Chapter 49
Advanced Threat Detection Based on Big Data Technologies

Madhvaraj M. Shetty
Mangalore University, India

Manjaiah D. H.
Mangalore University, India

ABSTRACT

Today constant increase in number of cyber threats apparently shows that current countermeasures are not enough to defend it. With the help of huge generated data, big data brings transformative potential for various sectors. While many are using it for better operations, some of them are noticing that it can also be used for security by providing broader view of vulnerabilities and risks. Meanwhile, deep learning is coming up as a key role by providing predictive analytics solutions. Deep learning and big data analytics are becoming two high-focus of data science. Threat intelligence becoming more and more effective. Since it is based on how much data collected about active threats, this reason has taken many independent vendors into partnerships. In this chapter, we explore big data and big data analytics with its benefits. And we provide a brief overview of deep analytics and finally we present collaborative threat Detection. We also investigate some aspects of standards and key functions of it. We conclude by presenting benefits and challenges of collaborative threat detection.

INTRODUCTION

In past few years, increase in the number of network intrusions has become severe threat to the safety and privacy of computer users. Billions of malicious cyber attacks are reported in each year (Fossi et al, 2011; Wood, et al, 2012). These attacks are becoming more stealthy and advanced, driven by an "underground economy" (Fossi et al, 2008).. Today hackers not only collecting private information from the compromised nodes, but also they are using these nodes to launch attacks such as distributed denial-of-service (DDoS) attacks. As a defence to these attacks, Intrusion Detection Systems (IDS) are used widely. These systems identify intrusions by comparing observable behavior against suspicious

DOI: 10.4018/978-1-7998-2466-4.ch049

patterns. Traditional IDSs can monitor activities on a single host or network traffic in a sub-network only. They do not have capabilities of a global view of intrusions in a network; therefore it is not effective in detecting new or unknown threats (Fung & Boutaba, 2013).

The rest of this chapter is organized as follows: firstly, provides background about cyber threats. Secondly, introduces big data with its analytics while deep learning concepts are presented thirdly. Fourthly threat detection with collaborative method explained with its benefits and challenges. Finally, the chapter conclusion is presented.

BACKGROUND

At the recent World Economic Forum (WEF) 2016, the growing number of cyber attacks was a major topic of concern. According to its 11th annual global risks report, cyber-attacks are ranked in the list of top ten threats in 140 economies ("The Global Risks" 2016). Failure in addressing and understanding these cyber attacks could affect economic sectors, national economies and global enterprises. Most of the firewall and other network-based security products provide mature and robust logging capabilities. Since the perimeter security is not enough, most of the security programs start with analyzing logs from the devices at the edge of the network. Nowadays most of the hackers of cyber conflicts are well organized with specific objectives, goals and having strong teams that are heavily funded. They are targeting information and communication systems of industrial, government, military and other private organizations. Also they are willing to use any amount of money, time to become expertise to reach their goals.

So understanding the limitations and problems of current technologies facing against advanced persistent threats (APTs) is important. APTs are significantly different from traditional attacks due to their own characteristics (Virvilis et al, 2014).

- APTs can bypass the majority of network intrusion detection systems and signature-based end points because they are using zero-day.
- The time taken by these attacks is outside the limited window of time of these detection systems due to the fact that they are generally spread over a wide period of time.
- Attackers are willing to spend significant time on focusing a particular target and explore all possible attack paths until they manage to overcome its defence.
- Attacks are highly selective. Targeted victims are selected very carefully, usually departments of an organization which are less likely to identify and report an attack and are nontechnical.
- Based on the analysis of the major APT attacks, it is observed that they are well-supported by nation-states that have significant capabilities enabled (covert physical access, manufacturing, intelligence collection) for cyber-attacks.

Due to these characteristics, present solutions of cyber security will fail to provide an effective defence against such attacks. Signature-based approach is used most widely used in intrusion detection. It is a simple testing methodology using known attack patterns where detection is based on small variations of attack patterns. But it has substantial limitations in intrusion detection systems against advanced persistent threats.