**EXPERIMENT NO. 8**

|  |
| --- |
| **Student Name and Roll Number:** |
| **Semester /Section:** |
| **Link to Code:** |
| **Date: 27/10/2020** |
| **Faculty Signature:** |
| **Marks:** |

|  |
| --- |
| **Objective:** Execute the malware found in the file Lab03-03.exe while monitoring it using basic dynamic analysis tools in a safe environment. |
| **Outcome:** Understand the usage of basic dynamic analysis tools |
| **Problem Statement:** Extract information about the malware using basic dynamic analysis tools in a safe environment. |
| **Background Study:** Static analysis can reach a dead-end due to Obfuscation and Packing. Dynamic analysis is efficient and will show you exactly what the malware does. Extremely powerful, they should be performed only after basic static analysis has been completed, because dynamic analysis can put your network and system at risk. |
| **Algorithm/Flowchart:** |
| **Code(Solution):** |
| **Sample Outputs:** |
| **Question Bank:**   1. What do you notice when monitoring this malware with Process Explorer? 2. Can you identify any live memory modifications? 3. What are the malware’s host-based indicators? 4. What is the purpose of this program? |