REvil’s Rise in Targeting The Healthcare Industry Through Ransomware

(Technical Report)

Impact of Ransomware on the Healthcare Industry with Policy and Education Considerations

(STS Research Paper)

A Thesis Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science, School of Engineering

Connie Zhang

Fall, 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature ____ Date 10/31/2022
Connie Zhang

Approved ____ Richard Jacques _______ Date 11/14/2022

STS Advisor: Richard D. Jacques, Ph.D., Department of Engineering & Society

Introduction

In 2021, the average cost of the direct impact from a ransomware attack was $1.85 billion, doubling the figure from the previous year (Beaman et al., 2021). Ransomware is a type of malware that attempts to extort an organization by freezing access to its data, typically requiring a payment or ransom in exchange (Morgan et al., 2020). The healthcare industry is an especially vulnerable sector to ransomware, as it contains Personal Health Information (PHI) making the retrieval of information from threat actors ever more important. Moreover, healthcare is a target as medical records and devices are a critical part of any infrastructure. Although there are some security policies in place to mitigate any impact, further analysis of the technical tactics and social implications are needed to ensure the protection of valuable assets and educate those in the healthcare industry. The technical aspect of this paper will cover common ransomware tactics as well as a deep dive into my work with analyzing a threat actor group known as REvil. Ransomware, specifically targeting the healthcare sector, directly affects our society and its critical infrastructure systems. The STS portion will analyze the impacts of a ransomware attack on such a crucial part of our society, and what healthcare systems can do to prevent them.

RANSOMWARE: COMMON TECHNIQUES AND ANALYSIS OF REVIL

Ransomware is typically introduced into a system through three common methods: scareware, locker, and crypto (Beaman et al., 2021). Scareware uses interactive interfaces such as pop-up ads and emails to lure an unsuspecting user to gain access, such as through phishing attacks. Through this method, an attacker can easily trick a user into clicking links that download malware directly onto their system. Locker ransomware works by encrypting files and locking computer functionality. This in turn blocks access from the user but can be combated through launching a malware detection program or rebooting the system in a secure mode. Lastly, and arguably the hardest to recover files though, is crypto malware. Crypto Malware encrypts data mostly using asymmetric encryption, which makes it especially hard for a victim to decrypt without restricted access to the attacker's key. Asymmetric encryption's defining characteristic is its two keys: public and private. Due to this type of encryption, a victim requires the attacker's private key to decrypt its missing files, which are only available for a hefty ransom. A common asymmetric encryption method is SSL, or Secure Socket Layer, which enables a secure connection between an online server and an internet browser. Another common asymmetric encryption algorithm isRivest Shamir Adleman (RSA). This algorithm involves key generation, key distribution, encryption, and decryption. Without knowing the location of the key distribution, decryption is nearly impossible (Castillo, 2020). Threat actors use these common techniques to "blackmail" their victims into paying a ransom.

As ransomware attacks increase, threat actors have begun to form more formalized groups known as Ransomware-as-a-Service (RaaS) to develop tools and design plans of attack. A rising Ransomware as a Service (RaaS) group, named REvil, has previously targeted the meat production company JBS and a Taiwan-based hardware supplier (Tarabay, 2021). REvil, like other RaaS, encrypts files of value, making them inaccessible. Proving their breadth and depth of tactics, REvil conducts extensive research on their targets to ensure a wealthy payout. Common tactics conducted by REvil include exploiting privilege escalation and encrypting files (Intel 471 Malware Intelligence team, 2022). Therefore, this organization presents a great threat to any critical infrastructure.

My internship focused on identifying key tactics, techniques, and procedures used by REvil in relation to the healthcare industry. I, along with two other team members, wrote a whitepaper to detail REvil’s attack history and common attack tactics. Our team consisted of a researcher, who focused on debriefing previous attacks conducted by REvil. Another team member worked on simulating REvil attacks in a controlled environment to include the results in the paper. My work focused on identifying any gaps of techniques and tactics we had in our whitepaper and previously found techniques in the MITRE ATT&CK Framework and the MITRE Cyber Analytics Repository. Working together, our paper served as an overview of REvil’s capabilities and methods to protect against their attacks. This paper is important to bring light to a precarious threat actor and to educate members of the cybersecurity community in hopes of spreading awareness to other critical industries. Brianna Morrison will serve as my technical support as I complete a technical report and continue my research on this topic.

THE IMPACT OF RANSOMWARE ON THE HEALTHCARE INDUSTRY

The healthcare industry is a critical infrastructure in our society. With 70% of cyberattacks in the healthcare industry amounting to ransomware attacks, it is imperative to acknowledge the extent of which an attack should be prepared for, and how even one vulnerability in a system could lead to potentially life-threatening consequences (Cohen, 2020). With the increase in use of digital technologies in the healthcare industry, our information and equipment stand at a greater threat than ever.

The first ransomware attack in 1989 introduced a new type of crime that disrupts daily life and can be conducted remotely from the other side of the world. Traditionally, attackers targeted internal networks, medical databases, and PCs. However, more recent attacks have started incorporating medical devices, creating an even deadlier outcome. The 2017 “WannaCry" attack spread to five UK hospital emergency departments and 81 National Health System

Hospitals, resulting in more than 19,000 appointment cancellations (Riggi, 2022). The sophisticated evolution of ransomware attacks has produced an even greater risk as most hospitals are not equipped to manage a disruption of this scale.

The effect of the COVID-19 pandemic has brought healthcare devices and systems to the forefront of cyber-attacks. The main challenges and vulnerabilities the healthcare industry faces include endpoint device management during remote work and human factors (He et al., 2021). Remote work introduces an abundance of vulnerabilities as employees not properly connecting to a virtual private network can introduce challenges to controlling entry points for possible attacks. Additionally, humans are the weakest links in a security chain. Healthcare workers and students must be educated on the proper use of medical devices, including the potential cyber risks to keeping systems running and their patient data protected (Niki et al., 2022). These historic events are only the beginning of more open opportunities and reveal vulnerabilities for threat actors to attack.

Threat actors continue to increase the severity of these attacks by threatening to post personal health information on the dark-web, and gain resources by forming organized groups to launch these attacks (Sumner & Keenan, 2022). One step that could drastically reduce the amount of damage a ransomware attack could incur, would be to have data backups either physically on the premises or on the cloud. A recovery strategy is imperative to getting a hospital system back up and running, particularly emergency or intensive units. An estimated 4.5 billion medical devices rely on the Internet, which accounts for $6 billion annually, making the healthcare industry an extremely vulnerable and lucrative market to attack (Ghayoomi et al., 2021). These attacks can lead to fatalities as medical devices fail, leaving patients unseen and surgeries canceled.

Looking at this issue through an Actor Network Theory (ANT) lens, it is clear to see the reliance on patient data and Internet connected medical devices for hospitals to function, as shown in Figure 1. Due to this central reliance, hospitals without proper backups and preparation are forced to provide payment of ransom to threat actors. The ANT diagram can be used to show the relationship between the threat actors, hospitals, and the valuable data and equipment. It displays the necessary relationship between hospitals and their equipment, as well as the demand for a payment from a threat actor.

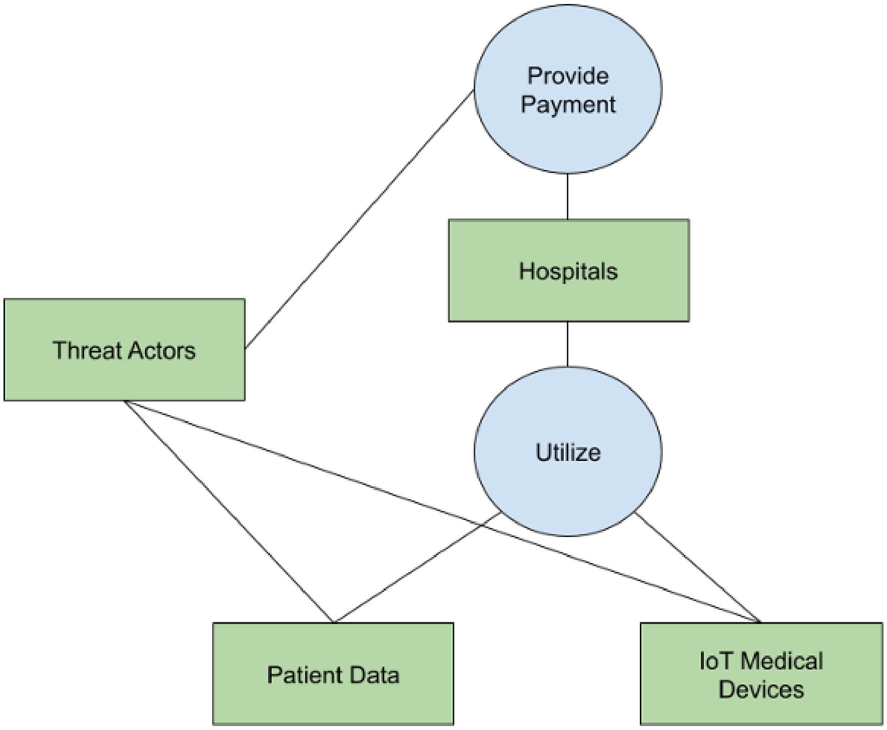

Figure 1. Actor Network Diagram of the relationship between Actor networks and Hospitals' reliance on medical devices and patient data as vulnerable assets (Zhang, 2022).

Ransomware poses a direct threat to patient privacy as it leaks personal health information (PHI). To combat this threat, The Health Insurance Portability and Accountability

Act (HIPAA) has in place security rules that mandate healthcare providers to conduct regular risk assessments to minimize their vulnerabilities as well as protocols in place to detect and prevent malicious software from infecting their computer systems. The policy also requires healthcare professionals to receive additional training to identify any malicious actions through phishing scams (DeMuro & Norwood, 2021). My research highlights the ramifications of ransomware in healthcare, analyzing potential threats and vulnerabilities in this critical sector of our lives. To prevent such attacks, the healthcare industry must control access to Operating Systems, monitor incoming and outgoing email traffic and educate users of their systems on good cybersecurity practices. However, even with these measures in place, the cybersecurity realm is ever changing. The healthcare industry must adapt to technological advances such as the Mobility, Cloud, and IoT, and prepare more adaptive response plans for future attacks (Chung, 2020).

My STS research will analyze the impact of ransomware on critical infrastructure, specifically the healthcare industry. I will use a literature and policy review to support my research findings. A literature review will consist of analyzing and evaluating previous works of literature related to ransomware and its impact on the healthcare sector. It will include a look into the history of ransomware attacks and summarize the current vulnerabilities and impact of these attacks. The policy review will focus on the specifications of the Health Insurance Portability and Accountability Act (HIPAA), which is in place to secure measures within the healthcare system. Looking at the impact of this policy will provide an important overview of the current laws that exist and how they could be improved to better prevent a disastrous attack on a hospital system. Using a conjunction of both methods, I will have the insights to detail the impacts of a potential attack and ways for improving the security posture of hospitals as well as the policies in place.

Ransomware directly affects our society and its critical infrastructure systems, and measures need to be in place to combat and prevent further damage. The technical deliverable will cover common ransomware tactics and discuss my internship experience collaborating with a team to analyze specific techniques from REvil. This project sheds light on how ransomware can control millions of systems and understand the workings of REvil in hopes to detect attacks earlier and in place protective measures against them. The deliverable will provide the cybersecurity community with a greater insight on threat actors and the common tactics to watch for, as well as reach other industries where ransomware attacks are common. My STS portion will answer the impacts of a ransomware attack on our daily healthcare systems and discuss what policies and procedures to be implemented to remediate the effects. This research will in turn help to educate the healthcare sector on how to prepare for such attacks, to prevent unauthorized access to patient data, and ensure essential medical systems run without disruption.

References

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, *111*, 102490. https://doi.org/10.1016/j.cose.2021.102490

Castillo, E. M. (2020). *Understanding the Use of Malware and Encryption*. https://doi.org/10.25778/TTJ9-SR29

Chung, M. (2020). New Ransomware Innovations Bring Shame and Fear to Health Care. *Journal of Health Care Compliance*, *22*(5). Business Source Complete. https://proxy01.its.virginia.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&site=eds-live&db=bth&AN=146114433

Cohen, J. K. (2020). Healthcare ransomware attacks intensify in severity and sophistication. *Modern Healthcare*, *50*(4). Business Source Complete. https://proxy01.its.virginia.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&site=eds-live&db=bth&AN=141479126

DeMuro, P. R., & Norwood, H. (2021). Ransomware in the Healthcare Industry. *Health Lawyer*, *34*(1). HeinOnline. https://proxy01.its.virginia.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&site=eds-live&db=edshol&AN=edshol.hein.journals.healaw34.7

Ghayoomi, H., Laskey, K., Miller-Hooks, E., Hooks, C., & Tariverdi, M. (2021). Assessing resilience of hospitals to cyberattack. *DIGITAL HEALTH*, *7*, 20552076211059370. https://doi.org/10.1177/20552076211059366

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *Journal of Medical Internet Research*, *23*(4), e21747. https://doi.org/10.2196/21747

Intel 471 Malware Intelligence team. (n.d.). *REvil Ransomware-as-a-Service: An analysis of a ransomware affiliate…*. Intel471. Retrieved October 25, 2022, from https://intel471.com/blog/revil-ransomware-as-a-service-an-analysis-of-a-ransomware-affiliate-operation

Morgan, M. G., Zacharias, E. G., & Doddi, D. (2020). Significant Increase in Ransomware Attacks on Healthcare Industry—OCR Offers Guidance. *Computer & Internet Lawyer*, *37*(6). Legal Collection. https://proxy01.its.virginia.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&site=eds-live&db=lgh&AN=143053259

Niki, O., Saira, G., Arvind, S., & Mike, D. (2022). Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. *DIGITAL HEALTH*, *8*, 20552076221104664. https://doi.org/10.1177/20552076221104665

Riggi, J. (n.d.). *Ransomware Attacks on Hospitals Have Changed | Cybersecurity | Center | AHA*. Retrieved October 25, 2022, from https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed

Sumner, P., & Keenan, R. (2022). Ransomware Attacks on Healthcare Providers—What You Need to Know. *Journal of Health Care Compliance*, *24*(2). Business Source Complete. https://proxy01.its.virginia.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&site=eds-live&db=bth&AN=156264792

Tarabay, J. (2021). THE AGE OF RANSOMWARE. *Bloomberg Businessweek*, *4702*. Business Source Complete. https://proxy01.its.virginia.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&site=eds-live&db=bth&AN=150811282