2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM) | 979-8-3503-4779-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICONSTEM56934.2023.10142575

Detection and Classification of Malware for Cyber Security using Machine Learning Algorithms

Judy S[1], and Rashmita Khilar[2]

[1]*Research Scholar, Saveetha School of Engineering, SIMATS, Saveetha University, Chennai, Tamil Nadu*
[2]*Professor, Saveetha School of Engineering, SIMATS, Saveetha University, Chennai, Tamil Nadu*

E-mail:[1]judys9014.sse@saveetha.com [2]rashmitakhilar.sse@saveetha.com

Abstract-— The threat of malware to information security is one that keeps growing. However, the Windows operating system faces a very high level of unintended security risk. System exploitation that is prohibited could pose a security risk. For instance, PayPal is frequently imitated because hackers can profit significantly from obtaining consumers' PayPal login information. The main drawbacks of existing system is that, it takes more time to process and they are less efficient. To overcome the above drawbacks current research arena proposes a way that businesses detect threats, adapt and implement numerous cybersecurity techniques in combination with Machine learning and IOT approaches. But still there are lot of issues occurring in the above-mentioned techniques i.e., the Signature based detection is unattainable. The conclusion stated was that no machine is able to detect the malwares of the new generation with complete preciseness. A threat's mitigation is intended in addition to its identification and prevention. This study gives an insight about the various detection and classification techniques that were proposed using Machine Learning algorithms.

Keywords— Malware, Malware Detection, Cybersecurity, Machine Learning Algorithms.

I.INTRODUCTION

Malware is a type of software code that is intended to cause harm to a computer network. Malware code can manifest as viruses, worms, Trojan horses, or spyware. Malware detection seeks to locate and remove any type of malware code from a network. A Cybersecurity Ventures report estimates that cybercrime will cost the world $10.5 trillion per year by 2025, up from $3 trillion in 2015. This is the largest transfer of economic wealth in history. Unavoidably, malware will enter the network. Defences that offer considerable visibility and breach detection should always be present. Malicious actors must be swiftly located in order to remove malware. It calls for ongoing network scanning. The malware needs to be taken off the network once the threat has been recognized. Modern antivirus software is insufficient to defend against sophisticated online threats. The recent malware threats and their effects are consolidated as below.

News Malware Attacks: COVID-19 related emails sent by hackers disseminate false information regarding the pandemic.

Fleece ware: Despite removing those apps, Fleece ware still charges with a significant amount of money.

IoT Device Attack: Hackers are attempting to use devices like smart speakers and video doorbells to obtain important information.

Social Engineering Attack: The hacker poses as a certain individual, queries about the victim's account are asked, and the customer service staff is tricked into providing sensitive data.

Crypto jacking: Hackers are attempting to install Crypto jacking malware on computers and mobile devices to aid in the mining process. Bitcoin has soared above $40,000; prices of crypto currencies will continue to surge through 2022.

Hackers will be able to exploit this technology to launch deadly cyberattacks as more tools are made accessible to developers who wish to create AI scripts and software. While machine learning and artificial intelligence are being used by cybersecurity firms to battle malware, similar technologies may also be widely used to attack networks and devices.