Virus Detection

Cristina Laing

Cybersecurity Principles

CYSE 600

August 6, 2021

Dr. George R. Mikulski

Author Note

This is my own work and has been done solely by me. This paper has been written for the Old Dominion University's CYSE 600 Cybersecurity Principles class and not used for any other purpose.

Cristina Laing

Abstract

This paper is an analysis of three different research papers on the topic of virus detection. The paper will start by giving a brief introduction on the topic of virus detection and its purpose. The introduction is followed by a summary of each of the three research papers analyzed. Then, an introduction to different virus detection methods will be explained as well gaps, loopholes, and overall vulnerabilities of each virus detection method. Lastly, this paper will state the solutions proposed by each research paper to compare.

Virus Detection

Introduction

A virus is a kind of program which can seriously infect any system (Chakraborty, 2017). Viruses are homogenous and are used for different malicious purposes. At a large scale, such as businesses, organizations, and governments, viruses can interrupt a whole system and halt productivity. At a smaller scale, for example, an individual's home computer viruses can be responsible for slow computer performance, erratic computer behavior, unexplained data loss, and frequent computer crash. Nowadays, data is the ultimate asset for individuals, businesses, organizations, and governments. However, as the popularity of the internet grows, so does the number of viruses being created. As a result, we are now in an arms race between the distributors of malware and those seeking to provide defenses (Carlin, Cowan, O'Kane, & Sezer, 2017). Unfortunately, lack of time, resources, and education have favored cybercriminals and their viruses.

Literature Review

There is hope due to the increase of attacks in the private and government sectors, monetary loss due to damages caused by viruses, and the media attention given to these attacks. As a result, organizations, businesses, governments, and universities have come together to quell these attacks. In this paper, we will review and discuss two different research papers on the topic of virus detection: (1) *Antivirus Security: naked during updates* and (2) *The Effects of Traditional Anti-Virus Labels on Malware Detection Using Dynamic Runtime Opcodes.* These two papers discuss virus detection from different perspectives bringing to light different issues and loopholes present in virus detection methods in use today.

(1) *Antivirus security: naked during updates*

The authors, Min, Varadharajan, Tupakula, and Hitchens, explain that attackers face two main hurdles when compromising a computer system. First, the attacker(s) needs to obtain temporary control over the target system (Min, Varadharajan, Tupakula, & Hitchens, 2014). Second, the attacker(s) needs to maintain or extended the control so that malware can achieve its goal (Min et al., 2014). However, both obstacles are getting harder for attackers to overcome due to improved security tools and implementations. Nevertheless, the authors warn that attackers have noticed and therefore shifted their method of entry and modified virus code. Attackers are resorting to staged malware; in other words, instead of creating a complete virus that enters the system, maintains control of the system, and harms the system; attackers divide the virus into stages. The first stage is entering a system undetected and modifying the system to allow entry for more viruses or the next stage of the attack. Attackers are also waiting for a window of vulnerability in anti-virus software. All anti-virus software must be updated frequently to protect their system with up-to-date definitions and engines (Min et al., 2014). During updates, the anti-virus software is partly or totally deactivated, leaving the system vulnerable to attacks.

(2) *The Effects of Traditional Anti-Virus Labels on Malware Detection Using Dynamic Runtime Opcodes*

The authors Carlin, Cowan, O'Kane, and Sezer focus on weaknesses found throughout different anti-virus software. The authors state that the main problem that anti-virus programs face in detecting preventing, and mitigating malware is the virus's ability to change signature, polymorphic nature. Therefore, the authors call for new anti-virus strategies that are immune to modern obfuscation methods. The authors also propose making a new database from which anti-virus gathers information about viruses that is capable of subdivision along with several variables, for example, type, family variant, file size, runtime, payload, attack vector, creation, obfuscation-type while retaining enough per sub-category (Carlin et al., 2017). Lastly, the authors suggest using virtualized dynamic analysis in conjunction with machine learning techniques for the effectiveness of classification per type of malware, resulting in better databases that will improve detection.

Discussion

Both papers are well researched and bring to light important issues concerning anti-virus software, from different perspectives. One paper is concern with vulnerability due to anti-virus downtime necessary for updates and the second paper is concern with vulnerabilities due to outdated or improperly organized databases. Both papers describe the problems and also come up with suggestions for solutions and yet all authors acknowledge challenges. For example, in *The Effects of Traditional Anti-Virus Labels on Malware Detection Using Dynamic Runtime Opcodes*, challenges included: the extensive detailed work it would take configuration of a host environment capable of automated dataset creation which captures the dynamic runtime of both benign and malicious software (Carlin et al., 2017). Generation of a dataset sufficient in size and depth to allow sub analyses along specific parameters (Carlin et al., 2017). Improve data mining and machine learning techniques already in use to extract meaningful information (Carlin et al., 2017). And explore malware types and the advantages of investigating per malware type (Carlin et al., 2017). In contrast, *Antivirus security: naked during updates*, faces the challenges of there being no limitation on the range of vulnerabilities related to updates, due to traditional implementation flaw, a fundamental design mistake or a logic fault.

Summary

It is important to stress that it is essential that at least one anti-virus software is present on every computer system, even if the anti-virus software is somewhat imperfect (Min et al., 2014). Both papers point out vulnerabilities in anti-virus software, yet all authors agree that imperfect anti-virus protection is better than none. Mainly because anti-virus protection and other security tools make it more difficult for attackers to breach a system, the papers focus on different areas of vulnerability in the context of anti-virus. All authors agree that more research in the field is needed and should be further invested. In addition, both papers suggest basic security training for regular users to reduce the chances of successful attacks and speed up detection. The papers analyzed here also give examples of real-world attacks where attackers have exploited the vulnerabilities described in the research. Which is an excellent tactic because it proves the authors' research is valid and relevant. Both papers are great examples of the research taking place in the anti-malware/virus detection research community, which strives for faster detection, prevention, and mitigation of virus attacks.

References

Carlin, Domhnall, Cowan, Alexandra, O'Kane, Philip, & Sezer, Sakir. (2017). The Effects of Traditional Anti-Virus Labels on Malware Detection Using Dynamic Runtime Opcodes. IEEE Access, 5, 17742-17752.

Min, Byungho, Varadharajan, Vijay, Tupakula, Udaya, & Hitchens, Michael. (2014). Antivirus security: Naked during updates. Software, Practice & Experience, 44(10), 1201-1222.