ECE 570 Project I: Investigating an Infected Machine

(Weight: 10%; Due June 8, 2020)

Case Description

A bank was attacked through spear phishing emails that pointed to malicious executables, which were clicked on by employees. This triggered ransomware infection of some machines hosting critical files for the bank's operations. After finding out about the ransomware infection, an investigation was launched immediately, where first responders were able to collect memory images of the suspected infected machines.

As a forensics investigator, your mission is to analyze one of the memory images and report on any suspected activities found.

Task

Provide a report analyzing suspicious activities by answering the following questions:

1. Identify running processes, and determine which ones look suspicious and justify why [3%].
2. Determine and explain the relationships (i.e., parent-child) between the suspicious processes identified above. Identify which process is most likely responsible for the initial exploit. [1.5%].
3. From the above list of suspicious processes, identify at least one process with hidden or injected code/DLLs, and identify corresponding hidden DLLs [1%].
4. Extract the executables for one of the suspicious processes identified above, and check whether at least one of these files is malicious using an online virus scanner [1%].
5. Identify the URLs (and a corresponding IP address) for one of the possible remote command and control servers visited by the malware. Confirm that the selected URL is malicious using an online scanner. Note: You can limit the search to the initial (suspicious) process that triggered the exploit, or any other relevant process [1.5%].
6. List available registry hives and identify a potentially malicious hive from the list. Explain and justify why such hive could potentially be malicious [2%].

Indicate the tools used for each of the questions and provide screenshots showing the typed commands and results. Justify your answers by providing convincing rationale.

Evidence

The memory image can be downloaded at:

https://drive.google.com/open?id=1o7K91dOek-DmHwCl6dWhvhV2wvIMnLCn