Chapter 3
The Age of Ransomware: Understanding Ransomware and Its Countermeasures.

Muhammad Ubale Kiru
https://orcid.org/0000-0002-7750-7649
Universiti Sains Malaysia, Malaysia

Aman B. Jantan
Universiti Sains Malaysia, Malaysia

ABSTRACT

This chapter focuses on the world's most frightening cybersecurity threat known as ransomware. Experts popularly describe ransomware as scareware that makes data and resources on a victims' computers inaccessible and forces the victims to pay a ransom with bitcoins or through other means by frightening and intimidating them. Ransomware these days needs no introduction. The perpetrators behind ransomware have done more than enough damage to critical infrastructures and collected billions of dollars from victims across the world and are still collecting. As such, this research aims at uncovering the underlying mysteries behind the sudden growth and popularity of ransomware through the in-depth study of literature and efforts made by experts globally in understanding ransomware and how to fight and stop it. Moreover, the research seeks to bring together the collective professionals' views and recommendations on how to set up strategic defense in-depth for fighting against ransomware.

INTRODUCTION

Ransomware is popularly described as a type of malware that makes a file on a victim's computer or device inaccessible and then demands the victim to pay ransom mostly in the form of bitcoin or other means of payment to regain access to the hijacked system (Micro, 2017). However, Liska and Gallo (2017) describe ransomware as a new type of extortion, hence describe it as a criminal practice for obtaining something especially money or its equivalence from an individual or institution through coercion or threats. Hackers and people with malicious intent are responsible for spreading ransomware. However, we know from

DOI: 10.4018/978-1-7998-7705-9.ch003

experience that employees also contribute to the spread due to human error and or ignorance caused by lack of awareness (Fimin, 2017). Some of the conventional methods of spreading ransomware include exploiting system's known or unknown vulnerabilities or by visiting compromised sites or deep webs.

Studies suggest that the sudden rise of ransomware attacks recently is a signal that ransomware has come back with full force in both complexity, impact and size (Downs, Taylor, & Whiting, 2017). The year 2017 was the year history will never forget as per as internet security breach is concerned. It was the year in which the world saw some of the most dangerous attacks in the history including WannaCry pandemic, Petya, NotPetya, Cerber, Cryptomix, Locky, CrySis and many others. The aforementioned ransomware attacks were massive global ransomware attacks that mostly affect Windows operating systems that were unpatched or unsecured. More importantly, the WannaCry attack became prominent following the leaked exploit kits which were stolen from the United States NSA by the infamous group known as 'Shadow brokers' which opens pandora's box for other variants of ransomware to be created and eventually affected thousands of devices across the globe. (Barracuda, 2017). These events led different social media observers and professionals in various domains to name 2017 as *the year of ransomware* (Cabaj, Gregorczyk, & Mazurczyk, 2017).

The damages erupted by ransomware did not catch much attention until recently when hundreds of companies and security agencies across the world have begun to cry out (Brodsky, 2017). So far, the popular variant known as WannaCry had rapidly spread to around 200,000 to 300,000 machines in over 150 countries across the globe since its first appearance (Yaqoob et al., 2017); making it the world's largest attack in history if measured in terms of wide coverage, complexity and impact. Earlier in 2016, the FBI reported that over $206 million was paid to ransomware criminals in the first quarter of 2016. In another report by the United States Department of Justice, there are over 4000 ransomware attack reports per day, and that every month new variant of ransomware is being produced, which makes it more likely to increase with 100% by Q4 of 2018 (Harpur, 2017). Perhaps, the emergence of IoT devices has also contributed as well as accelerate the wide spread of ransomware and the modern security challenges we are facing today (Yaqoob et al., 2017). The vast availability of devices on the internet has open access to all perpetrators who have malicious intent to start ransomware campaign at a massive scale.

The question many people keep asking is why is ransomware prevalent and unbeatable in every part of the world? The reason is that antivirus and anti-malware are no longer capable of detecting ransomware because modern ransomware use polymorphism and machine learning to avoid being detected. Secondly, the advent of Ransomware as a Service and the Exploit kits as a service in black markets make it even more difficult to deal with the situation. With RaaS, anyone including script kiddies can lay their hands on ransomware codes and reproduce their own. According to MacAfee Lab (2017), the writers of 'Cerber' (one of the most dangerous ransomware family) release a new variant of ransomware every 8 days on average, selling with bonuses and offers of 20% discount (Ashford, 2015; Singh, 2017).

Having said that, the objectives of this research include identifying new trends in ransomware attacks, the root causes of the attack, methods of the attack, mode of operation, attack vectors, and to identify popular suggestions given by experts on how ransomware attacks can be dealt with professionally using the simplest, cost-effective and most successful techniques for mitigating ransomware attacks. Other objectives include identifying the most suitable approach for ransomware mitigation as well as exposing and uncovering the mystery of ransomware to the users so that they become aware of how to recover in the aftermath of the attack. To break down these information, the sections are arranged as follow: Introductory section gives an overview on the focus of the entire research, a literature review section which comprises of ransomeware timeline, types of ransomware, mode of operation and other