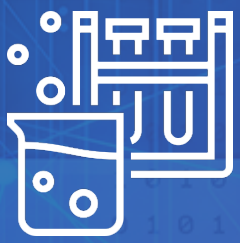
Lab Assignment



Cybersecurity Professional Program

Digital Forensics & Incident Response

Memory Analysis

DFIR-07-L3

Zeus

Lab Objective

Improve forensic investigation techniques learned during the lesson.

Lab Mission

Investigate the provided sample and locate the malware within it.

Lab Duration

20–30 minutes

Requirements

- Basic knowledge of memory analysis

Resources

- VirtualBox that includes NAT Network of:
  - Windows 10
    - ***Putty-64bit-0.74-installer***
  - SIFT Workstation (password: **forensics**)
    - **Volatility**
- Extra Lab Files
  - ***zeus.zip***

Textbook References

- Chapter 7: Memory Analysis
  - Section 3: Process Investigation
  - Section 4: Network Investigation
  - Section 5: Code Injection Investigation
  - Section 6: File & Process Dumping

Lab Task

Investigate the provided sample and locate the malware within it.

1. Ensure communication between the Windows 10 and SIFT machines.
2. Open the SSH service in the SIFT machine with ***sudo service ssh start***.
3. Transfer the file ***zeus.zip*** to the Windows 10 machine, and from there transfer it to SIFT. Use Putty to transfer the file with ***"C:\Program Files\PuTTY\pscp.exe" –P 22 zeus.zip sansforensics@[IP]:/home/sansforensics/Desktop***. This will put the file in the Sansforensics Desktop.
4. Perform memory analysis and attempt to find the malware with ***imageinfo***. Here, you will use the same command as in labs 1 and 2.
5. Investigate the processes with ***pslist*** or ***pstree***. While nothing seems suspicious, there is a lot of one ***.exe***.
6. Check the ***connscan*** and ***sockets*** volatility of the ***zeus.vmem***. There is a remote access connection with a PID. ***Grep*** the PID with the ***sockets*** command.
7. Next, we will create a directory to do a dump with ***malfind*** tagged to the PID to crosscheck the hashes on VirusTotal. Create a hash of the file with ***md5sum zeus/*.dmp***.
8. Perform a comparison of the hashes against VirusTotal.

Note: This was only a brief investigation. Many more things can be discovered with more advanced investigative knowledge.

Hints

Lab Task

- Use the ***ifconfig*** command to verify the connection between the machines (***ifconfig*** was introduced in ***NET-01***).
- The SSH default port is 22.
- Use ***pscp.exe -P [port] [file] [username]@[IP]:/[path to save]*** to transfer a file. (Introduced in ***DFIR-06-L3***.)
- **Volatility's *imageinfo*** can identify the memory's profile.
- **Volatility's *pstree*** and ***pslist*** can display used processes.
- **Volatility's *connscan*** and ***sockets*** can be used to test for network activities and connections.
- Dumping the executable's data can be performed with **Volatility's *malfind*** and ***flag --dump-dir***.
- The **md5sum** tool can be used to calculate MD5 hash values.