THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON DC

Computer Science 6907-10
Computer Network Defense

Homework #5

Kevin Yasuda
Matthew Norris

Memory Analysis

Compare and analyze two memory captures of the same system. Capture A was taken before any potentially bad behavior occurred (i.e. not infected). Capture B was taken after indications of an attack were detected.

- The memory captures can be obtained:
  - https://s3.amazonaws.com/gwucs.cnd.p2/CaptureA%2BB-MemoryAnalysis.zip

Answer the questions below and explain your answers - provide screenshots or details of your analysis to back up your findings/answers.

1) What OS is the memory capture of?
2) What process(es) exist in Capture A that do not exist in Capture B?
3) What process looks suspicious in Capture B and why? Explain how you have come to your conclusion.
    1) Does the suspicious process have any FILE handles different between Capture A and B? If so what are they?
4) What is the IP address of the host system in Capture A and Capture B?
5) What is the likely attacker's IP address? Explain how you have determined your conclusion.
6) Using the volatility malfind plugin, which segments (Process and Address) do you think are false positives or contain attacker code? Explain how you made your decision on each malfind finding.

Bonus (Extra Credit):
7) Can you identify a memory artifact (e.g. process handle) that would be a future indicator of a similar intrusion? Must explain your logic to get credit.

As usual for all of our homework assignments, state all assumptions made and why you made them.