Malware Reverse Engineering
Practical Assignment 4
Spring 2023

J.N. Wilson

Unknown Sample Malware Analysis

You are given a 7zipped pdf file `Practical4_sample.pdf.7z` (password *infected*) that was collected during a spear phishing campaign. You've been asked to prepare a report discussing what the impact of employees receiving and opening this document might be. You've also been asked to provide any indicators of compromise you might be able to identify and to prepare a YARA rule that should identify the documents and possibly variants thereof.

You have until the date specified on Canvas to complete your assignment and turn in your report.

Elements to Include in your report

Provide a single executive summary giving a rough description of the malware artifact, the expected behavior of the malware, the risk that infection with the sample could pose to an organization, methods of potential detection, and what can be done to mitigate infection.

Then analyze the malware artifact completely. For each aspect of anlaysis identified below, discuss the methods you used to identify the information you found out about the malware and its behavior. (Essentially give a walk-through of the steps one can take to reproduce the information you discovered, together with appropriate screen-shots or fragments.) Be careful to identify any special measures you must take (such as providing javascript definitions or making substitutions in code) in order to execute any code you may run. Be sure to discuss the following aspects of the malware:

- Interesting metadata such as internal dates, document and section names, etc.
- Languages and methods employed by the malware in downloading files or exploiting vulnerabilities.
- IP addresses or host names the software may attempt to contact.
- Files that are or may be created or executed. (If these are executables or documents, analyze them as well.)
- Any other methods or structures you find interesting.
- A YARA rule that will identify the document that is not be triggered by any of the Practical Malware Analysis malware artifacts.

Rubric

Each aspect of the report is assigned a point total. Feel free to provide section headings for each of these aspects of the report. The point totals are as follows:

(5) Report Title Block

(20) Executive Summary

(20) Analysis of Executable Code and Methods Employed

(15) Analysis of Possible Network Behavior

(20) Analysis of Dropped or Created Files

(15) YARA rule

(5) Excellent Reporting

The points assigned to your report for each aspect of reporting will reflect how well you identify and communicate the information you provide. In the title block, for example, five items must be supplied and each item garners one point. In each of the other sections, points will be awarded based on how much you uncover and how well you communicate what you have found. If I mention specific information that must be provided then not providing it will reduce your point total. Communicating a few observations well and providing excellent detail can overcome a lack of identification of other properties of the malware. Providing incorrect information or not providing information to support your conclusions will reduce your grade. Understand that I am grading what you demonstrate you know in your report, not what you actually know.

Questions and Observations to guide your thinking

- If you have not employed the program *exiftool* in the past, you may want to find out what it does.
- If you do not know how to extract a stream or embedded file from a pdf document, you may want to find out how to do that.
- If you find obfuscated code, make sure you can somehow extract useful information from it (either by deobfuscating it or using tools that can find information within that code).