Virtual Machine Malware Research Proposal

by

Soren Stauss

Submitted to the Department of Computer Science and Engineering

at the

UNIVERSITY OF MINNESOTA, TWIN CITIES

June 1, 2023 [Draft]

Abstract

Electronic health records (EHR) are the primary means of collecting and storing patient data in the United States. As of 2021, 96% of hospitals and 78% of private medical practices utilize EHR.[1] Healthcare organizations often use virtual servers, such as VMware ESXi, to offer a layer of protection against attacks on host machines which reach EHR. Using the ESXiArgs ransomware attack, the expected results of this study will show that this layer of security is largely ineffective and provides for clinicians and patients alike a false sense of security. The implication is that instead of focusing solely on perceived layers of security, protected health information (PHI) is better protected when malware itself is better understood by IT security staff. This is because by understanding the code, particularly when there are known patterns, IT staff will be better able to modify their security protocols rather than simply relying on virtual tools which have shown to present their own vulnerabilities.

Problem Statement

Background

Healthcare organizations, including hospitals, routinely utilize virtual machines to access and store critical clinical information which includes protected health information. A principal reason for this architecture is security, as it is traditionally believed that a virtual machine will protect the host machine from malicious malware. If the virtual machine is attacked by malware, including ransomware, the virtual machine can be dismantled and a new virtual machine can be created in its place without infecting the host machine. A series of attacks on virtual machines has shown this to be flawed, however, which places clinical data at significant risk.

This work follows the 2023 VMware ESXiArgs[2] server ransomware attack. In particular, we focus on continued VM server vulnerabilities, and their impact on healthcare IT, particularly the impact on calling electronic health records (EHR) and other health data.

Currently, the majority of EHR and clinical documentation containing protected health information (PHI) are accessed through virtual machine servers, presenting a cyber security risk for patient data in the United States and globally. Current cyber policies and procedures have shown to be inadequate against cyber attacks, but this is only a single defense. Historically, organizational IT teams have put a significant level of trust in virtual machines as a secure method to protect host machines and data.

This study will demonstrate the risk associated with VM architecture for healthcare information access to allow healthcare IT decision makers to assess the advantages and disadvantages of VM utilization, including the cost-effectiveness of maintaining VMs as a security measure. First, this study will analyze past cyber security incidents involving virtual machine client and server vulnerability exploitation which impacts host machines. Next, we will simulate new attacks and reveal how patched vulnerabilities are often incomplete, reverting the patched vulnerability to a zero day. The second part of this study will require a research lab environment which will be included in this proposal.

A malware R&D laboratory is critical to advancing research in various types of malicious software in order to defend critical systems, including healthcare. Behind this lab will be a team of University of Minnesota students and faculty researchers with diverse technical skills who are dedicated to research which will advance hardware and software testing, as well as write and test both new and existing malware in a controlled environment so patches and other malware

mitigating activities can be performed. This research will serve a significant security need, including healthcare information, biomedical devices, and other critical infrastructure.

Cyber vulnerability continues to be a significant threat to healthcare organizations as well as their patients. Using quantitative data and attack simulations, new and emerging threats will be highlighted and equip healthcare organizations to improve their security posture to protect their organization and their patients.

Hypothesis

We hypothesize that the use of virtual machines to access clinical information can compromise PHI security. Furthermore, patched VM vulnerabilities can be incomplete which allows an attacker to turn patched vulnerabilities back into a zero day, once again compromising the same machines with a similar or same attack.

Significance

The significance of this research is that it highlights malware vulnerabilities in healthcare settings which are undetected even if previously known, since vulnerabilities once thought to be patched by the software vendor turns out to contain other vulnerabilities which allow it to return to a zero day vulnerability. Furthermore, this study will serve as a proof of concept for an academic research laboratory, which is critical to understanding and mitigating this issue and ongoing security threats.

Methodology

In this project I propose to analyze malware code to discern patterns in code for attacking virtual machines as well as host machines. This will involve reverse engineering binary code into assembly language as well as low level human readable code, such as C++. It is expected that this research will give us a better understanding of whether virtual machines, notably virtual

servers, create a layer of security or have introduced a new vulnerability, thus placing PHI at risk.

Role of Researcher

In this project, I will be working under the supervision of my research supervisor, Professor Kangjie Lu. Professor Lu is an Associate Professor in the Department of Computer Science and Engineering. I will be analyzing the attack vectors which led to the ESXiArgs ransomware attack, and then write and analyze code to explore interactions between malware and virtual vs host machines. Furthermore, I will work with the CSE department and College of Science and Engineering to establish and build out a malware research lab where this and ongoing research will take place. Finally, I will work with Professor Lu to seek federal funding through the Defense Advanced Research Projects Agency (DARPA) and the National Science Foundation (NSF) for the research project and laboratory. I will also work with regional corporations and healthcare organizations to establish industry partnerships.

Other Insights

While this study is focused on healthcare organizations, we expect that this research will bring to light similar vulnerabilities and security issues in other critical sectors, such as utilities, finance, manufacturing, and academia.

Ethics Statement

This project does not include human subjects and will be conducted exclusively in a sandboxed environment, air gapped from the networks of University of Minnesota or any other network. We will not use any internet-facing networks during the course of this study.

References

1. **“**National Trends in Hospital and Physician Adoption of Electronic Health Records,” The Office of the National Coordinator for Health Information Technology, accessed May 23, 2023, https://www.healthit.gov/data/quickstats/national-trends-hospital-and-physician-adoption-electronic-health-records.

2. Hawkins, Edward, “VMware Security Response Center (vSRC) Response to ‘ESXiArgs’ Ransomware Attacks.” Last modified February 6, 2023. https://blogs.vmware.com/security/2023/02/83330.html