

Knight Foundation School of Computing and Information Sciences

Spring 2022 Capstone I Project

Ransomware Anomaly Detection

Students: Ivan Rosyaykin, Ricardo Tacconi

Mentor: Mike East, Kaseya; Carl Banzhof, RocketCyber

Instructor/Faculty: Dr. Masoud Sadjadi, Florida International University

Problem

Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. [1] Ransomware attacks are estimated to cost \$6 trillion annually by 2021. [2]

Current System

The current system of our project is a Python application that reads event log files, .evtx files, processes the files to get the event data from it, and pass the data to a string comparison algorithm to train the model at the beginning so later, we can determine if a ransomware attack is happening using our application comparing any dissimilarity to any previous events.

Implementation

- 1) Python 3.10
- 2) Sysmon v13.33
- 3) Dissimilarity Algorithm-String Comparison Model.
- 4) Google Docs
- 5) Github

Verification

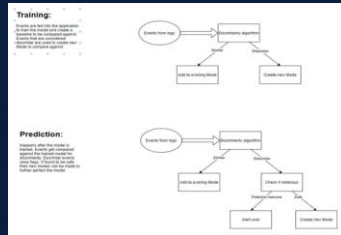
Application was tested with Sysmon Simulator and discovered a 75% success rate.

Summary

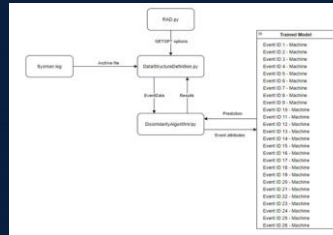
The team was able to implement an anomaly detection application written in Python. The application is able to analyze Sysmon Windows event logs that are used to predict unusual behavior using a comparison algorithm.

Personally, I was able to learn how to work in an Agile environment and learnt many topics in ML as well as how the System Log in Windows works.

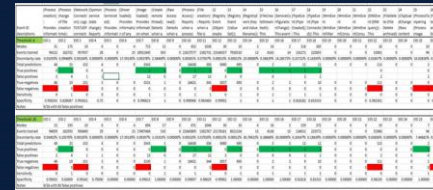
Object Design



System Design



Verification



References

- [1] "Ransomware." FBI, FBI, 3 Apr. 2020, <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware#:~:text=Ransomware%20is%20a%20type%20of,of%20critical%20information%20and%20data.>
- [2] "2021 Cyber Security Statistics Trends & Data." PurpleSec, 6 Aug. 2021, <https://purplesec.us/resources/cyber-security-statistics/#:~:text=Ransomware%20attacks%20are%20estimated%20to,attacks%20han%20ever%20in%202019.>