Lab 05 – Malicious Documents

In this lab, you will work with malicious documents and provide an analysis to determine what malicious behavior the documents contain using a variety of tools available. Determining the packaging, code obfuscation techniques, identifying potential behavior, and generating a list of possible IOCs will be helpful with your analysis. Maldocs, short of Malicious Documents, tend to contain macros. Not all macros contain malicious intent. You are tasked with trying to determine what the level of malicious behavior is for each file you analyze.

Once you have your analysis environment setup and the maldoc files are downloaded, **it is important to ensure that you are NOT connected to your local network or the internet**. These files contain malware, albeit old malware, they are still malware.

The lab files containing malware are archived as a .zip file. This is password protected. Please use the following password to extract these files within task one:

m@lwar3!

Complete the following tasks:

TASK ONE: Virtual Machine Setup

1. Engaging in malware analysis is an exciting, yet dangerous event. You must proceed with caution so you don't contaminate your host machine or another host on your network. It is important to ensure you have an isolated environment after you download all of the necessary analysis tools. Let's begin by downloading and installing a Linux Toolkit for Malware Analysis called REMnux.

   a) The following VMs should be downloaded, installed and running within your hypervisor of choice:

      ✓ REMnux VM
      → https://docs.remnux.org/install-distro/get-virtual-appliance

   b) Once you have your VMs downloaded and installed within your hypervisor, you should make sure oledump.py is installed. If it is not, or it's not up to date, please download it and install it from:

      ✓ oledump
      → 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
```

c) Once you have the tools installed for your analysis, download the samples file for this lab.

d) Isolate this VM from the network by simply disabling the NIC or placing the vmnic in an isolated vmnet.

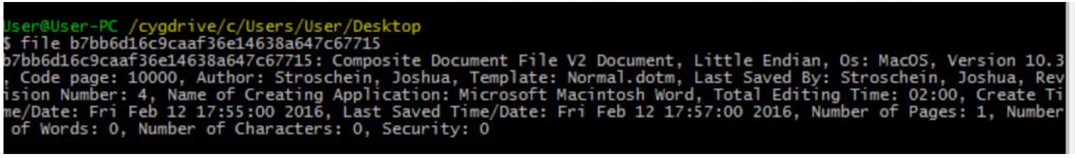
TASK TWO: Malware Analysis

a) Analyze three files using various tools at your disposal to determine what the malware is doing in the background.

i. For each file sample:

File 1: **MD5: b7bb6d16c9caaf36e14638a647c67715**
File 2: **MD5: 748ef5288c8388d43a89515ef43457a0**
File 3: **MD5: 7a618482be272bb1fcb4af69a3f649a3**

b) Use the **file** utility from a terminal to inspect the file:



```
User@User-PC /cygdrive/c/Users/User/Desktop
$ file b7bb6d16c9caaf36e14638a647c67715
b7bb6d16c9caaf36e14638a647c67715: Composite Document File V2 Document, Little Endian, Os: MacOS, Version 10.3
, Code page: 10000, Author: Stroschein, Joshua, Template: Normal.dotm, Last Saved By: Stroschein, Joshua, Rev
ision Number: 4, Name of Creating Application: Microsoft Macintosh Word, Total Editing Time: 02:00, Create Ti
me/Date: Fri Feb 12 17:55:00 2016, Last Saved Time/Date: Fri Feb 12 17:57:00 2016, Number of Pages: 1, Number
 of Words: 0, Number of Characters: 0, Security: 0
```

c) Use the oledump utility to inspect the file.

i. Does it contain macros?
ii. How can you tell if it contains macros?
iii. If the file contains macros, identify the streams that contain macros.
iv. If the file contains macros, inspect them.
v. Attempt to extract those streams.
vi. Can you identify any significant IOCs?
vii. Do you think the file is malicious?
viii. What makes you think the file is malicious (or not)?

d) Use the **strings** utility to inspect the file.

i. Try to identify key strings and objects.
ii. *Optionally*, if you have a programming/software development background, review the function calls. What do you think is occurring?

e) After you have completed your manual analysis, use a Windows VM or even your host computer and connect to the internet. Open your favorite web browser and browse to https://www.hybrid-analysis.com/ to complete your analysis.

i. Sometimes it’s nice to have a second opinion or use an automated tool along with your manual analysis to gain the full picture of what’s occurring with this malware sample. Use Hybrid Analysis to help with the deobfuscation of the code and gain more insight into what each malware sample is doing. Search for each sample using the MD5 hash.

ii. Investigate the process activity section. Attempt to figure out what this malware is doing. (hint: what is the command doing…is there a domain involved? If so, what is it? It’s ok if you can’t figure this out… this is not an advanced malware analysis course. I’m just introducing you to malware analysis here. 😊

DELIVERABLE:

1. Complete a professional write-up and include the following information:

    a. **Description:** Brief description, such as an executive summary, depicting an overall view of what topic or technology you are concentrating on within this lab. Keep this short and to the point. Think like a consultant and be mindful that what you are providing should represent you as a professional in the industry.

    b. **Topology/Diagram:** Use Microsoft Visio, or Lucid Chart, to create an aesthetically pleasing network topology or graphical representation depicting an overall view of what you're working on. This may include the source, the target organization, various tools, websites your visiting, file hashes, IP Addresses, domain names/information, credential used, and anything else you feel would be beneficial to add.

    c. **Key Syntax:** Sometimes it's nice to include key syntax used. For instance, if you're not a Linux guru, it might be nice to include how you configured a static IP Address in the Linux CLI, or what files you needed to modify in order to configure a primary DNS server IP Address or domain suffix. This is especially useful for tools that you may only use once in a while. Be specific here.

    d. **Verification:** Provide key screenshots that display verification that all tasks and all steps of the lab have been completed. For instance, if you used a specific tool, ensure that the reader knows the syntax you used to execute the tool and the intelligence gathered from the tool. Make sure you provide a description of what the screenshot is showing. Do not simply add the screenshot and state, "here is the screenshot". These descriptions and screenshots should paint a story of the work you put into this lab and verify you have successfully completed the virtual environment configuration. Be thorough and professional! A few things to focus on would be:

        i. Screenshots and tables documenting the IOCs you've acquired during your analysis.

        ii. Think of this report as a professional document that you would be handing to a customer (or provided to management for an organization you work for). Be professional and thorough!

    e. **Conclusion:** Wrap up your lab report with a short conclusion. If something did not work, state it. If everything did work successfully, state that as well.

    f. **References:** Make sure you include any works cited here as well as throughout your lab report. If you looked something up, include it.

2. Upload the following file(s) to the assignment within iLearn:

    a) Your .pdf file of your analysis report.

Good Luck with your lab!