REvil's Rise in Targeting The Healthcare Industry Through Ransomware

A Technical Report submitted to the Department of Computer Science

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

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

Connie Zhang

Spring, 2023

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

Briana Morrison, Department of Computer Science

REvil's Rise in Targeting The Healthcare Industry Through Ransomware

CS4991 Capstone Report, 2023

Connie Zhang
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
cz3vx@virginia.edu

ABSTRACT

The healthcare industry is becoming increasingly vulnerable to ransomware attacks making REvil, a rising threat actor group, a major threat to the health and privacy of patients and healthcare workers. The need to educate healthcare professionals and increase the availability of knowledge within the security realm inspired a whitepaper to dive into REvil's capabilities. To address this need, a team of cybersecurity experts and I constructed a virtual simulation environment to simulate attacks from REvil and display the potential impacts targeting the healthcare industry. Additionally, we used further literature review and gap-analysis to incorporate previous attacks and mappings to the MITRE ATT&CK matrix. Our paper detailed common techniques and tactics used by REvil from gaining initial access to exploiting victims for ransom. Additional research on REvil and an analysis of recent attacks should be updated to include the most recent findings of this threat actor group to further the understanding of their full capabilities.

1. INTRODUCTION

In 2021, the average cost of the direct impact of 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). Attackers use a variety of techniques to gain initial access and maintain control through a system undetected. Targeting critical systems, such as healthcare, works as a means to guarantee payment as they are heavily relied on in a functioning society, and have the potential to disrupt patients, doctors, and other healthcare workers.

Ransomware attacks have gotten increasingly common and damaging through the interconnected dependability on the internet. REvil, an upcoming ransomware-focused threat actor group, poses a great threat to the healthcare industry. They are known for performing organized attacks responsible for 75% of attacks on U.S. healthcare systems (Check Point Blog, 2021). The necessity of healthcare services gives attackers like REvil the authority to ask for more, feeding into a cycle of continuing attacks and weakening the ability of the healthcare sector to serve its purpose. Many healthcare systems also lack security awareness with outdated policies and applications, leading to uneducated users on exploitable systems.

The healthcare industry uniquely contains Personal Health Information (PHI), making the retrieval of information back from threat actors ever more important to protect the health and privacy of patients. Moreover, the healthcare industry relies on systems conducted through a network such as medical records, devices, and communication channels to function, meaning disruption to these systems could cause malfunctioning equipment, canceled appointments, and even pose life-threatening circumstances. As REvil develops into a sophisticated attacking organization and expands its work through Ransomware-as-a-Service, its damage will cascade throughout the healthcare sector, ultimately draining resources and causing delays in healthcare. Although some security policies are in place to mitigate any impact, further analysis of the technical tactics and common exploits performed by REvil is needed to ensure the protection of valuable assets and educate those in the healthcare and cybersecurity industries.

2. RELATED WORKS

MITRE (2022) proposed a publicly available ATT&CK knowledge base that provides common tactics and techniques utilized by threat actor groups. The model proposes an overall attack approach and philosophy as a means to educate those in the cybersecurity community. However, the knowledge base covers general attacks while my project expanded and mapped specific techniques that are commonly found in ransomware attacks conducted by REvil targeting healthcare vulnerabilities.

The Check Point Blog (2020) stresses the alarming increase of ransomware attacks on the healthcare industry committed by REvil. They emphasize the severity of these tailored attacks and the need to increase awareness and security in endpoint device management, educating personnel, and monitoring systems. This informed and scoped my project to the direct impact REvil could have on the healthcare industry and the objectives behind attacks.

Ghayoomi, et al. (2021) discussed an estimated 4.5 billion medical devices that rely on the Internet, which accounts for $6 billion annually, making the healthcare industry an extremely vulnerable and lucrative market to attack. They analyzed the potential impact of different sectors within the healthcare industry in conjunction with the resiliency and recovery strategies in place through a resource-constrained discrete-event simulation model. My project modeled a simulated environment similar to Ghayoomi, et al. (2021) to understand a potential response of the hospital, but further included specific pain points within the healthcare sector’s technology affected by a REvil attack.

According to Pears & Konstandintis (2021), an increase in social engineering and human-based vulnerabilities have contributed to the successes of ransomware threat actor groups. They proposed a list of actions for healthcare professionals to adapt to for securing future systems to serve as a solution to human led breaches, ultimately leading to a gain in confidence level in professionals. Although it is imperative to educate healthcare professionals, my project will broaden the scope to focus on technical and human-based intervention to further reduce vulnerabilities.

3. PROPOSED DESIGN

The method of a ransomware attack, along with specifications provided by the client and environment limitations contributed to the coverage of our whitepaper.

3.1 System Architecture

A typical ransomware attack consists of three major actors: attacker, victim, and the data that is compromised. This type of attack generally begins by gaining initial access to a system that a victim relies on for its data. An attacker can gain initial access through many methods. The techniques most commonly used by REvil include Drive-by compromises and Phishing attacks. After gaining access, attackers are given the opportunity to deliver malware to a system which typically locks critical files, allows attackers to gain higher access to a system, or causes outages and delays until a ransom is paid, causing significant damage. A hospital system functionally relies on the data exchange between doctors, nurses, patients, medical record systems, and devices in order to operate and provide proper treatment to patients. These technical systems include databases, web services, email content, or sensitive files, and when compromised, can lead to essential data being corrupted or exfiltrated.

3.2 Requirements

The requirements of this project were constructed by the content determined that would best aid a client undergoing a ransomware attack considering the system limitations in our research environment.

3.2.1 Client Needs

Our client's represented potential healthcare organizations that are major targets for ransomware attacks. Their needs were achieved through defining an agreed upon scope for the project. This included what to expect from ransomware attacks conducted by REvil and how to best prepare and prevent them moving forward. REvil was chosen as a subject to analyze due to its profound impact from previous attacks, and how little is known about the threat actor group. It was important for potential clients to understand the proper actions to take in assessing their security posture and knowing how common vulnerabilities apply in a healthcare environment.

3.2.2 System Limitations

The scope used to analyze the impact of REvil ransomware attacks on the healthcare industry is limited by the resources available at the time and the scale of which simulations were conducted. The team was only able to perform simulated attacks on some REvil techniques that were supported in the lab environment used. Additionally, it was hard to fully simulate a functioning hospital system to test the full impact of an attack. Therefore, certain tactics simulated may not show all of the damages done to a system.

3.3 Key Components

The paper was shaped throughout the process to cover important topics and expanded as the team encountered challenges.

3.3.1 Specifications

The whitepaper covered three main sections to achieve a comprehensive analysis of REvil as a ransomware threat actor and the impact it could have through a healthcare lens. The paper first introduced a typical workflow of REvil infiltrating a network. This section discussed commonly used techniques to gain initial access, maintain control, and ultimately compromise a system or exfiltrate data in exchange for a ransom on a large and critical scale such as a hospital system. Next, REvil's techniques were mapped against a well-known attack matrix to create a connection for cybersecurity professionals to recognize and protect against. The mapping contained a description of the general technique as well as how REvil specifically has used it, and what to expect in terms of changed functionality of a system or what data contents may be compromised.

3.3.2 Challenges

During our research collection, our team ran into the challenge of being able to demonstrate the severity of an attack in real time to our clients. Because our clients may not be familiar with REvil or technical attacks, it was important to show how a direct attack could impact their industry. The literature review gathered previous attacks and anticipated impacts of a ransomware attack by describing previously observed behaviors. However, being able to visualize and verify these actions was hard to accomplish through solely a literature review. Therefore, our team needed a solution that would accurately and clearly communicate what a direct attack from REvil would impact a hospital system.

3.3.3 Solutions

We conducted simulations through MITRE's internal lab on similar systems used in hospital in a Windows environment. These simulations revealed what certain attack techniques could do and showed expected outcomes of REvil techniques. For example, the responses for some techniques revealed locked files, disabled privileges, and showed alerts from the malware through a ransom note. These demonstrations supplemented the literature review conducted with active examples and actions REvil may implicate, allowing users to have a clear understanding of what to anticipate.

4. RESULTS

The completed whitepaper is available to the public for viewing, targeting healthcare professionals and the cybersecurity community. Publishing the paper enables us to reach a larger audience, and provide first steps towards mediation and initial awareness of this topic. REvil's impact and common techniques are shared in hopes that healthcare systems are updated to mitigate these attempts.

The paper covered 26 techniques in the categories of: Initial Access, Discovery, Defense Evasion, Privilege Escalation, Execution, Command and Control, Exfiltration, and Impact. Furthermore, it provided a number of mitigation and prevention techniques inclusive of analytic strategies and four defensive strategies. The collection of this research significantly reduces the effort needed by future victims of attack by compiling research from previous attacks common mitigation techniques into one document to aid the cybersecurity community.

5. CONCLUSION

Ransomware continues to threaten the health and safety of patients all over the world, with major threat actor groups growing stronger in resources and smarter in their attack techniques every day. Our project serves as a means to shed light on the capabilities and attack techniques conducted by REvil, and to show how destructive an attack could be through a deep analysis of previous attacks and carefully designed simulations. Our paper highlights the especially vulnerable areas of a hospital system that could guide life-saving actions when protecting hospital devices. This whitepaper is essential to all healthcare systems as it gathers together critical information from many sources about REvil into an informational document thereby distributing knowledge to the greater cybersecurity and healthcare communities.

6. FUTURE WORK

Further research can be conducted to refine our paper to reach its purpose to serve as an informational toolkit for healthcare and cybersecurity professionals. Continuing improvements on our whitepaper include the need to update the paper based on the most recent finding to ensure accuracy in our analysis and suggestions. Furthermore, expanding on additional variants or threat actor groups focused on ransomware as it relates to healthcare attacks would cover a larger scope of possible attacks that need to be prepared for.

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

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

Check Point Blog. (2020, October 29). *Hospitals Targeted in Rising Wave of Ryuk Ransomware Attacks*. Check Point Software. https://blog.checkpoint.com/2020/10/29/hospitals-targeted-in-rising-wave-of-ryuk-ransomware-attacks/

MITRE ATT&CK®. (n.d.). Retrieved February 23, 2023, from https://attack.mitre.org/

Morgan, M. G., & Zacharias, E. G. (n.d.). *Significant Increase in Ransomware Attacks on Healthcare Industry–OCR Offers Guidance*. The National Law Review. Retrieved February 23, 2023, from https://www.natlawreview.com/article/significant-increase-ransomware-attacks-healthcare-industry-ocr-offers-guidance

Pears, M., & Konstantinidis, S. (2021, May 5). *Cybersecurity Training in the Healthcare Workforce–Use of the ADDIE Model*. https://doi.org/10.1109/EDUCON46332.2021.9454062