurity IR plans, and 36% said their IR plans are not regularly exercised. A plurality of respondents also reported their organization lacked one or more practices that support IR including keeping comprehensive inventories of critical applications and who has access to them, inventories of hardware and/or software, and utilizing continuous monitoring products or services, were not used. (59%, 71%, and 61%)

Gateway Configuration & Firewall Deployment

Properly configured gateways and deployed firewalls are two components of quarantining malware as a form of risk mitigation and management. One constraint faced by many organizations, including this one, is lack of resources such as time, money, and energy. Therefore, it is not reasonable to expect that all systems within this organization can "adopt sufficient security mechanisms" (*Spatial Firewalls: Quarantining Malware Epidemics in Large-Scale Massive Wireless Networks | IEEE Journals & Magazine | IEEE Xplore*, n.d.). However, one concept to remedy this issue is putting the best security around "critical zones" on a network. Percolation theory studies the minimum number of spatial firewalls required that can sufficiently isolate malware on a network to protect the uninfected systems. The results from this study showed that random selection of devices to most securely protect provided the greatest protection in terms of malware isolation.

There are two main methods of malware detection via gateway, which are based on a file's signature or based on a file's behavior. One issue with signature-based detection is that one minor change can be made to a piece of malware's signature, making its signature not match any known malicious signatures stored in the system. There are other ways to bypass signature-based detection as well, such as creating new malware altogether, packing known malware in a different way, using steganography, and encryption. Typically, SMTP and HTTP/SSL Anti Virus (AV) gateways allow filtering based on file format (*Investigation of Bypassing Malware Defences and Malware Detections | IEEE Conference Publication | IEEE Xplore*, n.d.). This method can be helpful, but still has multiple known ways to be circumvented. The proposed

solution for issues in signature-based detection is to employ behavior-based detection. Honeypot systems can be used within an organization, where executables can run in a virtualized, segmented environment. Then, if malicious activity is detected, it can be deleted from a system and prevented from continuing to the main network.

Network Segmentation

Network segmentation is the concept of having devices on a network connected to only a few others on the same VLAN. While network segmentation itself does not prevent malware, it does prevent malware from damaging more of a system. Malware typically makes its way to connected hosts on the same network once it has infected one host. An organization that implements network segmentation via a VLAN and/or ACLs forces malware to stay "isolated to just the network segment the infected endpoint is on and does not spread through the entirety of the organization," (Frenz & Diaz, 2018). Endpoint devices are often targeted due to their vulnerabilities such as being operated by non-cybersecurity-aware individuals, making more critical systems less vulnerable to malware attacks.

Another type of network segmentation that can be employed is virtual machine segmentation. There are many benefits to working with a virtual environment, one of which is malware that infects the virtual machine, stays in that space, and bears no impact on the physical device running that virtual machine. If this organization chose to work with a more virtual environment, then virtual machine segmentation would be a feasible solution for preventing malware from spreading to other virtual machines as well, but is not highly useful at this time and rather a consideration for future operations.

Need for Employee Awareness

A common method for employee training of any kind is video training, where employees are required to watch a series of videos and then typically answer situation-based questions about the content presented. One study found that employees who received training in the form of a malware report, as opposed to videos, both types of training, or no training, showed changed beliefs regarding cybersecurity (*Improving Employees' Intellectual Capacity for - ProQuest*, n.d.). A 2019 literature review highlights that no state requires nurses to receive continuing education on the subject of "informatics or cybersecurity of patient PHI to maintain licensure." (Kamerer & McDermott, 2020) As a major user base of informatic systems including EHR it is crucial for organizations to require training beyond protecting PHI under HIPAA for compliance purposes, but the prevalence and consequences of data breaches, and the importance of effective data management and cyber hygiene.

One recommendation for this organization, based on this study, is to employ a report-based training requirement for all employees. To implement this, a malware report based on all outstanding data should be compiled. This would be based on all detected malicious binaries on the organization's system. Employees would read this report, and then over a year, a more detailed report would be compiled for the next training session, repeated annually. A barrier that would likely be present in this method would be that healthcare professionals such as doctors and nurses are already overwhelmed with the amount of patients they have, combined with the long hours they are expected to work. Additionally, many of these professionals also have to undergo continual learning experiences to keep their licenses. In the context of this

cybersecurity training, this means that these employees would have less time to complete and dedicate a full attention span to this training, or would fail to complete the training at all. In order to remedy this, it is recommended that this cybersecurity training is made mandatory and part of continuing education for healthcare professionals.

Endpoint Security Solutions

Endpoints in technology are referred to as the places in a network or system where someone can gain access to the system. Examples of this within this healthcare organization are laptops, phones, or any other devices that staff from the organization interact with on a daily basis. Healthcare professionals may use OneDrive for file storage, or use Microsoft Office 365 to take notes on patients' appointments and write treatment plans. Every piece of software has vulnerability, no matter how secure. These systems are interacted with on different hosts frequently, thus opening these systems and the information they store open to being exploited.

Several endpoint security solutions were found in the course of research. One mitigation is utilizing IoT (Internet of Things) protection, securing data stored in cloud systems and securing network traffic. Additionally, anti-virus software is highly recommended for this organization, as it is easy to stall on many devices, and is a relatively inexpensive and simple step to take in securing a system. Additionally, adding application controls and URL filters should be considered for this organization, both of which prevent users from accessing malicious or unknown files or applications (Kamruzzaman et al., 2022).

Results

Prioritize Outdated Systems - Migration & Hardening

Several factors need to be taken into consideration while hardening outdated systems. Firstly, systems should be identified and prioritized based on their sensitivity level and the need for improved security measures. Having a 'System and Network Security Design' or SNSD can enhance an organization's security system, making it effective and secure. Additionally, the SNSD framework can be used to predict future cyber-attacks. Secondly, malware, such as Advanced Persistent Threats (APTs), use covert communication channels to avoid being detected. Systems should include the prevention and detection of these channels to prevent data leakage resulting from malware. Thirdly, deployment of honeypots/honeynets can help with the detection and elimination of malware before it has the chance to function and spread. Lastly, additional application hardening techniques such as Data Execution Prevention (DEP) can help enhance the security of outdated systems. DEP is the mitigation of malicious code injection. It marks areas and prevents malicious code from being executed.

Use of Machine Learning

Machine Learning is a branch of Artificial Intelligence that involves computers analyzing, recognizing, and predicting patterns and trends from a large amount of data. The self-learning nature of machine learning allows it to constantly learn and improve, helping it develop newer strategies against malware (Sibi Chakkaravarthy et al., 2019).

Especially following the COVID-19 pandemic, many aspects of day-to-day health monitoring have moved to digital and cloud-based solutions. Take for example, a patient that uses a smart watch to monitor their heart rate. This data then is stored on a central server, which the patient and their healthcare providers have access to, in order to monitor for abnormalities. When trying to search for malware in these storage solutions, one way to try and find malware is to search for .exe files, but attackers creating malware have a multitude of ways around this method of detection. Already, an algorithm has been developed to detect malware from a database of heart rate data, and was shown to outperform machine learning tools in detecting malware in this context (Mohammed et al., 2023).

Machine learning certainly has its place in proactively finding and removing malware from an organization's system and network. However, it should not be considered the single golden standard in malware detection. The concept of cybersecurity is building a wall, having that wall penetrated in some way, and then building or repairing the wall. Oftentimes this wall must be repaired using new tools and existing tools. Machine learning is a useful tool to keep in a toolbox in this regard.

Security & Data Privacy Training

For effective defense in depth, the organization can not rely only on technical controls, as they are useless if circumvented by users like nurses, presenting vulnerabilities. In addition to security and privacy training required by regulatory standards, the organization may adopt additional training requirements, to more frequently inform staff of relevant changes to policies and procedures, enforce secure practices, and through the use of module quizzes or threat

simulations identify behaviors that need to be discouraged. Policies that may be integrated into security or privacy training may include incident reporting, role-specific responsibilities in IR or BCDR, acceptable use of internal systems and removable media, remote access, accessing internal systems from external/personal devices, shared workstation use/logout policies etc. Training may extend to third parties, including subcontractors that access sensitive systems or data, per additional third-party agreements.

Future Work

The ever-evolving landscape of cybersecurity demands innovative approaches to combat emerging threats within any industry. The revolutionary technological advancement of artificial intelligence (AI) helps to uphold, maintain, and lift cybersecurity standards. Future work of malware mitigation specifically within cybersecurity not only has the potential to solve advanced threats, but also has the capacity to revolutionize the entire landscape of digital security. Researchers from the University of Memphis are seeking to apply AI technologies as well as advanced algorithm techniques to develop easy-to-use tools applicable within any industry, including healthcare.

The underlying framework allows for the mundane tasks of both static and dynamic analysis conducted on pieces of malware to be completed in a more efficient manner. The tool has the ability to be run in any environment including virtual machines or sandboxes, which increases security when dealing with suspected malicious files or applications. With AI integration, a thorough and complete malware analysis can be conducted via automated code analysis and pattern discovery which then the AI can upload the digital signature of the piece of malware to an already existing database for use with other various types of antivirus software (S. Poudyal et al., 2020).

Researching technologies to be paired with AI is the future of technological solutions that can be applied in any industry. Being on top of cybersecurity is imperative for society as people have an increasing presence on the Internet. Further work into AI cybersecurity solutions are a strong foundation for the future of digital security.

Conclusions

In conclusion, the increasing volume of healthcare data, constituting approximately 30% of the world's information, has become a focal point for security and privacy concerns (Hoffman, A. E., 2020). As the healthcare industry undergoes exponential growth in data accumulation, the associated risks to personal customer data as well as confidential industry data are continually growing. It is imperative that industries such as healthcare take appropriate action to not only protect themselves, but their clientele as the realm of cyberspace becomes more dangerous with evolving threats such as malware.

By examining instances where similar companies have fallen victim to malware attacks, we gain valuable insights into the potential vulnerabilities and consequences faced by the healthcare industry. Understanding the underlying causes from these malware incidents allows us to form a foundation for developing mitigation strategies. The subsequent exploration into research methodologies for combating malware attacks unveils the multifaceted nature of this endeavor.

It is imperative any individual, company, or sector take cybersecurity seriously with regards to any threat, including the discussed topic of malware within this paper. Without a solid foundation for digital security and easy attack vectors, adversaries of any capacity or background will be able to penetrate into system architecture leaving those within the healthcare industry vulnerable to data breaches, blackmail, or extortion.

References

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020, July 3). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks - BMC Medical Informatics and Decision making. BioMed Central. https://doi.org/10.1186/s12911-020-01161-7

Bin Saleem, W. Y., Ali, H., & AlSalloom, N. (2020). A Framework for Securing EHR Management in the Era of Internet of Things. *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*. https://doi.org/10.1109/iccais48893.2020.9096788

Frenz, C., & Diaz, C. (2018). *Anti-Ransomware Guide*. https://owasp.org/www-pdf-archive/Anti-RansomwareGuidev1-7.pdf

Improving employees' intellectual capacity for - ProQuest. (n.d.). Www.proquest.com. Retrieved October 30, 2023, from https://www.proquest.com/docview/2533647659?accountid=108

Investigation of bypassing malware defences and malware detections | IEEE Conference Publication | IEEE Xplore. (n.d.). Ieeexplore.ieee.org. Retrieved December 2, 2023, from https://ieeexplore.ieee.org/abstract/document/6122815?casa_token=gyKspLH_6vcAAAAA:2GXAxNw50rjkDWrBiSx1Xh57xhnDAw-WfUWM7b_R6uoddYa1_ay5nXg1OCNI8ZPvCY-RrFcAIw

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for Healthcare Domains: A comprehensive review of recent practices and Trends. Cyber Security and Applications, 1, 100016. https://doi.org/10.1016/j.csa.2023.10001

Kamerer, J. L., & McDermott, D. (2020, January). *Cybersecurity: Nurses on the Front Line of Prevention and Education*. Journal of Nursing Regulation. Retrieved September 12, 2023, from https://www.journalofnursingregulation.com/article/S2155-8256(20)30014-4/fulltext

A. Kamruzzaman, S. Ismat, J. C. Brickley, A. Liu and K. Thakur, "A Comprehensive Review of Endpoint Security: Threats and Defenses," 2022 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 2022, pp. 1-7, doi: 10.1109/ICCWS56285.2022.9998470.

Mohammed, M. A., Lakhan, A., Zebari, D. A., Abdulkareem, K. H., Nedoma, J., Martinek, R., Tariq, U., Alhaisoni, M., & Tiwari, P. (2023). Adaptive secure malware efficient machine learning algorithm for healthcare data. *CAAI Transactions on Intelligence Technology*. https://doi.org/10.1049/cit2.12200

Managing Healthcare Risk In A Networked World | Independently conducted by Ponemon Institute LLC | Sponsored by Michigan Healthcare Cybersecurity Council. (2021, November). Michigan Healthcare Cybersecurity Council. Retrieved October 3, 2023, from https://www.mihcc.org/2021-mihcc-cybersecurity-study/

Microsoft. (n.d.). *Product Lifecycle FAQ - Extended Security Updates*. Microsoft Learn. Retrieved October 24, 2023, from https://learn.microsoft.com/en-us/lifecycle/faq/extended-security-updates

Microsoft. (n.d.). Windows Server 2003 - Microsoft Lifecycle. Microsoft Learn. Retrieved October 24, 2023, from https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2003-

Millard, W. B. (2017). Where bits and bytes meet flesh and blood: Hospital responses to malware attacks. Annals of Emergency Medicine, 70(3), A17-A21.

Permana, G. R., Trowbridge, T. E., & Sherborne, B. (2022, December 13). Ransomware Mitigation: An Analytical Investigation into the Effects and Trends of Ransomware Attacks on Global Business. https://doi.org/10.31234/osf.io/ayc2d

Sibi Chakkaravarthy, S., Sangeetha, D., & Vaidehi, V. (2019). A survey on malware analysis and Mitigation Techniques. Computer Science Review, 32, 1–23. https://doi.org/10.1016/j.cosrev.2019.01.002

Spatial Firewalls: Quarantining Malware Epidemics in Large-Scale Massive Wireless Networks | IEEE Journals & Magazine | IEEE Xplore. (n.d.). Ieeexplore.ieee.org. Retrieved December 2, 2023, from https://ieeexplore.ieee.org/abstract/document/9214384