SC4014 Concepts and Techniques for Malware Analysis

Assignment 1

Deadline: 11 Mar 2024, 2359Hrs

Context

You are working as a Digital Forensics Analyst as part of the Incident Response team in Advanced Cores Enterprises. You received an alert from your colleagues in the Security Operations Centre that they detected suspicious network activities originating from the computer belonging to one of the staff from the Finance department.

As part of your Incident Response Procedure, you have acquired the memory image from the suspected computer. You have been tasked to perform an analysis on the memory image, `assignment1.vmem`, and write a report to document your findings.

Guidelines

Here are some guidance (non-exhaustive) to help you along in your assignment:

- How did the threat actor first gain access into the machine
- What did the threat actor do after gaining access
- Can you identify any malicious processes/files/applications
- Can you identify any potential C2 IP addresses and ports
- Timestamps are your friend. Use them to help you track the threat actor's activities.
- **You can assume that all Microsoft Office application files on disk are legitimate (i.e Excel.exe, Word.exe, Outlook.exe, etc.)**
- The threat actor has left a secret message in the victim's computer that can be accessed using a password. He has kindly written down the password somewhere in the victim's computer. Are you able to find the password and retrieve the secret message?

Due to the nature of memory forensics, some of the information that you might need may no longer be present in the memory at the time of acquisition. In that case, you are expected to get that information through other means such as by dumping out the malicious files/processes and performing additional analysis on them. Rest assured that the contents covered from Weeks 1-5 is sufficient for this assignment. This means that you **are not expected to be reading assembly or using tools such as IDA**.

Instructions

Perform memory forensics on the memory image, `assignment1.vmem`, and write a report to document your findings.Your report should describe any suspicious/malicious activities that you can find from the memory image. All of your findings should be backed with evidence (i.e. screenshots) and an explanation on how you derive your findings from the evidence. In the event where you are unable to obtain conclusive evidence, you must clearly state that it is a hypothesis and explain how you arrive at your hypothesis.

Your report must be written coherently and, to the extent possible, present a comprehensive chronological account of the threat actor's activities. You will be graded on the completeness of your report, measured in terms of forensic findings and the accuracy of your proposed sequence of events. Do note that just dumping your findings with no evidence or explanation will not earn you any marks.

> Tip: While you are not graded on your report writing style, a neat and clearly labelled report makes it easier for the graders to read, track and mark your findings. It will likely put them in a better mood too.