Project Proposal: MalOs

Group Members:

Justin Guerrero – j87n896
Arnold Smithson – q46t616
Jada Bryant – b63j795
Teyler Halama – b56k732

Deliverables and Overview:

For our project, we are proposing an in-depth study focused on Linux based operating system malware attacks. Specifically, we will be investigating specific attacks such as rootkits, DLL injections, and NotPetya to see specifically what they do to manipulate an operating system in order to achieve their goal.

Our goal is to deliver a technical document and presentation that shows successful malware attacks and how they were able to manipulate the operating system freely. We aim to show code examples that can be related back to topics we have learned in class and show that these malware attacks are things we can understand. We also hope to show some components of an operating system that are now standard because of successful malware attacks.

Division of labor within the group

Each team member will take time to learn more about types of malware that targets operating systems. We will start by researching what malware attacks are popular. We will then meet to discuss what specific attack there is the most information on and is the most interesting to present. In our presentation we will demonstrate a thorough understanding of an attack from an idea all the way to the depth of the effects on an operating system.

Again, after having elected to research Linux because of its open source nature we aim to come together and discuss which malware attack we want to focus our efforts on. We will then divide the labor to investigate different parts of the Linux operating system that the said malware attacks target. We will then collect code examples of our tasked region of the operating system gathering enough info to walk through what the attack does to that part of the operating system to accomplish its goal. If the code has been updated as a countermeasure to the malware, we will walk through how the code was previously structured, and what updates were made to prevent the specific malware attack.

Rough Schedule

We aim to have a specific malware attack to focus on by the end of week one. After week one, we feel confident that we will have a clear goal in mind for the project and be able to work individually on the delegated work until meeting again to cover the project as a whole.

Desired Outcome:

We hope to deepen our understanding on the components learned through class by researching how they have been taken advantage of in hopes of presenting a document that shows how malware attacks are not magic and that they are simple to understand with the knowledge acquired through our class.