

Chapter 10

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

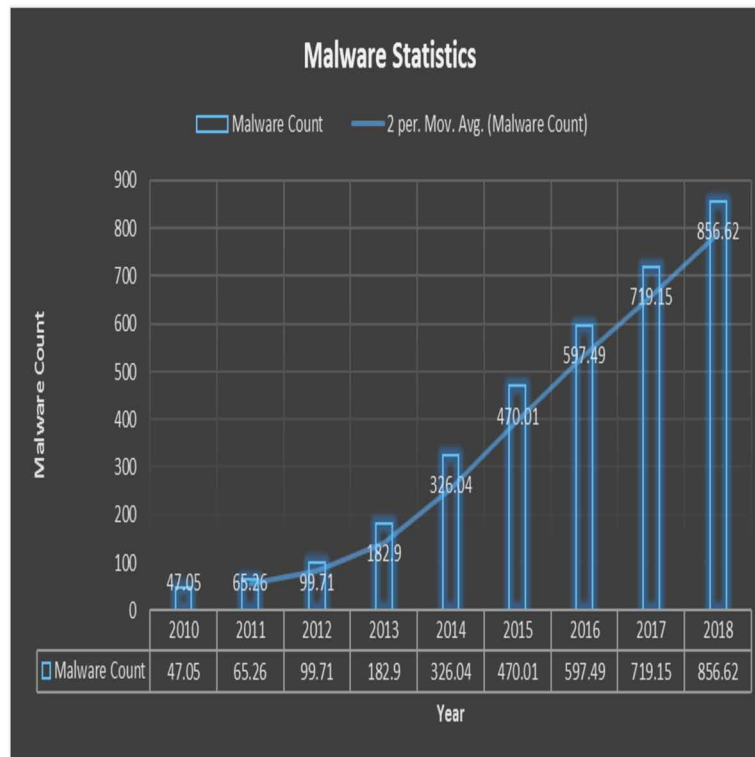
This chapter aims to discuss applications of machine learning in cyber security and explore how machine learning algorithms help to fight cyber-attacks. Cyber-attacks are wide and varied in multiple forms. The key benefit of machine learning algorithms is that it can deep dive and analyze system behavior 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.

DOI: 10.4018/978-1-6684-6291-1.ch010

Figure 1. Tabulation and graph on malware statistics



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.

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:

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

26 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/malware-and-anomaly-detection-using-machine-learning-and-deep-learning-methods/307451

Related Content

A Review on Time Series Motif Discovery Techniques an Application to ECG Signal

Classification: ECG Signal Classification Using Time Series Motif Discovery Techniques

Ramanujam Elangovanand Padmavathi S. (2019). *International Journal of Artificial Intelligence and Machine Learning* (pp. 39-56).

www.irma-international.org/article/a-review-on-time-series-motif-discovery-techniques-an-application-to-ecg-signal-classification/238127

Vapor Compression Refrigeration System Data-Based Comprehensive Model

Jesús-Antonio Hernández-Riverosand Gerardo José Amador Soto (2023). *Encyclopedia of Data Science and Machine Learning* (pp. 749-779).

www.irma-international.org/chapter/vapor-compression-refrigeration-system-data-based-comprehensive-model/317483

Shape-Based Features for Optimized Hand Gesture Recognition

Priyanka R., Prahanya Sriram, Jayasree L. N.and Angelin Gladston (2021). *International Journal of Artificial Intelligence and Machine Learning* (pp. 23-38).

www.irma-international.org/article/shape-based-features-for-optimized-hand-gesture-recognition/266494

Application of Machine Learning to User Behavior-Based Authentication in Smartphone and Web

Manoj Jayabalan (2022). *Applications of Machine Learning and Deep Learning for Privacy and Cybersecurity* (pp. 73-94).

www.irma-international.org/chapter/application-of-machine-learning-to-user-behavior-based-authentication-in-smartphone-and-web/311372

Graph Data Management, Modeling, and Mining

Karthik Srinivasan (2023). *Encyclopedia of Data Science and Machine Learning* (pp. 2023-2043).

www.irma-international.org/chapter/graph-data-management-modeling-and-mining/317604