Chapter 6
Malware and Anomaly Detection Using Machine Learning and Deep Learning Methods

Valliammal Narayan
Avinashilingam Institute for Home Science and Higher Education for Women, India

Barani Shaju
Avinashilingam Institute for Home Science and Higher Education for Women, India

ABSTRACT

This chapter aims to discuss applications of machine learning in cyber security and explore how machine learning algorithms help to fight cyber-attacks. Cyber-attacks are wide and varied in multiple forms. The key benefit of machine learning algorithms is that it can deep dive and analyze system behavior and identify anomalies which do not correlate with expected behavior. Algorithms can be trained to observe multiple data sets and strategize payload beforehand in detection of malware analysis.

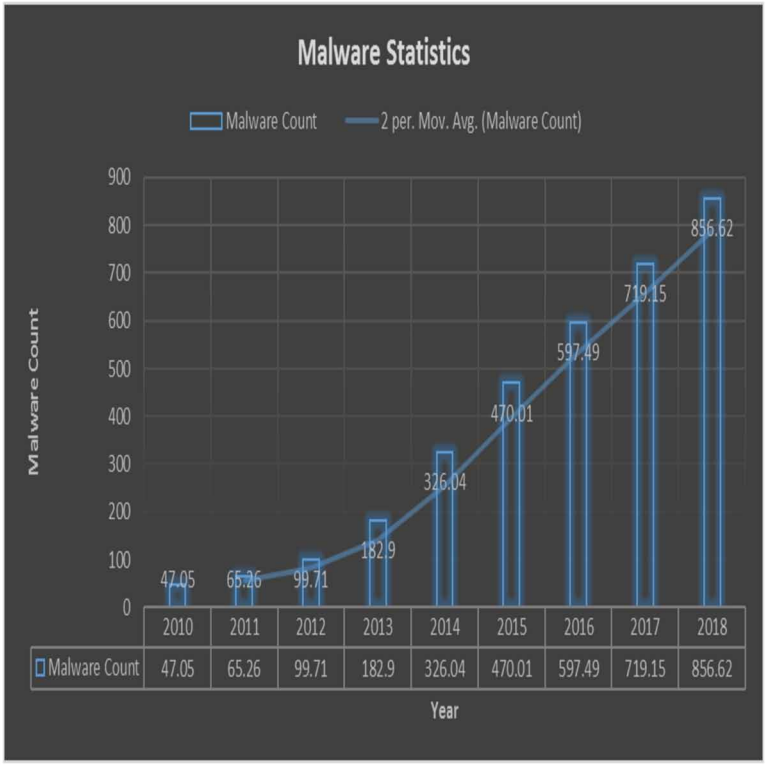
INTRODUCTION

Today, technology has become most essential part of our life. Internet usage has grown rapidly for the past years. Internet has brought about a new revolution in the fields of computing and communicating technology as it connects billions of infinitesimal devices. Potential intelligent support is provided by internet and the limitations of workplace is exempted using the wireless network providing excess mobility and flexibility over the conventional networks (Altaher. A, 2016). The sensitive information can be exposed by the transactions which were performed using the internet. Apart from the benefits of internet there are some drawbacks too like all our records, personal as well as professional, banking, medical, passwords, communication etc. can be made easily available to the antagonists using various illegal techniques and can finally receive our complete information, misuse our records imprecating the transactions which are online.

In the year 2018, the number of internet users has significantly increased. There are about 55.1% internet users as compared to the world population in table as Figure 1.

DOI: 10.4018/978-1-5225-9611-0.ch006

Figure 1. Tabulation and graph on malware statistics



Definition

Malware: It is a term used to describe malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software (Bhattacharya A, 2017). Inside the system, malware can do the following access:

Malvertising: This is the usage of web-based exposing to stretch malware. It ordinarily includes infusing malware-loaded commercials into genuine web-based publicizing systems and website links.

The number of cyber attacks has grown gradually during the last few years. In Figure 2, upshots shown that the malware attack have the highest percentage rate compared to other attacks. The increase of malware has presented a long-lasting and serious threat to the security of computer systems and

Box 1.

- Blocks access to key components of the network (ransomware)
- Installs malware or additional harmful software
- Covertly obtains information by transmitting data from the hard drive (spyware)
- Disrupts certain components and renders the system inoperable