Chapter 9
Advancements in Ransomware Detection and Prevention Techniques

Jayant Verma
VIT Bhopal University, India

D. Lakshmi
https://orcid.org/0000-0003-4018-1208
VIT Bhopal University, India

ABSTRACT

In today's world of ubiquitous sensors and intelligent devices, cyber incidents and crime have peaked. Ransomware poses a danger to the security of a computer system. Ransomware attacks have significantly increased over the past ten years. Inevitably, this has become the talk of the town quite extortionate due to considerable consequential damages and obstruction in sectors such as healthcare, insurance, business, and education. Automatic detection and prevention of ransomware attacks is a crucial aspect of cybersecurity. Various malware detection methods have still been unturned as new parts of malware emerge. In the last two decades, several machine-learning algorithms and behavior-based techniques have been developed to identify ransomware anomalies. This chapter provides a long-term understanding of ransomware and discusses current methods and advancements in ransomware detection and the phases of a ransomware attack. The authors also highlighted the brief history of ransomware from 1989 when the first ransomware was discovered to the recent year 2023.

DOI: 10.4018/979-8-3693-2185-0.ch009

INTRODUCTION

Nearly every member of society has been using the internet for every aspect of daily life in recent years. Because internet usage is so ubiquitous today, including net banking, health care transactions, and e-commerce, it would be impossible to live without it. Although it has rapidly gained popularity, its rapid adoption has also made it vulnerable to misuse and abuse. Attackers are conducting the majority of cyber-attacks with malicious software. Software that deliberately executes malicious payloads on target machines is considered malware. There are different types of malware, Adware, Botnets, Spyware, Ransomware, Rootkit, Trojan Horse, viruses, Worm.

Over the past few years, ransomware has caused significant damage to many sectors such as organizations, the military, industries, education, etc. There have been reports of ransomware attacks since the end of the 1980's. The first ransomware was known as AIDS Trojan-PC Cyborg. The concept is nothing new (Kharraz et al., 2016), but it gained popularity because of its increasing number of attacks in today's world. The attack can be undertaken via various social engineering techniques, which are done by tricking users into clicking a malicious link in an email or another way. Ransomware targets a computer by infecting it with malicious code and spreading rapidly to encrypt the data of that particular machine. As a result, the malware makes the user's files inaccessible, and because of this, attackers demand ransom (money) from them for the files to be unencrypted. In most cases, Bitcoin or other Blockchain-based currencies are used for payment; the anonymity of Bitcoin makes it a popular choice for attackers as it is difficult to trace the identity of the attackers who use it. **There are three main types of ransomware:**

(a) **Locker Ransomware** - An infected individual sees a lock screen with a ransom message and instructions for decrypting the system. Locker ransomware stops the user from using the machine until the ransom amount was not paid. Users can recover the locked files by physically moving the hard drive to a safe system. The sequence of ransomware attack is shown in the Figure 1.