Project Plan Presentation
Predicting Malware Command and Control Channels

The Capstone Experience

Team Vectra
Ettore Campriani
Aidan Erickson
Nathaniel Ferry
Sam Kwiatkowski-Martin
Muhan Luo
Aidan McCoy

Department of Computer Science and Engineering
Michigan State University
Spring 2023
Project Sponsor Overview

- Sponsor Overview
  - Cybersecurity threat detection and prevention
  - Products built on machine learning and artificial intelligence
  - HQ: San Jose, CA | Employees: ~600
Project Functional Specifications

• Develop a ML Model to detect C2
• Intrusion Detection Systems
  ▪ Mainly use signatures
  ▪ Not always effective
• Vectra currently uses ML model to detect C2
• We will develop a complementary approach using signatures and ML
Project Design Specifications

- Web Application
  - Vectra color scheme
- Graphs
  - Visualize network data
  - Emphasize malicious activities
- Data Tables
  - In depth analysis
- C2 Predictions
  - ML modeling
Screen Mockup: PCAP Analysis Page
Screen Mockup: Session Data Page
Screen Mockup: C2 Prediction Page
Screen Mockup: ML Graph Page
Project Technical Specifications

• Data Collection
  ▪ Wireshark: Packet sniffing
  ▪ Suricata: Intrusion Detection System

• Python Machine Learning
  ▪ PyTorch, Scikit Learn, LightGBM

• Web Application
  ▪ AWS EC2: Server
  ▪ Flask: Backend web development
  ▪ SQLite: Relational Database
Project System Architecture

Packet Sourcing
- Wireshark
- Web Scraper

Data for Training

Processed Dataset
- SURICATA

Data Preprocessing

Machine Learning Model
- PyTorch
- LightGBM

User

Web Application
- JavaScript

Front End
- Flask

Back End

AWS EC2

SQLite Database
Project System Components

• Hardware Platforms
  ▪ iMacs
  ▪ AWS EC2 instance

• Software Platforms / Technologies
  ▪ WireShark
  ▪ Suricata
  ▪ Python ML Libraries
  ▪ Python Flask Library
Project Risks

• Visualization
  ▪ Majority of the project is “under the hood”
  ▪ Create a visualization with mock data

• Varied Data
  ▪ Need more varied data
  ▪ Get web scraper running and further client contact

• ML Model Graph
  ▪ We are unsure if it is possible to integrate a graph of our model onto the web app
  ▪ Build a prototype graph of model

• Prediction Accuracy
  ▪ Achieving a prediction accuracy proving our machine learning model is viable for practical application
  ▪ Multiple prototypes showing an increase in accuracy
Questions?