Module - 09

**Monitoring Malware**

# Malware Activity

**Lab Description:** This lab will be presented with two activates of identifying malware network activity.

**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 ProcMon and Wireshark.

**Lab Files that are Needed:**

Crypto locker & CryptoLocker.PML are used in the first activity. CryproLocker.pcap & Word-Dropper.pcap are used in the second activity.

### **Lab Exercise 1:**

*Learning Outcomes 1, 2, & 3*

Use CryptoLocker.txt & CryproLocker.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:

* Identify the malicious process, what is its process ID (PID)?
  + 428
* What process started this process?
  + It was started by bash.exe. Maybe hollowed
* Describe the process activity for the malware.
  + It queries a lot of registry’s and makes changes to most of them. It also creates multiple files, reads them and closes them. It also changes the hosts files and adds its own address to the list.
* Did the malware modify any registry keys? If so, what is the significance of the keys it modified?
  + Yes, one of the keys it changes the host file. This file holds the address of your default host. For example, if google is your host than it will change its address from google to the malware website.

**LAB EXERCISE 2:**

*Learning Outcomes 1, 2, & 3*

The purpose of this part is to understand the behavior of malware based on its network activity of CryptoLocker.pcap. Answer the following questions by providing short answer and/or screen shots:

* What domains do you think the malware tried to connect to?
  + Hit-malware.opendns.com – 67.215.66.149
  + Server.speedytelecom.net – 184.164.136.134?
  + Li624-4.members.linode.com – 217.71.250.4
  + None - 65.172.31.19
  + None – 65.55.200.138
  + Bcast.magtouch.co.za – 144.76.192.135
* How many were there roughly?
  + 6
* Look up some of the IP addresses that were resolved using this service <https://ipinfo.io/> (or any you prefer) – did you notice any trends in the IP’s used?
  + It attempts to get to large cities throughout the world. It mainly tries to get to one that is in San Francisco.
* What happens when the sample is able to connect to a host?
  + It used Get commands to request an .exe file from the server it connects to.
* Does it appear that the sample was able to successfully connect to any hosts? Hint, see the DNS query number 808 and the resulting TCP stream.
  + Yes

**LAB EXERCISE 3:**

*Learning Outcomes 1, 2, & 3*

The purpose of this part is to understand the behavior of malware based on its network activity of Word-Dropper.pcap. Answer the following questions by providing short answer and/or screen shots:

* What domains were used?
  + ip78.ip-167-114-56.net - 167.114.56.78
  + akamai.sxflsdch38r.sdnet.net - 64.33.232.56
  + static-192-165-52-250.cust.crystone.se - 192.165.52.250
  + Microsoft Corporation - 40.83.182.229
  + Microsoft Corporation - 104.45.215.238
* What happened after the domains tried to connect?
  + It uses gets to get a /configs then downloads a .crt file. DNS standard quires called for a TCP handshake that uses GET commands to pull different file types.
* What did the sample request and how did it request it?
* Do you think the sample was successful in infecting the host?
  + Yes, by the files transferred back and forth it looks to have been successful.

## What to submit

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