What is the project?

Our project is malWALL© (Firewall for malware). We are creating a program to prevent programs from accessing external IP addresses and communicating with them if they do not have DNS mapping. In other words, if a bot or other malware is installed on someone's local machine, and it attempts to connect to a C&C server directly through an IP address, the communication will be blocked. If the program attempting to run is known to the user to be safe, they can whitelist the program and allow it all network access, or it can be blacklisted and prevent all network traffic.

Why is tackling this project important?

Malicious programs such as malware, ransomwares connect with Command and Control (C&C) servers to await further instructions on their chain of command, send sensitive user data , and perform other steps of their damage. We can limit a significant amount of damage by preventing malicious activity of the malwares from the network level by building this network filtering system. The filtering system thus designed will protect transfer of sensitive data to the adversaries , as well as impede the operation of malwares which would otherwise require some sort of network interactions. A system like this would force the malware developers to use DNS mapping , which could potentially help the defense systems to make tracking them down easier, and require more effort from the adversaries.

How do you plan on tackling the project?

Week 1: Figure out how to examine and filter network traffic on a Windows machine as well as how to figure out whether a program is accessing an IP directly or a DNS url and what program is performing the request.

Week 2: Figure out how to block program network traffic with our own program running as administrator and piece. Automate system to determine IP vs DNS request.

Week 3: Piece together work from the first 2 weeks, create a full program that can be run by a user that will block all network traffic from a program that is detected to be communicating with an IP directly, and a method for the user to allow network traffic for that program.

Week 4: Keep working on week 3 work if necessary, as well collect malware that will be statically analyzed to determine if it actually attempts to connect to an IP directly (or by examining source code from a malware using in other epochs) for use in a demo. Generate a permanent whitelist that can be modified by the user as well as a blacklist, both of which will be checked for each program attempting to

perform network access. In addition if other work has been completed, create other features such as notifying the user and logging data.

List of 3 sets of deliverables (I'll take these under advisement when grading, but I don't promise to strictly abide by them):

Passing Grade

A simple program that can detect when a program attempts to communicate with an IP not associated with the DNS and blocking network traffic to these IPs.

A Grade

We are not sure. Suggestions?

Beyond A Grade:

A network filter CLI with notifications for when and which program attempts to communicate with an IP address not associated with DNS, black list and whitelists for programs, and logging of data. GUI(?)

Link to a git repository where you'll keep all the code, documentation, and development through the project.

https://github.com/camdenkr/EC700_Epoch3