Malware Reverse Engineering
Practical Assignment 3
Spring 2023

J.N. Wilson

March 24, 2023

Unknown Executable

You are given a piece of malware in the file *sample3.7z* in the Desktop directory of each VM. The 7zip password for that file is *infected*.

You've been asked to find out what you can about this program. You have until the date specified on Canvas to complete your assignment and turn in your report.

Do all the good things you've learned to do from Practicals 1 and 2.

Your report should take the following form:

1. Report Title Block

The report title block should include

(a) Report title

(b) Date of preparation

(c) Your name

(d) Your email address

(e) Assignment and Class

2. Executive Summary

Briefly describe the suspected purpose and observed behavior of this software including a summary of any obfuscation methods, notable imports, registry activity, file system activity, and network activity. Also briefly note any host or network indicators that might be used to identify the presence of this malware.

3. Static Analysis

Check for at least the following:

(a) Identify the apparent compilation date of the program.

(b) Identify whether the program is a Windows GUI or Command-line program.

(c) Is the program packed? Use multiple indicators, explaining the significance of each.

(d) Identify the PE file sections and their likely contents.

(e) Identify any suspicious functions imported by the program.

(f) Identify any suspicious or relevant strings (IP addresses, urls, process names, file names, etc.).

4. Dynamic Analysis

Check for at least the following:

- Registry Keys created/modified by the malware.
- Files created/modified by the malware.
- Services or processes started by the malware.
- Machines and services the malware attempts to identify or contact by IP or domain/host name.
- Interesting behaviors that occur after the malware has executed.

5. Indicators of Compromise

Identify any host- and network-based indicators of infection that could be used to detect the presence of this program. Be as specific as you can.

Also include a Yara rule that you have tested against all the Practical Malware Analysis .exe and .dll files to insure none of them are false positives. I will ask for a separate Yara rule text file to be submitted. Make sure you follow the following two requirements:

Rubric

Each section of your report is assigned a point total. The point totals are as follows:

(5) Report Title Block

(10) Executive Summary

(30) Static Analysis

(30) Dynamic Analysis

(20) Indicators of Compromise

(5) Excellent Reporting

The points assigned to your report in each section will reflect how well you identify and communicate the information associated with the section. 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.

Suggestions to guide your thinking

- Save a copy of the code before you run it just in case. (BTW, this is always a good idea.)
- The program does some anti-debugging. Check out calls to `CreateWindowExW` in particular to overcome this.
- You will likely want to run `accept-all-ips start` so you can capture traffic directed at known IP addresses.
- It looks like there are a few warnings in ghidra about bad instructions in `FUN_004152a3`. They don't seem to have the same problem, though. What the heck is going on there?
- And what is happening in `FUN_00415af8`?