Know Thy Enemy Project Proposal

Clay Shubert, Lu Liu, William Quesinberry, Wesley Fortner, and Ethan Ly

Abstract— **This is a project proposal for KnowThyEnemy, a program that determines the most common origin country of sophisticated attacks (Zero-Day, Ransomware, IoT) and ranks them. Industries may utilize to better understand their attack surface.**

I. Project Objective

KnowThyEnemy is a project thats aims to provide more visibility to industries who are often targeted by sophisticated cyberattacks. Oftentimes, industries are battling attacks of all different kinds, requiring them to maintain several block lists full of IP addresses and other indicators that have attempted attacks in the past. This can become problematic because the biggest danger in security is not knowing and industries can still be targeted by unique indicators. KnowThyEnemy aims to provide a solution to this problem by providing a ranking of the most common origin countries of sophisticated attacks. This ranking will allow industries to better understand their attack surface and take the necessary precautions to protect themselves. Using the rankings, industries may chose to apply geo-blocking to the origin country with the highest ranking if access from this location is not required for business operations. This might be especially beneficial to small businesses whom may not have the resources to maintain an ever-changing and large block list or the ability to pay for a third party service to do so.

II. Motivation

The motivation for this project comes from experience and interest in the field of cybersecurity. The connection between threat actors and their location is an interesting topic and we are interesting in seeing if there is any correlation between attack location and sophistication. We also are interested in investigating how open-source can be used to analyze and visualize data to provide a solution to a real-world problem.

III. Data Sources

The data sources for this project will be the following:

- **AlienVault OTX:** AlienVault Open Threat Exchange (OTX) is an open information-sharing and analysis network that provides real-time, actionable threat intelligence. AlienVault OTX provides an API that allows users to retrieve this data programmatically.
- **VirusTotal:** VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware. It is a repository of known malware samples and a service that analyzes them. VirusTotal provides an API that allows users to retrieve this data programmatically.
- **AbuseIPDB:** AbuseIPDB is a free project to check IP address reputation. It includes information about the IP such as Country Name, Hostname, Email, Community Rating, etc. The project is used by tens of thousands of users every day. AbuseIPDB provides an API that allows users to retrieve this data programmatically.
- **URLhaus:** URLhaus is a project from abuse.ch with the goal of sharing malicious URLs that are being used for malware distribution. URLhaus provides an API that allows users to retrieve this data programmatically.

IV. Member Responsibilities

- **Clay Shubert:** Clay will be responsible for the data collection and analysis. He will also be responsible for the project report and presentation.
- **Lu Liu:** Lu will be responsible for the data collection and analysis. She will also be responsible for the project report and presentation.
- **William Quesinberry:** William will be responsible for the data collection and analysis. He will also be responsible for the project report and presentation.
- **Wesley Fortner:** Wesley will be responsible for the data collection and analysis. He will also be responsible for the project report and presentation.
- **Ethan Ly:** Ethan will be responsible for the data collection and analysis. He will also be responsible for the project report and presentation.

V. Milestones

Milestone 1: Data Collection

- **Description:** Collect data from the data sources listed above.
- **Due Date:** 10/15/2023
- **Responsible Members:** All

Milestone 2: Data Analysis

- **Description:** Analyze the data collected and determine the most common origin countries of sophisticated attacks.
- **Due Date:** 10/31/2023
- **Responsible Members:** All

Milestone 3: Data Visualization and Error Correction

- **Description:** Visualize the data and correct any errors.
- **Due Date:** 11/15/2023
- **Responsible Members:** All

Milestone 4: Project Report

- **Description:** Write the project report.
- **Due Date:** Late November 2023
- **Responsible Members:** All
- **Deliverable:** Project Report

Milestone 5: Project Presentation

- **Description:** Create the project presentation.
- **Due Date:** Late November 2023
- **Responsible Members:** All
- **Deliverable:** Project Presentation

VI. Expected Outcome

At the end of this project we expect to provide deliverables that include a project report and presentation outlining the details of our work. In addition, we expect to deliver a presentation to the class of our findings and results. Lastly, we expect to provide a working program that can be used to determine the most common origin countries of sophisticated attacks that will live in the open source community.