Chapter 6
Introduction to Ransomware

Qasem Abu Al-Haija
https://orcid.org/0000-0003-2422-0297
Princess Sumaya University for Technology, Jordan

Noor A. Jebril
Princess Sumaya University, Jordan

ABSTRACT

Ransomware can lock users' information or resources (such as screens); hence, authorized users are blocked from retrieving their private data/assets. Ransomware enciphers the victim's plaintext data into ciphertext data; subsequently, the victim host can no longer decipher the ciphertext data to original plaintext data. To get back the plaintext data, the user will need the proper decryption key; therefore, the user needs to pay the ransom. In this chapter, the authors shed light on ransomware malware, concepts, elements, structure, and other aspects of ransomware utilization. Specifically, this chapter will extend the elaboration on the ransomware, the state-of-art ransomware, the ransomware lifecycle, the ransomware activation and encryption processes, the ransom request process, the payment and recovery, the ransomware types, recommendation for ransomware detection and prevention, and strategies for ransomware mitigation.

1. INTRODUCTION

In the last years, ransomware was grown very quickly, with many disturbing trends pointing to effective and targeted attacks against either organizations or individuals. These profiteering attackers indiscriminately aim at public and private sector entities for maximum gain (Bajpai & Enbody, 2020).

DOI: 10.4018/978-1-6684-8218-6.ch006

The word ransomware is derived from "ransom" and "malware". Ransom is described as "money paid to release a person who has been captured or abducted" and as "paying to return or required for the free of a person or thing from a vanishment". The word "malware" means malicious software (Ali, 2017) since attackers use it maliciously. Finally, ransomware is a sort of malicious software that applies encipherment as a main weapon (Glassberg, 2016).

O'Gorman and McDonald (2012) gave a fuller description as "a class of malicious software that, when run, disrupts computer functionality in some way. The ransomware shows a message demanding payment to retrieve functionality. This definition illustrates ransomware when it disrupts computer functionality and is later called an "extortion racket." Still, there is no specific information about paying the ransom in exchange for keeping the computer ransom. In other cases, ransomware can do certain harm to computer data files. Although it can access any file on a computer, ransomware often aims at certain types of files (O'Gorman & McDonald, 2012). Luo and Liao (2007) showed that ransomware targets files with the following file name extension: .txt, .doc, .rft, .ppt, .cbm, .cpp, .asm, .db, .db1, .db1, .dbx, .cgi, .dsw, .gzip, .zip, jpeg, .key, .mdb, .pgp, and .pdf.

The Cyber Threat Alliance provided the most integrated meaning for the ransomware. This alliance is a group of cyber security companies formed in 2014 to track cyber threats. In its first report published in 2015, the Cyber Threat Alliance (2015) gave the following definition of ransomware:

Ransomware is a kind of malware that encrypts the victim's files and then orders paying for the key that enables decrypting mentioned files. When ransomware is first installed on a victim's device, it usually aims for critical files such as important financial data, business records, databases, personal files, etc. Personal files, such as photos and home movies, may have sentimental value to the victim.

Since then, the attack has become automated and professional. It is considered very profitable, with past damages estimated at hundreds of millions of dollars annually. For example, the harm from one type of ransomware, CryptoWall3, was estimated to be more than $320 million in 2015 alone (Cyber Threat Alliance, 2015).

Consumers are believed to be the most common victims of ransomware (Symantec, 2017; Kaspersky, 2016). While most attacks are believed to be untargeted, consumers are often less likely to have robust security, which increases the likelihood of dropping victim to an attack (Symantec, 2017). However, regarding the damage that ransomware can cause, relatively little is known about the spread and characteristics of such attacks in the general population. Reliable estimates of ransomware prevalence are essential to understanding the nature of the threat landscape today and for long-term comparison and analysis.

Many government and industry organizations and researchers tried to document the phenomenon but results often needed to be more consistent. This is largely due

Related Content