Malware Reverse Engineering
Practical Assignment 1
Spring 2023

January 24, 2023

Unknown Sample Malware Analysis

You are given a malware sample in a 7zipped file named *sample1.7z*. This sample can be found on on the desktops of your Remnux, Windows 7, and Windows 10 hosts. You can inflate this program using 7z. (The password is *infected*.)

You have been told that this was found on a machine and was flagged by an intruston detection system as being *suspicious*. You've been asked to find out what you can about this program. You have until the due date published on Canvas to complete your assignment and turn in your report.

I suggest you reserve four hour or longer blocks for analysis of this malware and release your reservation as soon as you are finished. Take screen shots, make good notes, record everything necessary for either your report or to continue analysis in a later Netlab session. You can store artifacts on the Ghidra server using the account credentials supplied to you. The ghidra machine is directly accessible from your Remnux host and can be made accessible to other hosts by adjusting their network parameters or by setting Remnux to do ip forwarding.

I strongly suggest you make a task list identifying all the steps you plan to take in dynamic analysis in the order in which you take them, e.g.:

- Win: Start Process Hacker
- Win: Start Procmon, then pause and clear
- Win: Start RegShot and take 1st shot.
- REMnux: Start fakedns
- REMnux: Start INetSim
- REMnux: Start Wireshark and begin listening
- Win: Un-pause Procmon
- ....

This malware is more complicated than the examples you've seen in the text, but you should be able to find out many of its interesting properties. You may need to consult MSDN documentation online to identify the behavior of function calls that are made (e.g. Google for search terms like *GetCommandLine MSDN*). If you don't know the expected argument and return types and their possible values, it is impossible to understand what the program is doing.

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 *notable* obfuscation methods, imports, registry activity, file system activity, and network activity. Make sure you clearly identify the type of malware you think this is (adware, bot, ransomware, trojan, spyware, wiper, etc.) and provide (very brief) evidence you have classified it correctly.

Also briefly note any host or IPS signatures that might be used.

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:

(a) Registry Keys created/modified by the malware.

(b) Files created/modified by the malware.

(c) Services or processes started by the malware.

(d) Machines and services the malware attempts to identify or contact by IP or domain/host name.

(e) 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. False positives are the bane of host and network IDSs.

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

(40) Dynamic Analysis

(10) 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 **your grade depends on what your report demonstrates that you know, not what you actually know**.

I reserve five points for excellent reporting. These points are awarded if your report goes above and beyond what is expected. If, for example, you creatively reverse engineer a clever coding scheme, identify an API used by the malware for communication, create a server that responds to requests, or identify novel properties of the malware that are not evident on normal inspection, you can be assigned these points. Do not become obsessed about these points, you can get a solid A without them.

Questions and suggestions to guide your thinking

- Pay close attention to any files created by the malware. What are they used for?

- If the malware connects to other machines, can you identify what it is trying to communicate?

- Check to see if the malware is persistent. Does it operate after reboot? Does it operate after logout and login?

- Look at the function at address `0040350F`. Can you figure out what the arguments are by looking at the code in this function? What do you think this function does?