OREGON STATE UNIVERSITY

CS 373

WINTER 2019

WEEK 1

Weekly Write Up

Author:
Thomas Noelcke

Instructor:
D. Kevin McGrath

I. Overview

This week we learned about the basics of malware. Through out the lectures this week we learned import terminology. In the first part of this write up I will talk about the topics that I found interesting during the lectures. In the section section I will talk about the lab and what I learned during the lab. In the last section of the write up I will create a list of important terms I learned during the lecture. This last section is mostly for the purposes of reference.

II. Lecture Topics

A. Why Does Malware Exist

A the beginning of this week we started off by talking about why malware exists. We determined that malware primarily exists to cause harm or destruction, for monetary reasons, political gain and to steal intellectual property. We also determined that there are a wide variety of people who write malware. This includes governments, lone wolf hackers, groups of hackers, companies, and terrorist organizations. Essentially there are a wide variety of people who might write malware for a wide array of reasons.

B. History of Malware

We then moved on to talking about malware research basics. We started with a brief history of malware and malware research. This included how malware was stored. It was originally stored and distributed on floppy disks. At one point the worlds leading malware database was able to be contained in cabinet. Today there are many many terabytes of different malware samples. The endpoint protection industry has also become a 10 billion dollar industry.

C. Types of Malware

We then moved on to talking about what types of malware there are. There are viruses, Parasitic and polymorphic along with Worms. Interestingly, polymorphic malware is malware that mutates and rewrites the code as it is trying to be detected. This type of malware is less common and is probably written by some sort of government or other large organization. There are also Trojans of various types. These often take advantage of some sort of back door. Finally, there are also potentially unwanted programs. These are programs that may look real but end up being unwanted. During this section of the lecture we also discussed the idea that the weakest point in a system from a security standpoint is the user.

D. Infection Vectors

At this point in the lecture we started talking about how malware gets on to users systems. Malware is put on user systems via USB sticks, mobile apps, drive-by downloads, pdfs and office files. Its also important to note that malware can be written in Microsoft Office Macros. In fact this was such a problem that Microsoft was force to release an update to Office that forced macros to be off by default.

E. Handling Malware

Another important topic we covered this week during lecture is handling malware. In this section we talked about some good practices when handling malware. We learned that you should always transport malware in an inactive state. It is also important to lock down the development environment using anti-malware software, a firewall and using policies to prevent mishaps. For the purposes of this class we are using a security hardened VM hosted by the university. This VM will prevent the malware from doing any thing that it really shouldn't be doing.

F. Malware compression

One thing I learned this week that I found really interesting is packing code. Hackers to this to disguise the malware. This can make it harder to figure out what the malware does and makes it much more difficult to detect. To do this the hackers use packers. There are many different packers out there however, one of the more popular packers is UPX. This is a handy bit of information because it means that we can also decompoile the code and view the code more easily. There are also some packers that you won't be able to upack using UPX. There are also tools that allow us to crack this code as well.

III. LAB

This week in lab we got the chance to play with real live malware. This included using various tools to observe the malware. For more details please see the Lab 1 write up.

IV. VOCABULARY

Below is a list of important terms we learned this week during lecture.

- **Malware:** any piece of software that attempts to preform unwanted malicious operations.
- **Patient Zero:** first computer infected in a targeted attack often an APT.
- **Packer:** a Piece of software that will compress or encrypt a piece of software.
- **Goat:** A machine or computer that you sacrifice to observe a piece of malware that is running. This is typically done in a VM with some special software running to prevent the malware from actually doing any thing malicious.
- **ATP:** Advanced Persistent Threat. This is a targeted attack by some sort of large organization that has a clear and targeted objective.