OREGON STATE UNIVERSITY

CS 373

WINTER 2019

WEEK 2

Weekly Write Up

Author:
Thomas Noelcke

Instructor:
D. Kevin McGrath

I. Overview

This week we are diving deeper into a different area of malware. Last week we learned about malware research where we set off some malware and tried to figure out what it did.This week we are learning about Forensics in malware. In this write up i will talk about different sections of the lecture I found interesting. I will also list out any vocabulary terms that are new to me that I think are important to remember.

II. Lecture Topics

A. Forensics Basics

The number one thing that the lecturer wanted to say was that safety is the most important part. If you are ever asked to investigate something in an area that is unsafe just to pull the plug and take it some where safer. This does have some problems as this will cause the memory to dump and may cause some data to be lost. If you can do the memory analysis while its safe it is a good idea. There are also several over types of investigation that we can also do. This includes hard drive analysis, postpartum analysis, analysis of gaming systems and other types of analysis. Generally, when doing an investigation there are three stages of an investigation Evidence acquisition, Investigation and analysis and reporting results. During the first of these three stages the main challenge is ensuring that things are safe while trying to do live analysis. The second stage is the stage that we are going to dig into this week. The final stage the main challenge is reporting what happened on a system in a way that people with non technical people can understand. There are also four principles you must always adhere to:

- Minimise data loss
- Record everything
- Analyze all data collected (evidence)
- Report findings

It is also important to note that it is important to report the time when things happened, including the system time.

B. Evidence

Evidence is any thing you can use to prove or disprove a fact. For the purposes of computer forensics, the different types of evidence that can be found at many different layers. These may include network, operating system, databases and applications, peripherals, removable media, and human testimony. It is important to use Triage when investigating. This means to prove in many different ways that some thing is true or untrue. One of the challenges you may face while investigating has to do with the sheer size of the media that is out there. You can image that with a 1 or 2 TB drive how much data that could be placed on that disk. There are some tools that we can use to help move this along such as using the checksums for files and comparing them to other known files from other cases. This can also help limit exposure to uncomfortable material. Another challenge that you may face during an investigation is dealing with SSDs. When getting evidence from some one with a checksum you should verify that the checksum is correct. It is also common to use write blockers to ensure that data cannot be written to a hard disk that you are trying analyze. Write blockers are cool.

C. legal stuff

For the most part this stuff this isn't super interesting but there are some things its important to note that you can't do. If you find passwords for accounts while investigating you are not allowed to log into those accounts. That is strictly a no go with out getting a warrant from a Judge.

D. Incidence Response

This is another area in Forensics is responding to incidents. Having a team for this is generally a luxury. Some companies have them but often they are thrown together teams. Often these teams aren't training enough. It is important to ensure that you are training a lot if you are doing this type of work as you want to make sure that things go wrong in training rather than during a real attack. When doing IR and forensics it is important to ensure that you have the correct access level to gather information. While doing IR it is important to try to catch threats early. Its possible to catch information early in different firewall logs along with in other system logs. Is is especially true for ATP attacks. However, it may be difficult to do this as there will be many logs to sift through.

E. Locard's Exchange Principle

When any two objects come into contact, there is always transference of material from each object onto the other. In other words, you cant interact with a live system with out leaving some sort of trace on that system. This is part of why it is so important to document every thing that you do on a system while you are investigating.

F. Order of Volatility

Below is the order of volatility.

- System Memory
- Temporary File Systems (swapfile/paging file)
- process table and Network Connection
- Network routing information and ARP cache
- Forensics Acquisition of Disks
- Remote logging and Monitoring data
- Physical configuration and network topology
- backups

This list is important because it will dictate what actions you take while doing an investigation. You should seek to gather the most volatile information first and the least volatile information later.

G. Practical tips

When investigating machines there are some things that you shouldn't do. Firstly, It is important to have your tools installed on some sort of external media. This should then be run from the external media. You should never install this software on the suspects machine. as you are modifying evidence. When storing other evidence such as memory dumps or registry logs, you should also make sure not to store these on the suspects machine. There are several options for doing this such as, a network share or some sort of other external media. This ensures that you are preserving the suspects machine.

H. RAM

We get get lots of different things out of ram. We can get things like all running processes, cryptography information, passwords, and commands run on the command line. Memory Dumps are one of the most powerful tools you can use to see what was happening in a system and any given time. This can also be used for investigation into malware attacks. There are also many important things about memory and how it works at the software level and physical level that we will talk about in later lectures.

I. Volatility

This week in class we learned about a new tool called Volatility. This allows us to examine many different things in a memory dump. There are also many different plugins for this tool. This will allow us to examine many different things in memory. This is piratical because this will help us find things in memory that we would miss if we were just viewing raw memory. We can also derive what operating system the device is from using this tool. This can be handy because some of the commands wont be able to run on certain operating systems.

J. Timeline creation and Analysis

Another thing we learned about this week that is very important time line creation and Analysis. This is the process of putting together a timeline of what happened on a suspects machine or on a machine that may have been attached. There are many tools that can be used to do this. One part of this that is very important is the mft file or the master table file. This will allow us to put together a time line of what happened with all the files on the target machine. We can use volatility to view these files. There are also a number of tools that will allow us to import this file and view it in a nicely formatted way.

K. Data Recovery

This is also know as data carving. This is when we recover data on some piece of media that was deleted. The reason that this can be done is because when you delete something its not really deleted. Really what's happening is that some flags are changed such that this space becomes available to be written over. However, the data is still there and can be read if you know how to read it. The only way data is truly deleted is that it is written over, wiped, or destroyed with a 12 gauge. This will allow us to recover all sorts of different media. There are even tools that can recover deleted photos. Some times its possible that you it's not possible to recover the whole file. There are tools to handle this that will allow you to recover part of a file.

III. VOCABULARY

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

- **Evidence:** Any thing you can use to prove or disprove a fact.
- **Triage:** Can I proof in multiple different ways? Such as log files, registry, database entries, or sql log files.
- **mft:** Master file table. This file allows you to see the history of what happened to the files.
- **Data Carving:** Recovering deleted files from any type of media.