YS5-Red Cybersecurity in Malware Analysis Weekly Report

Connor Skidmore, Jonathan Tarrant, Andy Guo

Date: 9/23/2022

Meeting Notes From This Week:

Meeting 1 (Thursday 9/22/2022 2 PM):

In this meeting we discussed the following:

- Created Google Site Framework to contain both research and Github links for source code programs.
- Discussed deliverable due dates and planned out workload distribution throughout the semester
- Settled on which malware modules we would be completing for the project
- Discussed the project scope with Dr. Perry and determined that we would be unable to do AI/ML programs for all 5 of the modules
- Discussed and looked at various sources for data sets of malware attacks, including Kaggle

Meeting 2 (Friday 9/23/2022 12 PM)

In this meeting we discussed the following:

- Discussed project scope with Dr. Perry
- Discussed need to do source code program for all 5 modules
- Discussed using non-AI/ML source code for 3 of the Modules
- Decided on doing in-depth research and AI/ML analysis/detection for DDoS and Port Scan attacks
- Decided on doing non-AI/ML source code program for other 3 modules

Goals for Next Week:

- Begin filling in Google Site with preliminary research for DDoS, Port Scan, Cryptojacking, AI Attacks, and IoT Attacks
- Continue searching for and gathering data sets on these malware topics from various sites such as Kaggle
- Continue learning about ML/AI, how they are used to detect malware, as well as how they apply to our specific modules

Next Meeting: Thursday 9/29/2022 2 PM