Module - 09

**Network monitoring**

# 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
* Process Hacker 2

**Lab Files that are Needed:**

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

## Lab Setup

*domain\_Generation.c*: This file requires you to compile using Microsoft Visual Studio command-line interface (CLI) to access the Windows API.  
  
**> cl domain\_generation.c**

This file allows students to analyze a program with trivial domain generation without the need to handle live malware. Consider adjusting the program to modify timing and the impact that may have on analysis in a sandbox (i.e. timeout issues). The primary goal of this sample is to identify domain usage. Also consider showing the disassembly of the program logic to generate domains then compare static analysis to dynamic analysis, this can be used to highlight a situation which is more effective using a dynamic approach.

*Word-dropper.pcap and CryptoLocker.pcap:* Both of these PCAPs will require the student to use WireShark to analyze and identify relevant sample communication. The use of PCAPs avoid students having to handle malicious software. Focus can be given on filtering basic protocols such as HTTP and DNS, then following those conversations to identify key pieces of information.

### **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 the sample and answer the following questions:

1. How many domains were generated?

*Without modification, the program is designed to generate 100 DNS requests.*

1. Is there a discernible pattern to the domains used?  
   *No, each domain is dynamically generated and not synchronized. There will likely be some overlap but each run of the program should generate largely unique domain names.*
2. Did they change with each run of the program or were the domains consistent?   
   *They will change – this is a good point of discussion on domain generation algorithms and how they synchronize (if they do). Static analysis could also be discussed in regards to determining exactly how the DGA works – as it may not be clear by basic dynamic analysis.*

**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)?  
  *Approximately 85 – you can use Statistics -> DNS to get an overview of DNS activity for this PCAP. Students should also note that many domains resolve to the same IP and that some of the DNS queries were essentially blocked by using OpenDNS as a domain name server.*
* 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?  
  *This is designed to get students research IPs, there is likely no real pattern as IPs resolve around the globe.*
* What happens when the sample can connect to a host?  
  *It will attempt a POST with binary data, likely information about the victim’s machine.*
* 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.  
  *Yes, the host and subsequent HTTP request shows not only the POSTed information, but also an apparent response from the host. Without further analysis, it is difficult to understand what this data represents. Since this is malware, the response likely contains information such as the encryption key.*

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

This capture came after opening a malicious Word Document.

* What domains were used?  
  *Filter on DNS, there are only a few requests – endlessdeals.info and bigdiscountsonline.info should stand out. Since these may be legitimate hosts, they were likely compromised to host malicious content.*
* What happened after the domains tried to connect? What did the sample request and how did it request it?  
  *Filter on HTTP or follow TCP request after DNS. Both domains were used for a GET request for a TXT file. Both hosts responded with a 404 error.*
* Do you think the sample was successful in infecting the host?   
  *Since both requests returned a 404 it was not successful and the attack failed.*