Thesis Project Portfolio

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)

An Undergraduate Thesis

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

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

Connie Zhang

Spring, 2023

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

Introduction

The healthcare sector is the top target for ransomware threat actors, containing vulnerable assets, systems, and data that we rely on. 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. My technical capstone research is based on a summer internship where my team and I completed a Whitepaper that details the attack capabilities, techniques, and mitigation techniques of the upcoming ransomware attack group, REvil. Our research was directed to aid the healthcare industry in supporting a stronger security posture in response to REvil attacks. My STS research paper expands on the impacts of a ransomware attack on a healthcare system from the perspective of damage to medical devices, patients and staff, and the financial burden. Additionally, my research investigates policies and education strategies to suggest future implementations of secure practices in a healthcare organization.

Project Summaries

The technical portion of my thesis produced a publicly available whitepaper that targets the need to educate and spread awareness of the capabilities of REvil, one of the largest ransomware threat actors towards the healthcare community. The completed paper covered 26 common techniques in the categories of: Initial Access, Discovery, Defense Evasion, Privilege Escalation, Execution, Command and Control, Exfiltration, and Impact that were previously identified as REvil techniques. Additionally, our paper included attack simulations to show targeted communities what to anticipate from REvil. Furthermore, it provided several 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 and reveals common weaknesses to patch. My research 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.

My STS research draws attention to the disparity of cybersecurity knowledge needed to prevent attacks and emphasizes the need for enforcing security policies. I examined the reliance and interconnected relationships between patients, doctors, and data passed between medical devices to prove the profound impact an attack could incur revealing significant damage to all actors involved. My findings show the damage of an attack affecting all areas of a hospital ecosystem, as shifting relationships between medical devices, patients, and staff have life-threatening consequences. The current standings of security knowledge and implemented policies reveal a need for improvement in education through the partnership of healthcare workers and security professionals. Ensuring consistency in security across all facets will contribute to the confidentiality of patient data, availability of medical systems, and treatment integrity from doctors. It is important that healthcare and cybersecurity professionals take these factors into consideration when producing strong security plans for hospitals as they prove to have a very delicate and vulnerable system.

Conclusion

Completing my technical capstone during a previous internship heavily influenced my interest in analyzing the damage of a ransomware attack from a social and ethical point of view. My technical research focused on the ransomware threat actor group, REvil, examining the technical capabilities, threats, and targeted vulnerabilities to protect those in the healthcare space. My STS research builds off of this research from a different perspective through analyzing the impact and motivation of such an attack on all actors, human and non-human, within the ecosystem due to a ransomware attack. Not only does this perspective take into account the technical challenges due to an attack, but also investigates the social and financial implications during and post attack. Researching ransomware from a technical and social lens allowed for a holistic view on who and what are impacted, and a better understanding to protect our most important assets in healthcare.