CS 373 Summer 2019
Week 1

Malware Basics

This course is the first time I had really considered malware outside of the context of wanting to make sure that I was protected from it as best as possible, and I found the topic quite fascinating.

One thing I found particularly interesting was the discussion on how polymorphic viruses, ones that change with each installation or iteration to confuse and bypass detection, while very good at doing that, and also fairly easy to code, are not very common. This really brought home to me just how vulnerable we all are. Even easy improvements like polymorphism are not necessary because it is so easy to design malware that will work regardless. This is pretty scary. It made me realize just how vulnerable we all are, even when we have protection installed.

I also had never through of the business behind malware, and the fact that most malware is purchased and run. This makes sense in retrospect but I sort of always had the image of the bad guys writing code and using it for evil. The fact that they make a kit and then sell it is really interesting. Most people that are using the malware are not actually super code literate, they are just following instructions. And it is also fascinating how these kits work, first gathering up information about the target's system, then deciding what the best ways into the system would be from many potential vulnerabilities. This gives them a quite robust product that is very easy for the purchaser to just implement and have good results (unfortunately for all of us being targeted).

One topic that I had a particular interest in was the use of malware in corporate espionage. The fact that most of this type of attack starts with gathering available information to find potential way into the company is pretty scary when you realize just how much information is available and how easy it is to disguise malware as something real if you have even a little information. IT is also scary how customized these sorts of attacks are. Normal antivirus software is not going to protect a company. I am interested in learning more about how companies can protect themselves when infection seems as easy as throwing some USB sticks on the ground in the parking lot or sending an email that looks like it comes directly from a trusted vendor.

I also had not ever thought much about how ransomware worked, and was interested to learn just a bit about how it holds the victims hostage. This is a really big threat and again I feel extremely vulnerable knowing just how easy something like this is.

At the end of the day my most important take away was that the biggest infection vector is still the user. People click on OBVIOUSLY suspicious links every day just inviting the malware in. As

scary as all these ways of being attacked are, the best defense is still not to click that weird thing.