Chapter 7

Demystifying Ransomware: Classification, Mechanism and Anatomy

Aaeen Naushadahmad Alchi
https://orcid.org/0000-0002-0802-5363
Gujarat University, India

Kiranbhai R. Dodiya
https://orcid.org/0009-0001-9409-7303
Gujarat University, India

ABSTRACT

Malware, classified as ransomware, encrypts data on a computer, preventing individuals from accessing it. The intruder then demands a ransom from the user for the password that unlocks the files. Recent cyberattacks against prominent corporate targets have increased the extensive media attention on ransomware. The primary reason for computer intrusions is financial gain. Ransomware targets individual owners of information, keeping their file systems captive until a ransom is paid, compared to malware, which permits criminals to steal valuable data and then use it throughout the digital marketplace. Ransomware's terrifying complexity level heralds a paradigm shift in the cybercrime ecosystem. Ransomware has become more mysterious, with some latest forms working without ever connecting to the Internet. In this chapter, the authors will discuss the overview of ransomware, the history and development of ransomware, some of the famous cases, the anatomy of ransomware attacks, types of ransomware attack vectors, and the prevention of such kinds of attacks in cyberspace.

DOI: 10.4018/978-1-6684-8218-6.ch007

1. LET US KNOW ABOUT RANSOMWARE

Ransomware is wicked software that encrypts a victim's documents, making them unreachable, and demands a ransom payment in exchange for the decryption key. The price of a cryptocurrency like Bitcoin and the ransom amount are often relatively high. Ransomware can be delivered through various means, such as malicious email attachments or software vulnerabilities, and can significantly impact individuals and organizations. It is a cyber-attack and can cause serious business interruption and data loss. (FinCEN, 2021)

2. HISTORY AND DEVELOPMENT OF RANSOMWARE

Ransomware has been around in various forms since the late 1980s, with the first known instance being the "AIDS Trojan", distributed on floppy disks in 1989. However, it was not until the mid-2000s that ransomware began to gain widespread attention as a serious cyber threat. Early versions of ransomware typically just locked the victim's screen and displayed a message demanding a ransom payment, but over time the malware has evolved to include encryption of files, making them inaccessible until paid the ransom.

In the 2010s, ransomware began to be distributed on a large scale via email phishing campaigns and exploit kits. The use of cryptocurrency as a means of payment also became more common, providing a way for attackers to receive the ransom payment while remaining anonymous. The malware also began targeting individuals, businesses, healthcare organizations, and government agencies(CryptoDeFix, n.d.).

In recent years, ransomware has become even more sophisticated, with some variants using double extortion techniques, not only encrypting the files but also exfiltrating sensitive data and threatening to release it if the ransom is unpaid. In addition, some ransomware can spread laterally across a network, encrypting multiple machines and causing widespread disruption.

Overall, ransomware has evolved from a nuisance to a severe cyber threat that can cause significant damage to organizations and individuals.

2.1 History of Ransomware

One of the first examples of this type of malware was the AIDS Trojan, discovered in 1989. The malware encrypted the victim's files and demanded payment for the decryption key.