CSCE 689: ML Based Cyber Defense - Whitebox Attacks

By Nhat Nguyen, Sonjoy Paul, Erik Muller

Blackbox Attacks

4 Attacks

- Packing Files with UPX
- Adding Benign Section Data to the files
- Appending random strings to the end of files
- Combining all 3 methods

Results

- Very Poor overall results, but did see some success with packing versus team 4 and adding sections versus ourselves
- What we missed: Droppers, Droppers, Droppers

List of Whitebox Attacks

1. Black box's added section version+ Professor’s Dropper **(Version 1)**
2. Professor’s Dropper + Section Data + Random String + UPX **(Version 2)**
   a. Sections from ntdll.dll
3. Professor’s XOR Dropper on version 2 **(Version 3)**
4. Version 3 + Section from two dlls + Random String + UPX **(Version 4**)
   a. Sections from *ntdll.DLL* and *filesystem.DLL*

Could not find a way to bypass all models with one method

Problems Faced

- Inability to get droppers working until late in the process
- Could not make one method to bypass all models
  - Found different attacks that worked for some models, but not for all
- Could not get team 3's docker image to run on our machines
  - Not sure the reason, maybe too memory intensive?
- Dealing with malware is kinda scary
  - Had trouble running windows VMs
  - Github repos are sketchy

Questions ?