Lab 01 - Office Documents

For this lab we’re going to be working with **oledump** from Didier Stevens. Oledump is already installed in the REMnux VM that is available in the IA lab. You can optionally download **oledump.py** from:

<http://blog.didierstevens.com/programs/oledump-py/>

You may need to install additional dependencies to get the script to work. Once you have the script working, review the documentation by invoking the script:

**$ python oledump.py -m**

You may want to pipe it through **more** to allow you to read all of the output:

**$ python oledump.py -m | more**

Use these tools as well as anything else you’re familiar with to analyze the following files:

**Provide responses with screenshots and explanations in support of each.**

**Password is infected**

**File 1 - MD5: 342a997b2c5ab65787188287af4f2dba**

* Use the **file** utility from a Cygwin terminal to inspect the file:  
  file 342a997b2c5ab65787188287af4f2dba
* Use **Oledump** to inspect the file, does it contain macros? If so, inspect them.
* Is this file malicious?

**File 2 - a530354ffc4d8272feff07cb6fdd064831a2bcfc205b97623800ff01a8bfdada - Drops Dridex?**

* What file type is this sample (i.e. Word, PowerPoint, etc)?
* The macro code makes a connection to a URL, what is the URL? Use static analysis only!
  + HINT: You won’t find it as ASCII text; you will need to convert integer values into chars. Writing a small script, e.g. Python, might help you to accomplish this.
* Describe the functionality in this Maldoc. What is it trying to do?

**File 3 - b4b4f0623f3fd5652b4fe53147831f471a1d691f83428756b239a2969ac1c435**

* What streams do we want to look at here? Why?
* Once you figure this out, refactor the code and make it more readable.
* Where does the malware start?
* Are there any distractions?
* Explain what goes on in this malware in terms of the actual malicious functionality? What is the end result? What does it do? What is the overall purpose of this malware? Use yours words and 2-3 supporting screenshots.

**Deliverable:**

A Word Document or PDF with answers to the lab questions.