The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges

[1]Samar Kamil
Department of Computer Science and Information Systems,
Al-Mansour University College
Baghdad, Iraq
Samarkamil2021@yahoo.com

[2]Siti Norul, Huda Sheikh Abdullah
Center for Cyber Security, Faculty of Information Science & Technology,
Universiti Kebangsaan Malaysia
Bangi, Malaysia
snhsabdullah@ukm.edu.my

[3]Ahmad Firdaus
Faculty of Computing, College of Computing and Applied Sciences,
University Malaysia Pahang, Pekan, Pahang Darul
makmurfirdausza@ump.edu.my

[4]Opeyemi Lateef Usman
Department of Computer Science, Tai Solarin University of Education,
Ogun State, Nigeria
usmanol@tasued.edu.ng

2022 International Conference on Business Analytics for Technology and Security (ICBATS) | 978-1-6654-0920-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICBATS54253.2022.9759000

***Abstract*— Cybersecurity is important in the field of information technology. One most recent pressing issue is information security. When we think of cybersecurity, the first thing that comes to mind is cyber-attacks, which are on the rise, such as *Ransomware*. Various governments and businesses take a variety of measures to combat cybercrime. People are still concerned about ransomware, despite numerous cybersecurity precautions. In ransomware, the attacker encrypts the victim's files/data and demands payment to unlock the data. Cybersecurity is a collection of tools, regulations, security guards, security ideas, guidelines, risk management, activities, training, insurance, best practices, and technology used to secure the cyber environment, organization, and user assets. This paper analyses ransomware attacks, techniques for dealing with these attacks, and future challenges.**

Keywords—cybersecurity, cyber-attacks, security, Ransomware

I. INTRODUCTION

The Internet is currently the fastest-growing infrastructure. In today's technological world, many modern technologies are changing the face of human activities. However, we cannot adequately protect our personal information due to these emerging innovations, and cybercrime is becoming more prevalent by the day. Today, more than 60% of all business transactions are conducted online. Hence, ensuring transparency and the highest level of security is a major problem.Consequently, cybersecurity has become a major concern. The scope of cyber security includes protecting information in the IT sector and many other areas such as cyberspace [1][2].

This work was supported by Ministry of Higher Education, Malaysia under research LRGS-1-2019-UKM-UKM-2-7.

According to Brewer [3] the term "***ransomware***" is derived from the words "*ransom*" and "*malware*". It is a significant factor contributing to the rise in cyber-attacks that include the ability to profit from victims. Meanwhile, Noubir believes that cybercriminals had a difficult time profiting from attacks in the past, but that has changed. Ransomware attacks, or attackers who gain access to a victim's data, encrypt it, and demand a ransom, are becoming increasingly popular among cybercriminals [4]. Ransomware refers to a type of virus that demands payment for a hacked service. The most common ransomware heavily employs file encryption as a method of extortion. They essentially encrypt data on victims' hard drives before demanding a ransom to unlock them [3]. According to Richardson and North [19], Ransomware is a growing threat to personal and corporate data files. It encrypts data on an infected machine and keeps the secret key to decrypt the contents until the victim pays compensation. Every year, this virus causes damage worth hundreds of millions of Dollars. Consequent upon the large sums of money that must be paid, new versions emerge on a regular basis. This enables the avoidance of security software and other intrusion prevention techniques [5].

Ransomware has been one of the most significant cyber frauds that have affected businesses in recent years. Indeed, the FBI predicts that ransomware will cause $1 billion in damages in 2016. Ransomware is a type of malicious software that allows a hacker to restrict access to vital information of a person or business and then demand payment to remove the restriction. Encrypting critical data on a computer or network is the most common type of restriction nowadays. It primarily allows the attacker to keep user data or a system backup [6].

Therefore, the objective of this study is to conduct a review of phases of critical ransomware attacks, discuss some techniques for dealing with them, and highlight future challenges.

II. PHASES AND TECHNIQUES OF RANSOMWARE

A ransomware attack occurs in stages, depending on whether it is a mass deployment or a targeted attack. Recognizing and comprehending what happens at each stage, as well as the compromise indicators (IOC) to be identified, increases the likelihood of successfully defending against or at least mitigating an attack. [7]. The phases and techniques of ransomware attacks are summarized below:

1. *Exploitation and infection:* For this phase to be successful, the dangerous ransomware must be executed on a machine. This is frequently accomplished through an infected email or vulnerabilities, a toolkit for the exploitation of security vulnerabilities for malware spread in software programs. These kits are designed for

978-1-6654-0920-9/22/$31.00 ©2022 IEEE