Module - 09

**Network Monitoring Malware**

# Malware Activity

**Lab Description:** The goal of this lab is to analyze

**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:

* ApateDNS
* Wireshark
* Process Monitor (ProcMon)
* Text editor

**Lab Files that are Needed:**

* Domain\_generation.exe
* Word-dropper.zip
* CryptoLocker.pcap

### **Lab Exercise 1 – Using Wireshark to perform Live collection**

*Learning Outcomes 1, 2, & 3*

Using both *ApateDNS* and *WireShark*, capture the DNS requests made by domain\_generation.exe and answer the following questions:

1. How many domains were generated?
2. Is there a discernible pattern to the domains used?
3. Did they change with each run of the program or were the domains consistent?

**LAB EXERCISE 2 – Using Wireshark to Analyze a PCAP**

*Learning Outcomes 1, 2, & 3*

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

**Task 1 - Use CryptoLocker.pcap**

* What domains do you think the malware tried to connect to (how many, roughly)?
* 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 IPs used?
* What happens when the sample can connect to a host?
* Does it appear that the sample was able to successfully connect to any host? Hint, see the DNS query number 808 and the resulting TCP stream

**Task 2 - Use Word-Dropper.pcap**

This capture came after opening a malicious Word Document.

* What domains were used?
* What happened after the domains tried to connect? What did the sample request and how did it request it?
* Do you think the sample was successful in infecting the host?

## What to submit

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