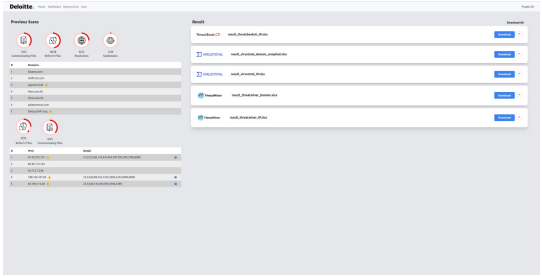
THE DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
計算機科學及工程學系

Enhancing Cyber Threat Intelligence: IP Domain Investigation and Attack Surface Management through Intelligent Scripting

Wilson Thiesman
Supervised by Professor Shuai WANG

Introduction

Cyber security has been the main focus of some of the major headlines in the 21st century due to the rise of cyber-attacks. Modern threat actors tend to target large enterprises through social engineering (phishing) and malware to carry out their malicious activity. Thus, the need for an efficient Cyber Threat Intelligence (CTI) investigation tool is crucial to prevent such tragedy from happening



Objectives

The objective of this project is as follows:

1. Discern potential vulnerabilities within organizations or corporations
2. Enabling the Deloitte CTI team to assist in risk mitigation via exhibiting indicators of compromises
3. Potentially establish a professional partnership with the subject of investigation and enhance their cybersecurity resilience

Methodology

The intelligent script can receive any form of input, both from the query it gets and from a file being uploaded. The input content will be filtered automatically to fetch the relevant data to be scanned, IPv4 and Domain Names. On top of that, the intelligent script will perform web scraping of various reliable external threat intelligence to gather recent suspicious IPv4 and Domain names that have been discovered.

The data is passed into multiple sub-scripts asynchronously, where each will perform API calls into some Open-Source Intelligence (OSINT) technologies: VirusTotal, ThreatbookCTI, ThreatMiner. The result of each OSINT is formatted following a professional analyst request, uploaded to the database for historical record, and visualized in the front-end for quick investigation. The script enables

Each OSINT integrates a lot of AntiViruses that vote internet entities whether they are malicious or not. By incorporating data from AV raters such as AV-test, AV-Comparatives, and SE labs, the script gives weight to each antivirus. As a result, reputable antiviruses possess more weight compared to the others.

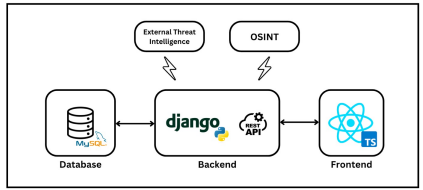
Thus, the probability that an entity is malicious is calculated as follows:

$$\frac{\sum_{i=1}^{n}(w_i * vote\ malicious)}{\sum_{i=1}^{n}(w_i * vote\ malicious) + \sum_{i=1}^{n}(w_i * vote\ nonmalicious)}$$

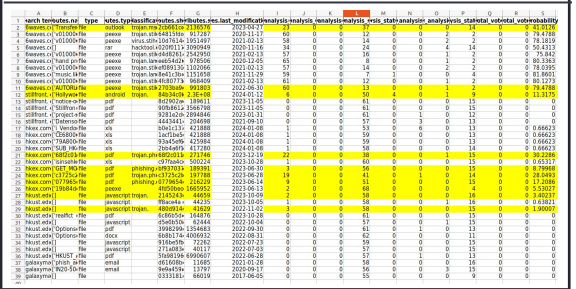
$vote\ malicious = boolean\ (1\ or\ 0)$

$w = weights$

System Architecture



Result



Conclusion

The intelligent script serves as a tool to alleviate CTI analysts in identifying potential malicious entities, from legitimate and illegitimate sources, by providing the likelihood of an entity being malicious, which might act as an Indicator of Compromises for the subject of investigation both directly/indirectly.