CPE457/557 Software Reverse Engineering

**14 - process monitoring**

# Malware Activity

**Lab Description:** Using dynamic analysis tool Process Monitor, apply the correct filters to identify relevant information from the sample.

**Lab Environment:** Use of variety of tools is needed for this lab. It is recommended to do this lab in a virtualized environment. The tools we will be using are:

* Process Monitor (ProcMon)
* Text editor
* Process Hacker 2

**Lab Files that are Needed:**

* CryptoLocker.pml
* CryptoLocker.txt

### **Lab Exercise 1 – Using Process monitor**

*Learning Outcomes 1, 2, & 3*

Use *CryptoLocker.txt* & *CryptoLocker.PML*.  The TXT file is a capture of process activity at the time of the infection, the .PML is a log from Process Monitor during the same attack.

1. Identify the malicious process, what is its process ID (PID)?
2. What process started this process?
3. Describe the process activity for the malware.
4. Did the malware modify any registry keys? If so, what is the significance of the keys it modified?

## What to submit

Submissions should be neatly organized. Each question should include at least one screenshot and a brief explanation if possible.