Elec 570 – Project III: Network Forensics Investigation

(Weight: 20%; Due: July 31, 2020)

Case Description

Joe Jacobs, the security officer responsible for the network of a corporation, is suspecting that the machine used by one of the employees has been infected with malware, after visiting some compromised website. The suspicion was based on observing significant departure of the infected host activity from the network baselines.

Network traffic sample involving the compromised host activity is provided in TCPDUMP format (as a separate file: elec570-project-2020.pcap). As a forensic analyst, you have been tasked to analyze the network capture and decode the suspicious activities involved.

The trace file can be downloaded at:

https://drive.google.com/open?id=1gSsbAFZjYO8hpmIAYInyBbyreCC-zh79

Task

More specifically, you must provide answers to the following questions:

1. Identify the following characteristics for the infected host (2.5%):
   a. IP address of computer
   b. Host name of computer
   c. MAC address of computer
   d. Operating System (OS)
2. What is the IP address and URL of the compromised website the user looked at that triggered the malware traffic (i.e. before the malware traffic happened)? (2.5%)
3. What is the IP address and domain name that delivered the malware? (2.5%)
4. Identify the type of malware involved and check the payload by running the associated file (or files) against an online virus checker (i.e. VirusTotal). (3%)
5. Identify **other** malicious hosts or sites with which the compromised host interacted. Only malicious hosts should be included in this list. Provide your response in a table listing the following (4%):
   - Host name/URL and IP Address
   - Role
   - Communication protocol or service
   - Date and time range of the interaction (i.e. start date/time – end date/time)

6. Give an outline of the attack scenario by describing it in a few paragraphs and by providing a graphical sketch. The attack scenario must include both the infection and post-infection steps (4%).
7. Discuss remediation and mitigation solutions for such threat (1.5%).

Important Note: For questions 1-6, ensure that you justify your answers by providing screenshots of the analysis tools used and identifying related packets samples.

Tools

Feel free to use any tools you feel necessary in your investigation. In any case, the following combination of tools could be useful: Wireshark, NetworkMiner, p0f, Snort, and Suricata.