Chapter 4

Trends in Malware Attacks: Identification and Mitigation Strategies

Abhishek Kumar Pandey
Babasaheb Bhimrao Ambedkar University, India

Ashutosh Kumar Tripathi
https://orcid.org/0000-0003-4021-9819
Babasaheb Bhimrao Ambedkar University, India

Gayatri Kapil
Babasaheb Bhimrao Ambedkar University, India

Virendra Singh
Babasaheb Bhimrao Ambedkar University, India

Mohd. Waris Khan
Babasaheb Bhimrao Ambedkar University, India

Alka Agrawal
Babasaheb Bhimrao Ambedkar University, India

Rajeev Kumar
https://orcid.org/0000-0002-1813-1362
Babasaheb Bhimrao Ambedkar University, India

Raees Ahmad Khan
Babasaheb Bhimrao Ambedkar University, India

ABSTRACT

Security issues are ever-evolving in today’s scenario due to the heterogeneous nature of software applications, multimedia features, multilingual interactive and responsible features, and rapid rise in third-party software products. The main objective of this chapter is to focus on the difficulties and components that the users have to contend with on the internet. This chapter investigates and manages ongoing malware attacks. It also explains the significance of the research, malware investigation, social engineering, and user awareness in the field of malware attacks. Cyber-attacks are the most common problem in recent years, and the increasing number of malware is becoming a challenging task for security experts. This chapter underlines key issues along with various aspects for experts to discuss and focus on reducing the threats posed by malware and planning the strategy for prevention in the future. The chapter provides an effective future direction for researchers to produce impactful outcomes.

DOI: 10.4018/978-1-7998-1558-7.ch004
INTRODUCTION

The recent decades have witnessed a spate of cyber-attacks that have led to disastrous results for both business organizations and the individual users of the cyber world. Every business is computerized now and every organization has its existence on the internet, but the main problem is that most of the online organizations don’t understand security factors or issues (threats) of the cyber world. This lacuna creates a massive platform for hackers to attack commercial enterprises and to make money through a digital platform. In today’s era, attackers are easily able to infiltrate systems because of malware. Attackers find it very easy to employ malware as it infects the system directly and that is the reason for malware emerging as a major threat for cyber-security. Software companies have to constantly work to write newer versions and security patches, and release them so that the existing and in-use software system can be upgraded to confront new forms of threats. Furthermore, it has been observed from the recent studies that software security breaches have dramatically increased around online financial activities such as- online banking, debit and credit card transactions, ATM transactions and other such activities.

According to a survey, “In December 2018 to January 2019, the malware activity has increased by 61% (Outpost24, 2018). This is indeed a cause for alarm as it creates a major issue for today’s cyber-security experts. According to the India Times survey 2019, “58% of data breach victims are the organizations who have a small business and do not have a proper cyber setup (Srinivasan C.R., 2019). Surveys also cite that 10 years ago malware attacks were relatively less as compared to the frequency with which they are implemented by attackers today. This type of growth shows the weakness of human awareness and system security as well as the lack of quality research in gauging and finding effective solutions to contain malware attacks. Awareness is the key factor in every organization’s security policy because if the employees are not aware of the possible threats they can be easily exploited by an intruder. Malware attacks can lead to huge losses for an organization not only in revenue but also in a brand niche, clients’ trust, business secrets, and other such vital statistics.

Malware Analysis is the process that has gained considerable focus as an effective tool to eliminate malware attacks. Malware analysis is the methodology for finding the functionality and objective of any malware. This article, in particular, shows that malware analysis methods are an effective deterrent against malware attacks. The second section of this article deals with the related incidents in malware attacks. The third section highlights the types of malware which have been detected recently and are major threats to the cyber security of several organizations. Furthermore, the author attracts the focus on the factors and challenges that need significance to weaken the malware attacks.
Digital Steganography Security
www.igi-global.com/chapter/digital-steganography-security/247291?camid=4v1a