Week 1 Notes

Trent Vasquez

7/3/2018

1 Evaluating Evil.exe

While this first set of lectures was pretty simple, it opened up for the sets of terminology we will be using in the course, and its worth reiterating here in the weekly write up. Malware is the heart of this course and can be basically defined as any malicious software. The three major brands of malware fall under viruses, Trojans, and unwanted programs. When working with pieces of code, we label them one of three categories, white, black, and gray. While white code is considered "clean", black code is typically malicious on the spectrum.

Some of the major tools we use in the investigation of malware are goats, honeypots, and hashes. Similarly to the name implies, a goat is a system that you "sacrifice" to the malware by having it infected on purpose. While you may think that a honeypot is the same thing, honeypots aren't directly infected, but are out in the wild trying to fish a malicious attack. Another tool we use in security are hashes. A hash is a cryptographically secure one way function that will give you a unique result for the input. This allows for us to hash files and see if they've been changed in any way since the last time they were hashed.

A key thing in analyzing malware is knowing the different types of attacks that can be implemented using malware. Boot-kits are a tool that allow for a malicious software to take control over the rootkit and thus infect the master boot record. Trojans are a type of malware that work by giving backdoor access to your computer that were unintentional. Spyware are pieces of

unwanted code that relate information that your doing such as a key logger. In a glowingly digital world, ransom-ware has become increasingly prevalent. Ransomware is software that will lock you out of your computer/file, typically by holding your private keys hostage until you pay the ransom.

Something that is important to pay attention to is the attributes of an adversary attacking your systems. As described by the US Air-Force in 2006, adversaries can be tagged as Advanced (fluent with cyber intrusion methods and can create custom exploits), Persistent (Attacker with an objective/goal and will work to achieve goal without detection), and Threat (An attacker that is orginized, funded, and is motivated to attack).