Module - 09

**Process Monitor**

# 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 Setup

To complete this lab the students only need access to Process Monitor.

### **Lab Exercise 1 – Using Procmon**

*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)?   
   *The student can identify the malicious process by inspecting the TXT file and noticing the abnormal process name {213D7E33-3912-1C20-3D38-1A0B15CDFFF3}.exe, which has a PID of 3196. This has a child process running with a PID of 2052. If the student analyzes the ProcMon log, they’ll determine that PID 2948 created PID 3196 and was no longer running when the process listing (TXT) file content was captured.*
2. What process started this process?  
   *The sample was executed with Bash (PID 3636) which created PID 2948, this process relocated the malware and spawned a new instance with PID of 3196, which has a child process of 2052.*
3. Describe the process activity for the malware.    
   *Students should focus on critical activity such as registry modification, process creation and file system modification. Students can easily get list in all of the reads that a process performs during normal operation. They can also misunderstand filters, particularly in the operations section. For example. CreateFile is not just used to create a file but also to obtain a handle to an already existing file. A discussion on the Windows API is appropriate before delivering this content.  
     
   Process Activity: discussed in the answer to question 2.*  
   *File System Activity: filter on Operation -> WriteFile: PID 2948 wrote a new file in C:\Users\User\AppData\Roaming\{213D…}.exe. This is common behavior; the sample is relocating itself for persistence. It also writes to ntuser.dat.LOG1 and NTUSER.DAT but this is normal activity for a process.  
     
   Registry Activity: PID 2948 creates the sub-key - HKCU\Software\Microsoft\Windows\CurrentVersion\Run\CryptoLocker with a value of C:\Users\User\AppData\Roaming\{213D7E33-3912-1C20-3D38-1A0B15CDFFF3}.exe. This is done for persistence, as RUN will run any program in this list when the user logs in. This also matches with the file system activity we observed.  
     
   ProcMon does not do a good job of capturing network activity.*
4. Did the malware modify any registry keys? If so, what is the significance of the keys it modified?  
   *Yes, see answer above. This is importance and while the question may be redundant, stresses analysis I want the students to perform.*