Chapter 10
Global Wannacrypt Ransomware Attack:
Tackling the Threat of Virtual Marauders

Benjamin Enahoro Assay
Delta State Polytechnic, Nigeria

ABSTRACT

Cyber-attacks have become a global phenomenon that organizations, government agencies, and business entities have to contend with as cyber criminals frequently target their operations. One such cyber-attack is the Wannacrypt ransomware that was unleashed on the global community in early May 2017 with a resultant devastating effect. The attack, described as the largest in the history of the internet, disrupted major organizations and affected over 200,000 computers in 150 countries. It is against this backdrop that this chapter examines the issues and trends in the Wannacrypt ransomware attack and recommends ways to avert future occurrences.

INTRODUCTION

There is no doubt that cyberspace has become a battle ground for the launching of all sorts of attack. Even the most powerful nations of the world have moved their battle turfs from mortar to this notional environment in which communication over computer networks occur. They now engaged in cyberespionage (Rubenstein, 2014 p.1), targeting classified data from government agencies, circumventing the system, and getting the data for profit, thus raising concerns about cybersecurity.

Many countries have been caught in the web of cyberattacks orchestrated by nation-states, organizations, groups or individuals who deliberately target computer information systems, infrastructures, computer networks, and/or personal computer devices to commit malicious acts for personal objectives (Matusitz, 2005 p.137). Over the years, experienced cyber terrorists who are skilled in hacking have caused massive damage to government systems, hospital records, and national security programs leaving countries, communities or organizations in turmoil and in fear of further attacks (Laquer, Smith, &

DOI: 10.4018/978-1-5225-5927-6.ch010

Spector, 2002 p.52). The objectives of such terrorists may be political or ideological since this can be considered a form of terror (Indian Council of World Affairs, 1986 p.122).

In the last few years, there has been much concern from government and media sources about potential damage that could be caused by cybercriminals, and this has prompted efforts by several government agencies such as the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency (CIA) to put an end to cyber attacks and cyber terrorism (Laquer, Smith, & Spector, 2002, p.53). Cyberattackers are driven by several reasons. Andreasson (2011, p. xiv) averred that the reason for non-politically motivated attacks is generally financial, and most attacks are considered as cybercrime. Other attacks, as Gandhi et al. (2011, p.28) put it, are propelled by deeply-rooted socio-cultural issues. However, Shakarian et al. (2013, p.62) noted that in many cases, the real purpose and primary objective of a cyberattack may be hidden or obscured even if the attacker claims responsibility.

Cyberattack can range from installing spyware on a personal computer, spreading viruses or worms, to attempt to destroy the infrastructure of entire nations. Of late, networks and computer systems worldwide have become susceptible to attacks by all kinds of malware. Some common threats, according to Williams and Sawyer (2015, p.347), are "denial-of-service attacks; viruses; worms; trojan horses; rootkits and backdoors; blended threats; zombies; ransomware; and time, logic, and email bombs".

Cyberattacks have become increasingly sophisticated and dangerous as stuxnet (Karnouskos, 2011, p.4490) and Wannacrypt ransomware worm have demonstrated. The Wannacrypt ransomware worm was unleashed on the global community on 12 May 2017 with devastating effect. Wannacrypt ransomware was described as the largest global ransomware attack in Internet history. The Register, an online publication, said the Wannacrypt ransomware worm, also known as Wannacrypt or Wcry, exploded across 74 countries infecting hospitals, universities, Germany's rail network Deutsche Bahn, Spanish telecommunications operator Telefonica, US logistics giant FedEx and Russia's interior ministry, and more organizations. Bob Wainwright, head of European Union's law enforcement agency, Europol, described as the attack as 'unprecendented' in its reach, with more than 200,000 victims in at least 150 countries (The Register, 2017).

The ransomware took over users files and demanded US$300 (£230) in bitcoin to restore them. Elliptic Labs which tracks illicit use of the Internet or digital currency Bitcoin disclosed that about US$50,000 (£39,000) was paid after it was unleashed globally (Bitnewsbot, n.d). However, the ransomware said the cost would double after three days, so the payments might have increased. It threatened to delete files within seven days if no payment was made. The Wcry attack has come and gone but one cannot rule out the possibility of future attacks that could be more devastating. Most of the countries that were victims saw the attack coming, but they were not sure of when it would occur hence they appear not to be prepared. Computer giant, Microsoft said the attack, which affected hundreds of thousands of computers, should serve as a wake-up call (Microsoft, 2017).

The focus of this chapter therefore is how to tackle the threats of virtual marauders in order to stem the tide of global cyberattacks. The objectives of the chapter are the following:

1. To examine the issues surrounding the Wannacrypt ransomware global attack
2. To identify the lessons from the wannacrypt ransomware global attack.
3. To stress the need for governments, institutions and organizations to increase the defense mechanism against vulnerabilities.
4. To come out with recommendations on how to prevent and/or minimize the impact of future attacks.