Assignment 01: Investigating an Infected Machine

Due Date: Jan 28, 2019, worth %15 of the total course mark

Case Description

One of the managers of a company fell for a spearphishing scam, which was delivered through a spam email containing a file attachment. After opening the file, the manager did not notice anything, however, recently they have started experiencing unusual activity in the company's accounts. This triggered an investigation, where first responders were able to collect a memory image of the suspected infected machine.

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

Requirements

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

1. Identify running processes, and determine which ones look suspicious and justify why process is most likely responsible for the initial exploit. [4%]
2. Identify suspicious network connections from/to the victim machine, and determine which process(es) is(are) most likely responsible for the initial exploit, by refining tthe previous list of suspicious processes. [4%]
3. Identify the IP addresses and locations of the suspicious machines involved. [1%]
4. List the sockets involved, and identify suspicious ones by analyzing the timeline (i.e. created around incident timeline) [3%]
5. Extract all executable (files) from the suspicious processes running on the victim's machine (as determined in question 2), and ccheck whether some of these files are malicious using an online virus scanner. [1%]
6. Identify the URL for one of the financial iinstitution's that may be in the suspected process(es) memory space. [1%]
7. Identify at least one related IP address and corresponding location (in addition to the ones found earlier) that may be in the suspected process(es) memory space. [1%]

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

The memory image can be downloaded at:
https://drive.google.com/file/d/0B1xnRxT-Y8DMTlUwSlo1S2R2MTg/view?usp=sharing

Important Notes:

- Document your answer using screenshots of your scanning activities and explain the scanning methods you used. Report both your successful and failed attempts.
- Any collaborative or plagiarism activities will be sanctioned (i.e. collaborate and will be assigned zero scores).
- Your submissions need to be typeset and in pdf.