République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

Ecole Supérieure en Informatique de Sidi Bel Abbès (ESI-SBA)

Mémoire de Fin d'étude

Pour l'obtention du diplôme de **Master**

Filiére: **Informatique**

Spécialité: **Ingénierie des Systèmes Informatiques (ISI)**

Thème

Detection of malicious PowerShell: Approaches and Techniques

Réalisé par:

- MERZOUK BENSELLOUA Ahmed Yasser
- MESSADI Said Abdesslem

Année Universitaire

2022/2023

Abstract

PowerShell is a powerful automation and scripting language that is extensively used across several platforms, which has resulted in a surge in the number of malicious scripts written using it, since it has many capabilities that aid in obfuscating scripts and evading standard detection techniques. In this thesis, we will compare several ways made by researchers to identify dangerous scripts using various methodologies. We will go over each paper's approach and discuss pros and disadvantages before concluding with a comparison table with various metrics. We concluded that recent research in the security field focused on using machine and deep learning techniques that improved detection. The most common techniques included NLP-based approaches with different twists, as well as completely new techniques like the GCN (Graph Convolution Network). We also noted the importance of detecting obfuscated scripts because they are the most frequently used to bypass classic detection techniques, and we noted the importance of detecting obfuscated scripts because they are the most frequently used to bypass classic detection techniques.

Introduction

PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework. PowerShell runs on Windows, Linux, and macOS[45]. PowerShell is built on the .NET framework and allows third-party users to write cmdlets and scripts that can spread to others through PowerShell[53].

PowerShell scripts can be directly executed in memory without being downloaded and saved on disk, which makes existing file-based anti-virus solutions useless against attacks using PowerShell scripts[53], since these anti-virus solutions monitor PowerShell events and use a signature-based approach. They scan for known intrusion events, as well as track command-line parameters that are commonly used in malicious attacks[55], this can be easily bypassed by attackers using the `-EncodeCommand` ↪ flag to pass Base-64 encoded commands and bypass the PowerShell execution regulations[57].

Machine learning and deep learning have transformed the security industry, introducing new options and better capabilities for threat detection, prevention, and response. These approaches have considerably enhanced the accuracy and efficiency of security systems by analyzing massive volumes of data. Machine learning algorithms may learn from previous data to recognize trends and abnormalities, allowing prospective risks such as malware, intrusion attempts, or suspicious behaviors to be identified. Deep learning, a subset of machine learning, has progressed the science even further by utilizing neural networks with numerous layers to handle complex and unstructured data such as photos, videos, or natural language.Machine learning and deep learning algorithms have become crucial tools in reinforcing the security environment, enabling proactive defenses, and helping businesses to remain ahead of developing threats by constantly learning and adapting from new data.

In the following chapters we will be discussing PowerShell, its use and importance along side with the security mechanisms implemented to detect malicious activities

and their problems in chapter 1, afterwards we will look into machine learning and deep learning techniques and their use cases in chapter 2, then we will be diving into the different approaches taken by researchers to tackle the problem in chapter 3, and finally we will be comparing the different approaches results with a synthesis in chapter 4.