Tu Lam

CS 373 (Defense Against the Dark Arts)

Dr. Bram Lewis

October 12, 2021

Homework #3 Write-Up

Week #3 of the class demonstrate towards malware defense where we learn about how the malware enter for the attack, how would the system would detect the threat, and what kind of defense does it use to block these attacks. These types are core focus of three steps: ***attack vector***, ***opportunity for defense***, and ***type of defense***. On top of that, we will also dive into an example of this through ***myQ door bypass*** and a couple of lab example of this defense.

First, we dive into the point of contact about the attack vector, this is where the first introduction of the malware enters the system is happening. The category for these types of vector are broken down to ***first contact***, ***local execution***, ***establish presence***, and ***malicious activity***. Below is a figure breaking down each category and examples of how you would see this in a malware form.

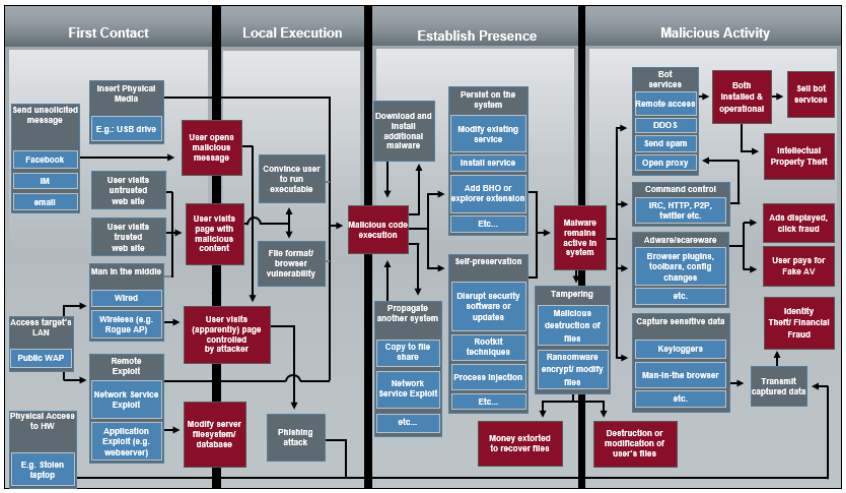

Figure #1: Attack vector and their category of each malware attack (From Lecture)

Looking at the first category, ***first contact***, this type of malware introduces to the system or user through email, instant messaging, physical address, advertising, website link, and more. Next is the ***local execution***, this is in the form of script and executable file that you click on after getting the

initial stage of introduction to the malware. Then, moving to establishing presence, once the malware is on the system, it will try to disguise itself as a legitimate part of the system that it is easy to pass off as a threat. Finally, the ***malicious activity*** happens where the malware deploy it stuff through unwanted pop-up ads, self bot service, fraud, and more. These are the steps it takes for the malware to go through the system and reaches the inner core of it.

The ***defense for these malwares*** will have the same kind of layout and at each step, there is a way for the defense to detect, block, or warn about the malware. In the first contact stage, some of the program that offer these types of protection could be anti-spam, firewall, network IPS, URL reputation, disk encryptions, HTTPS, and more. Moving to the next level, local execution where in the form of client-side filter, content filter/scanning, whitelisting, etc… Some of this application establish the same thing when switch into establishing presence with anti-virus, whitelisting, HIPS, and more. Lastly, when the malicious activity happens, couple of the repeating defense use in this case are firewall, anti-virus, IP, content filter, etc… Through these defenses, this is what the system could do to help and prevent the attack of malware on the system once an early sign of attack happens. Below will be two figures showing the layer of defense through the system.

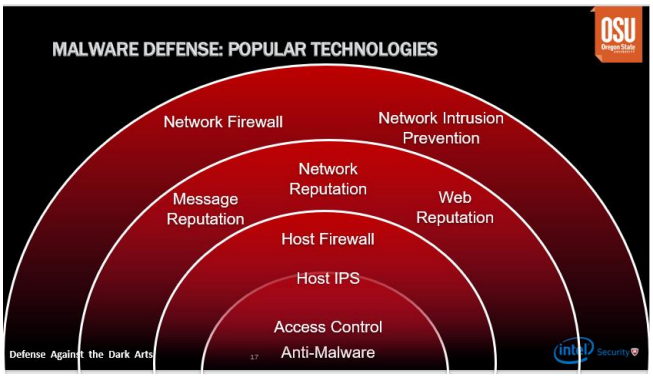

Figure #2: The technology that help fight against malware attack

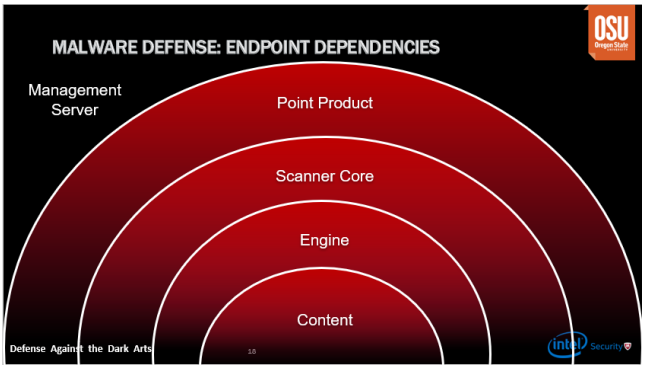

Figure #3: The endpoint dependencies of how defense look

Moving to the lab section of this week, we were introduced to YARA lab. To understand YARA, this short for ***Yet Another Recursive/Ridiculous Acronym,*** this is a tool where it is primarily used in malware research and detection. The tool provides a rule-based approach to create descriptions of malware families based on textual or binary patterns. In the lab, we will be exploring this topic and see what kind of malware detection the YARA tool can identify and give us base on the result it found.

Lastly, we look at an example of type of defense through the example of ***myQ door defense against bypass***. myQ has been part of the smart garage door where user get to control their garage door through their smartphone or any other smart device. We use this as a way to see how myQ uses a defense to block the attack of a jammed door through people at myQ disguise as an attacker. The myQ uses OOK system (On Off Key) to create a motion frequency by color for the sensor to detect threat. Through this the motion sensor was able to pick up the jam that was not part of the system and filter out the attacker by this through the figure below.

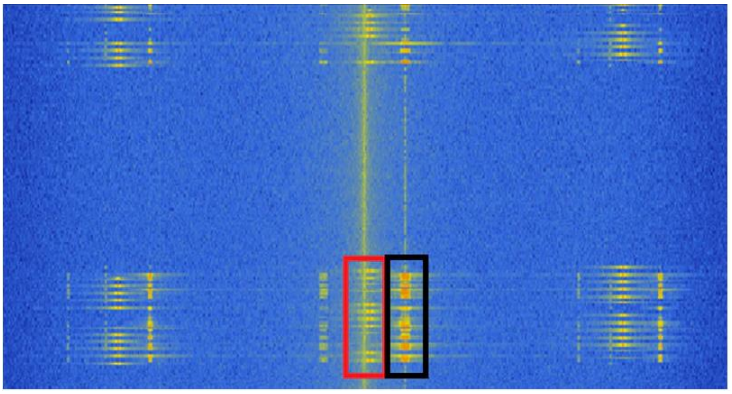

Figure #4: The frequency the garage door sensor picks up, red from the myQ signal, while black is the attacker

Through this, the sensor would then detect the threat and would confirm that the signal is from myQ or not and try to block it from happening. This kind of technology that myQ implement can give us a sense on how they are able to detect and keep use safe from unsafe malware and put fear aside when setting up a smart garage door.

This week process of learning type of defenses is a great way to learn how technology that we use daily help us block from our malware attack. Looking at it in the inner depth layer give us a sense of how the attack happen and how at each stage will do base on the severity. Using the defense system, we also see that they overlap with each other and helping out as each stage of the category of the attacker and help us from getting infected.