Thanawat Tejapijaya

Weekly report Week 8 (10/7/2023 - 14/7/2023)

For my progress report this week, I have prepared my presentation for mahidol faculty visit so I didn't make much progress. However, the presentation came out pretty good. Moreover, I have continue writing research proposal where I have finished the background of it as shown as below:

Botnet Detection with Ensemble Machine Learning Method

Thanawat Tejapijaya
2316001

Background

Botnets is a network of computers infected by malware and remotely dominated by one attacking party. The word botnet came from robot and network combined together because it is a computer that acts like a robot and tries to do malicious actions such as spamming, Distributed Denial of Service(DDOS) etc. to the network through internet, local access and more. Botnet is one of the most aggressive cyber attack threads as it is very hard to detect their action, also their behavior evolves from time to time. In other words, botnet techniques, life cycle and behavior can evolve at any time, as a consequence, detecting it becomes very challenging for people that are working on the defensive side like SOC. Moreover, to detect a botnet action may take a lot of time and there are not many people who is working on this defensive side. For instance, 3ve in 2018 which is an botnet attack incident where botnet evaded the detection from Security Information and Event Management(SIEM) and first detected by human when it was too late and it infected over 700,000 personal computer, compromise over 1 millions IP address and millions of dollars are lost. That is why machine learning is needed for using in botnet detection also it become the motivation on this research because of using the machine learning to help detecting botnet action through the network much faster and more efficiency, also with machine learning it be able to work all day and night while human still need to rest there body and mind from the work, hence with use of machine learning will help reduce the workload of people who is working in the SOC team.

For this week I will continue writing progress report and start doing data preprocessing stage.