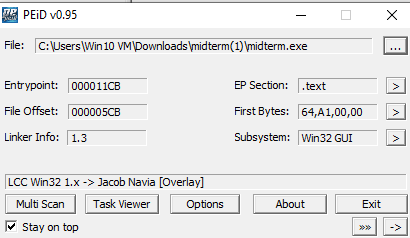
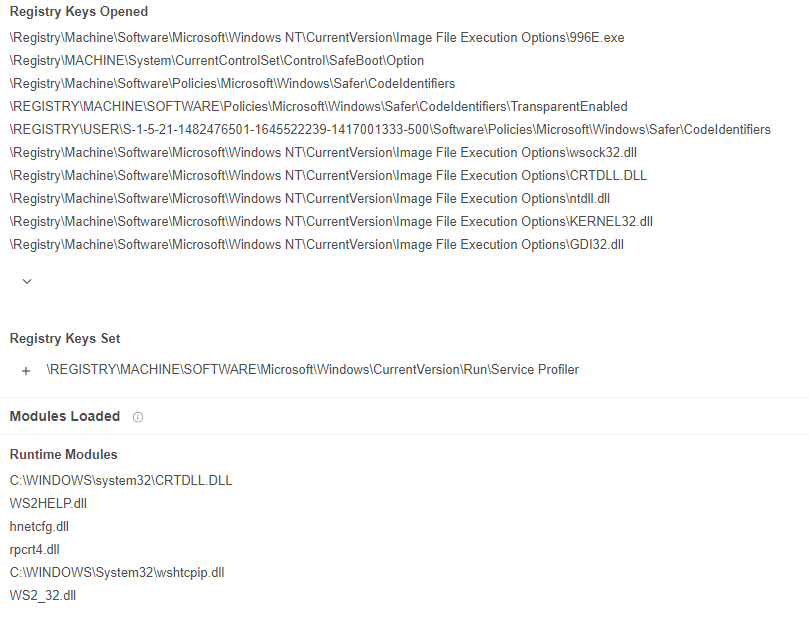
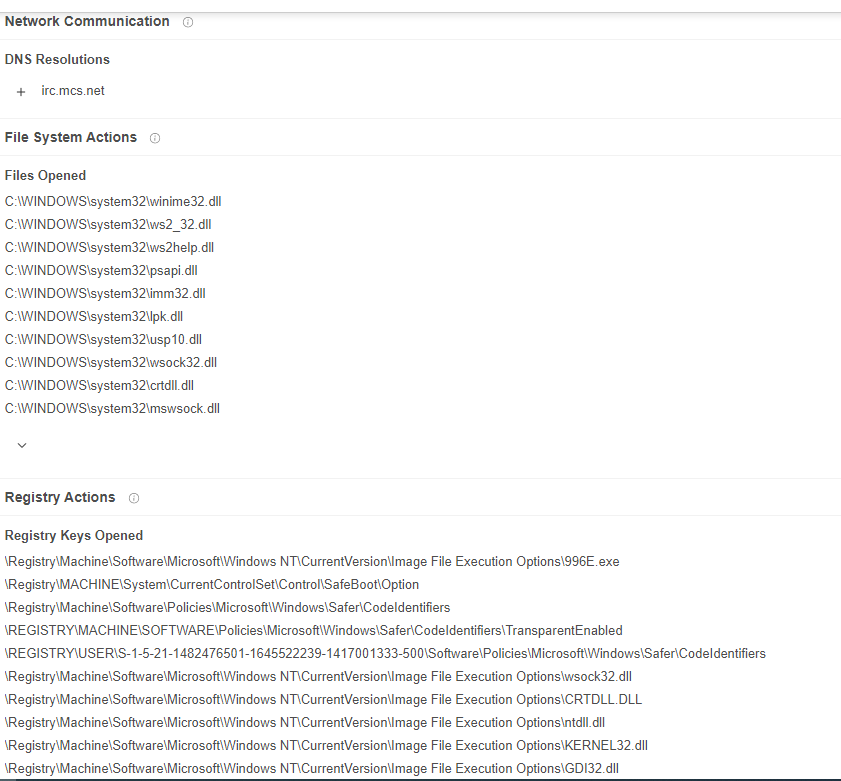
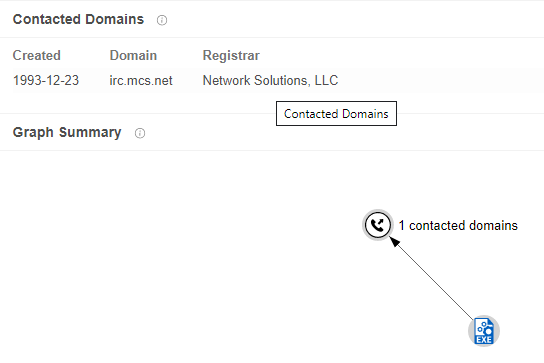
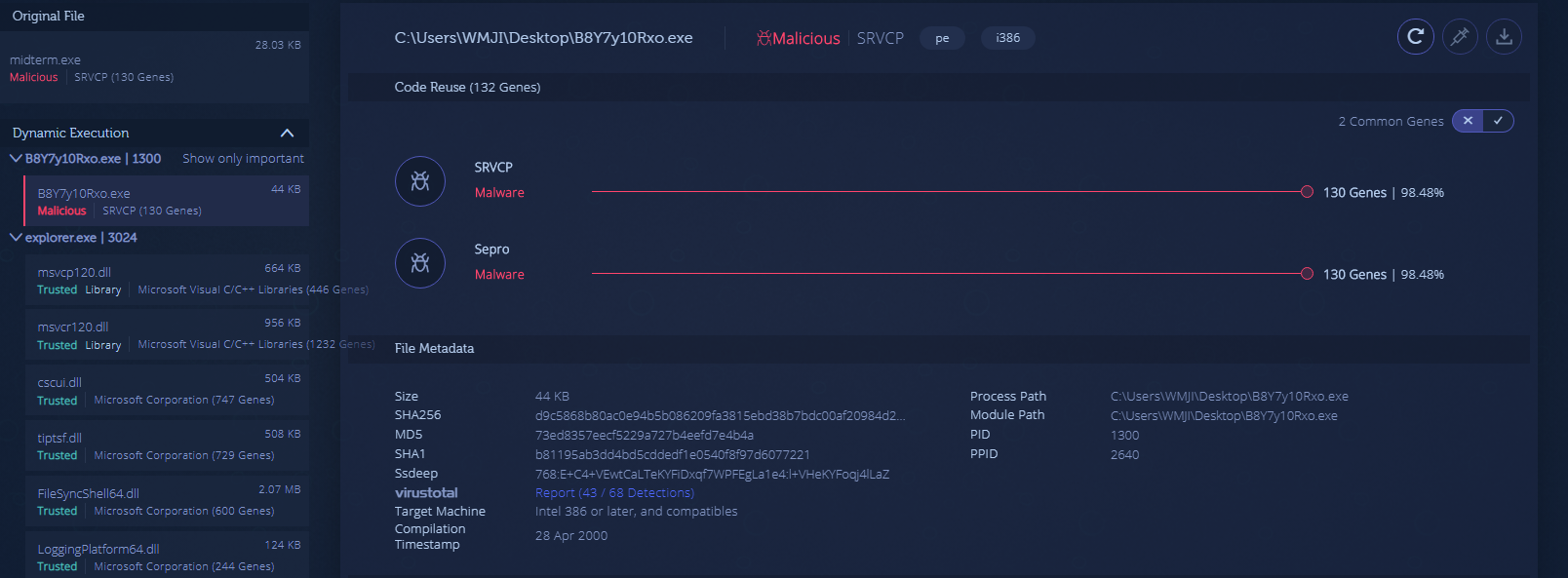
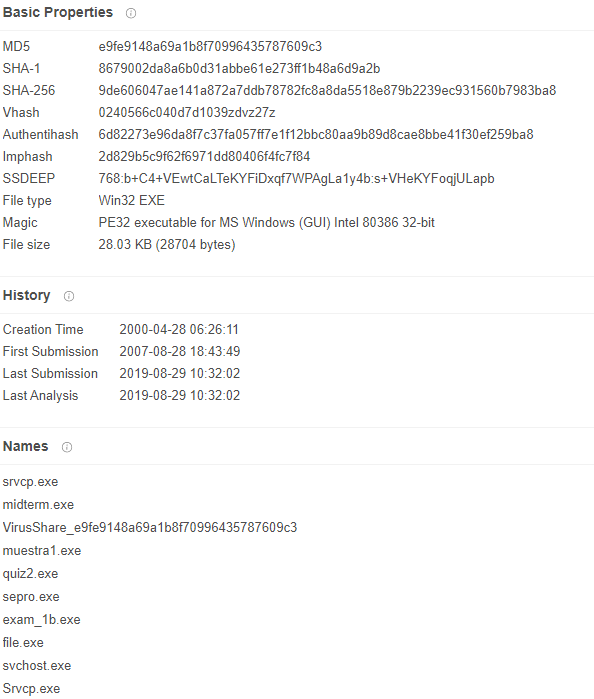
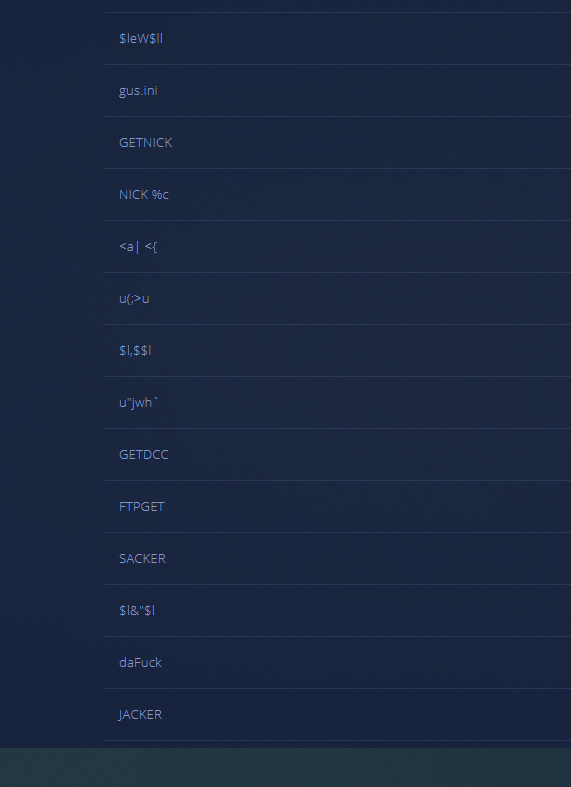
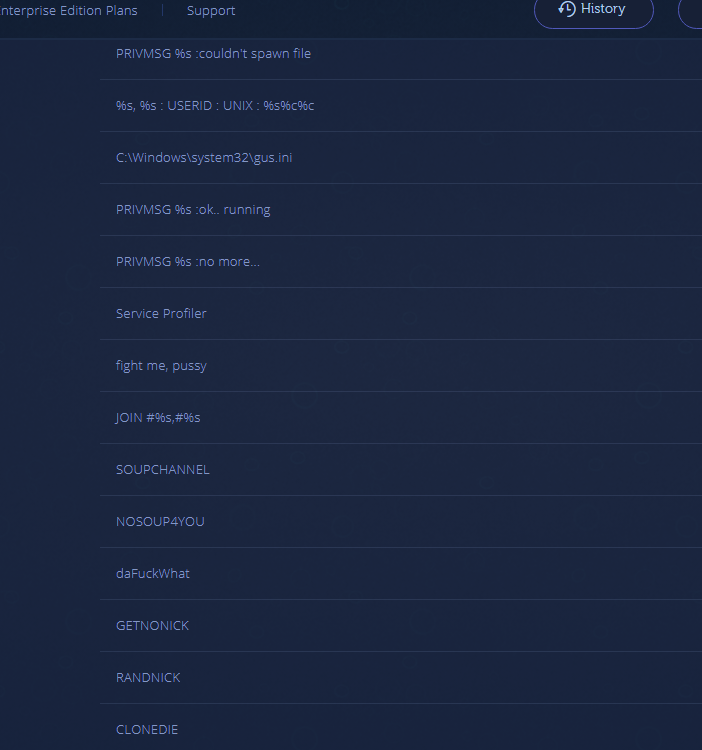
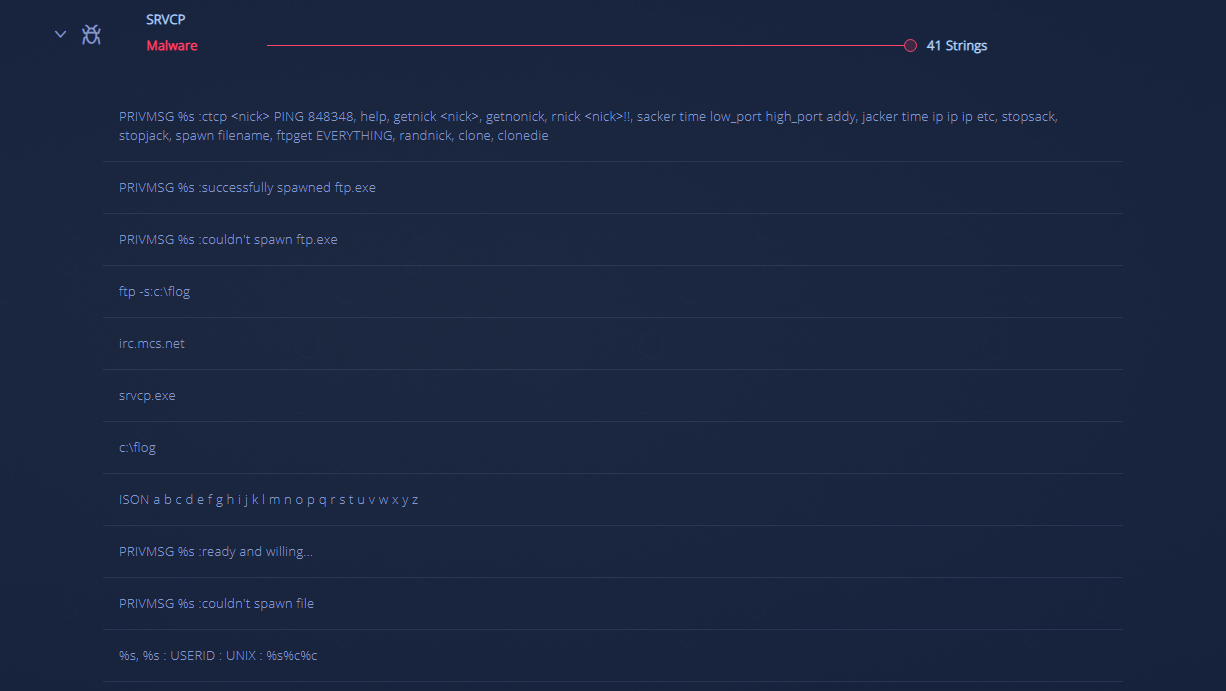
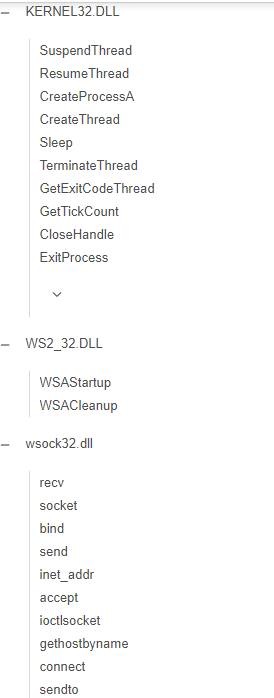
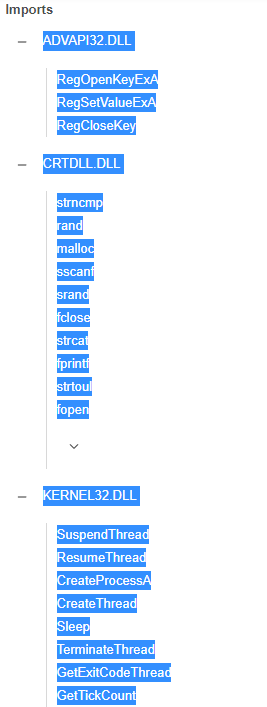
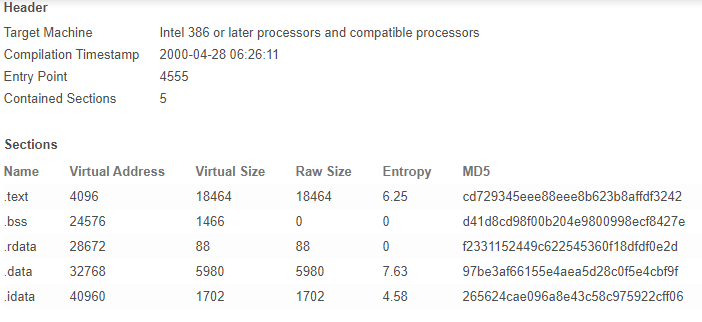
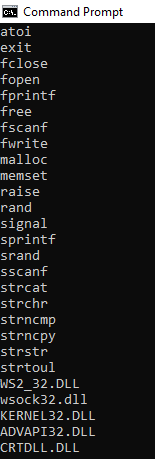
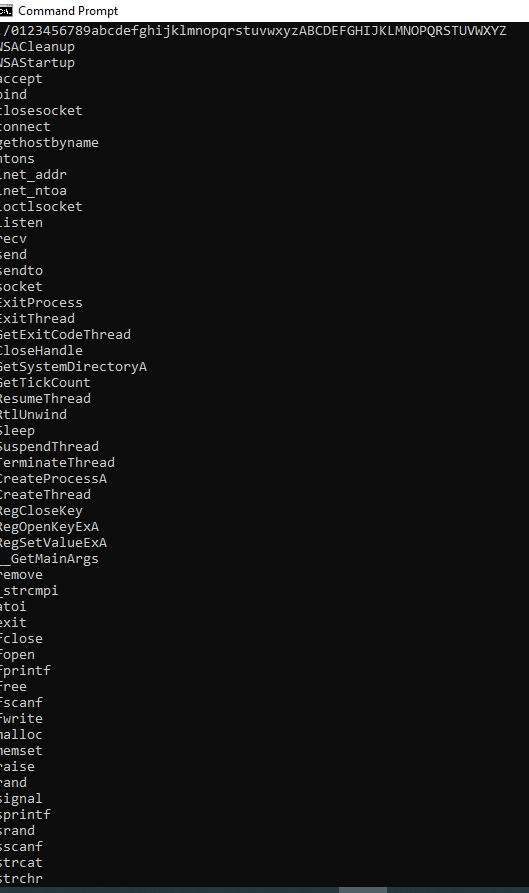
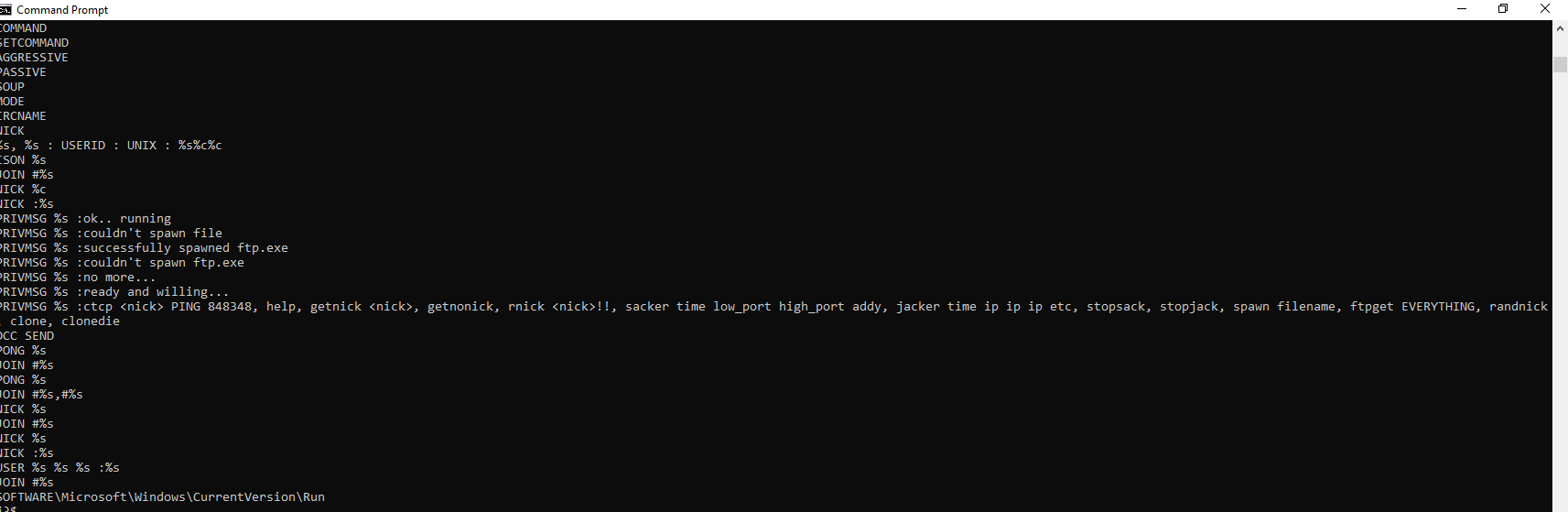
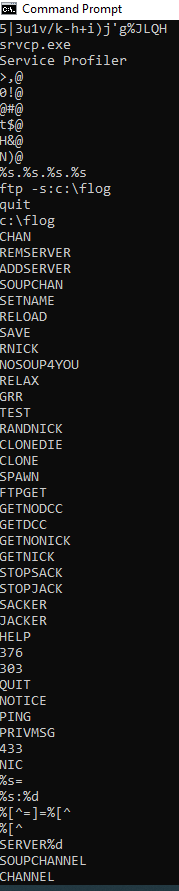
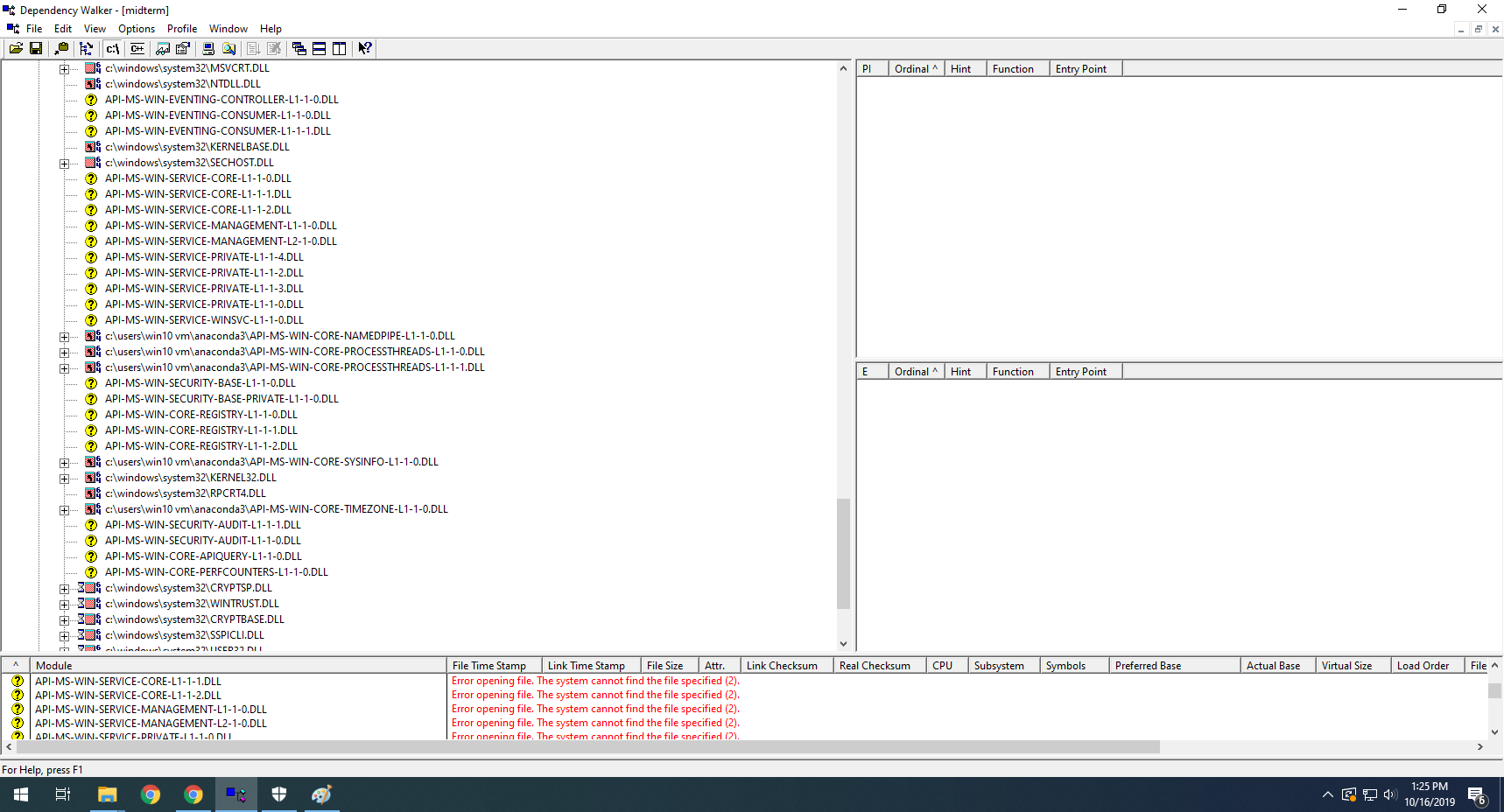
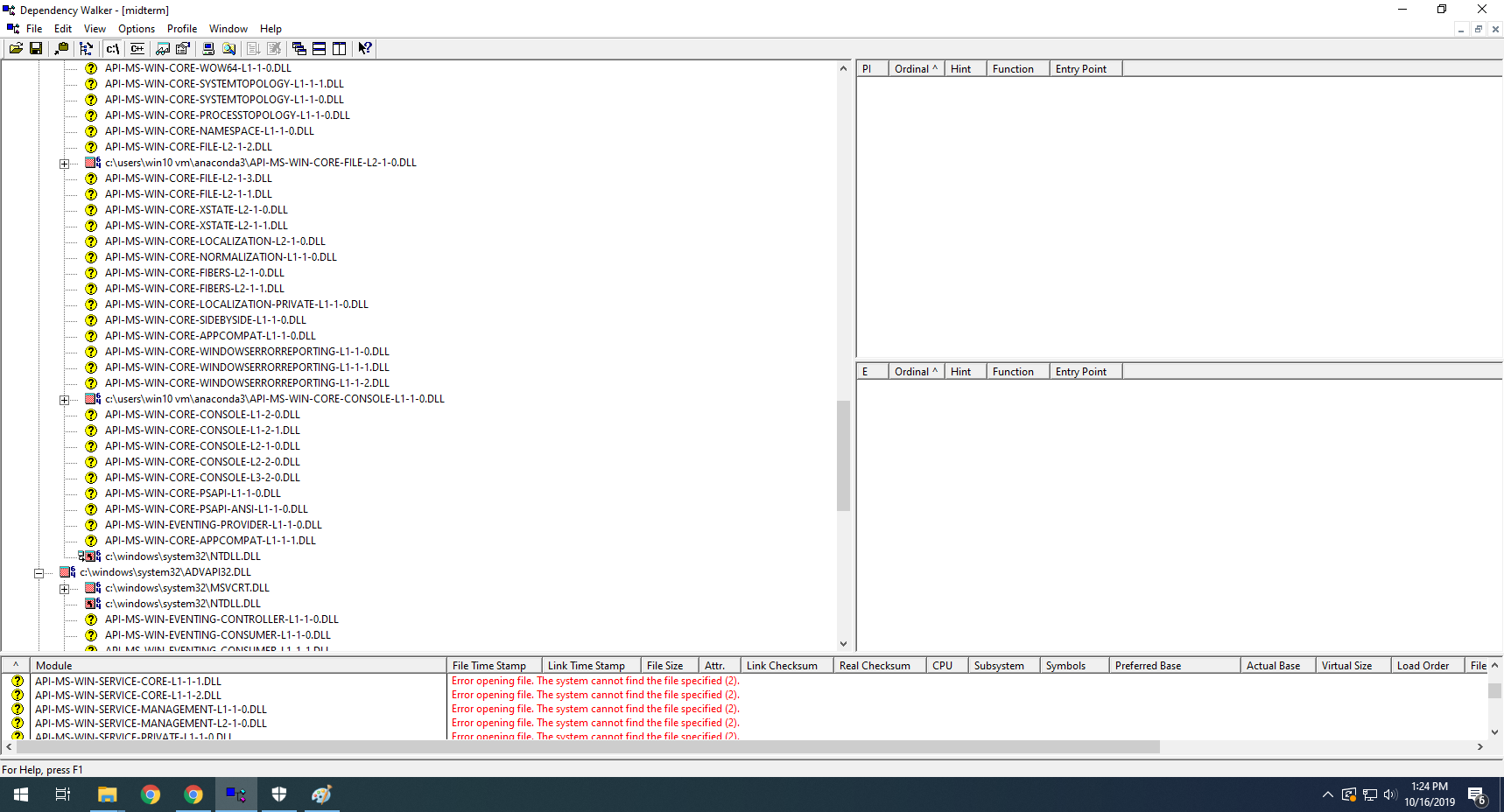
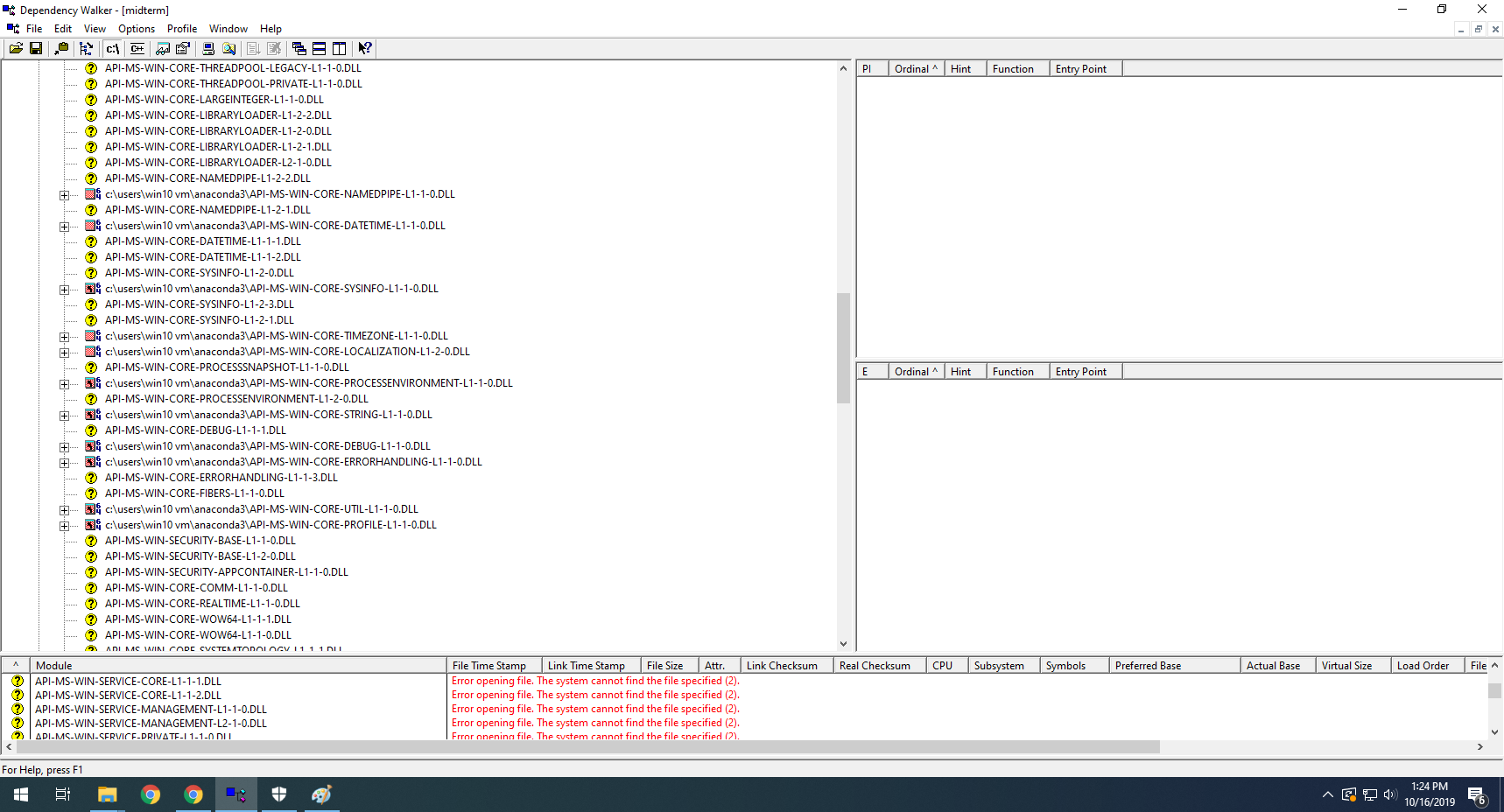
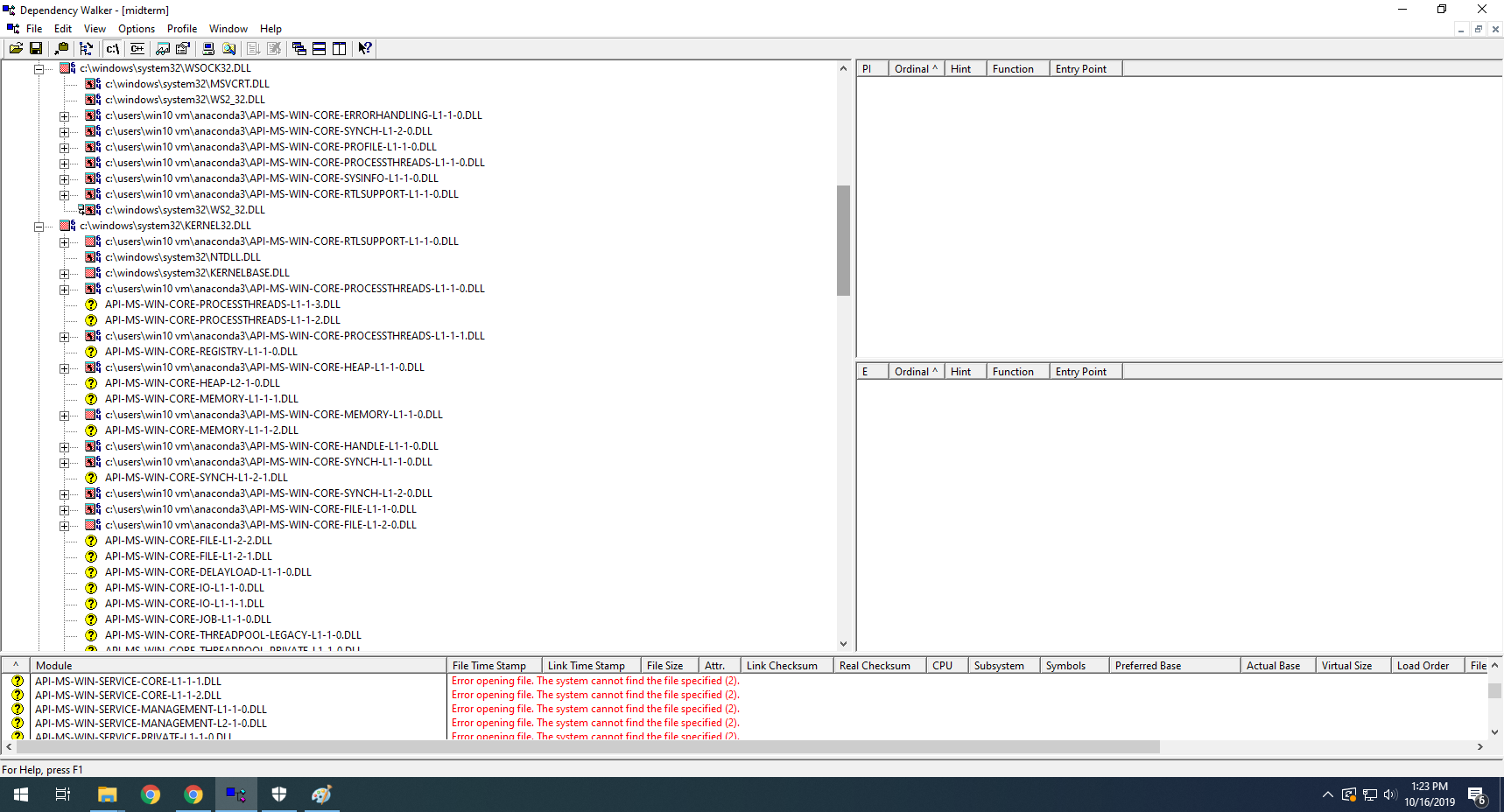
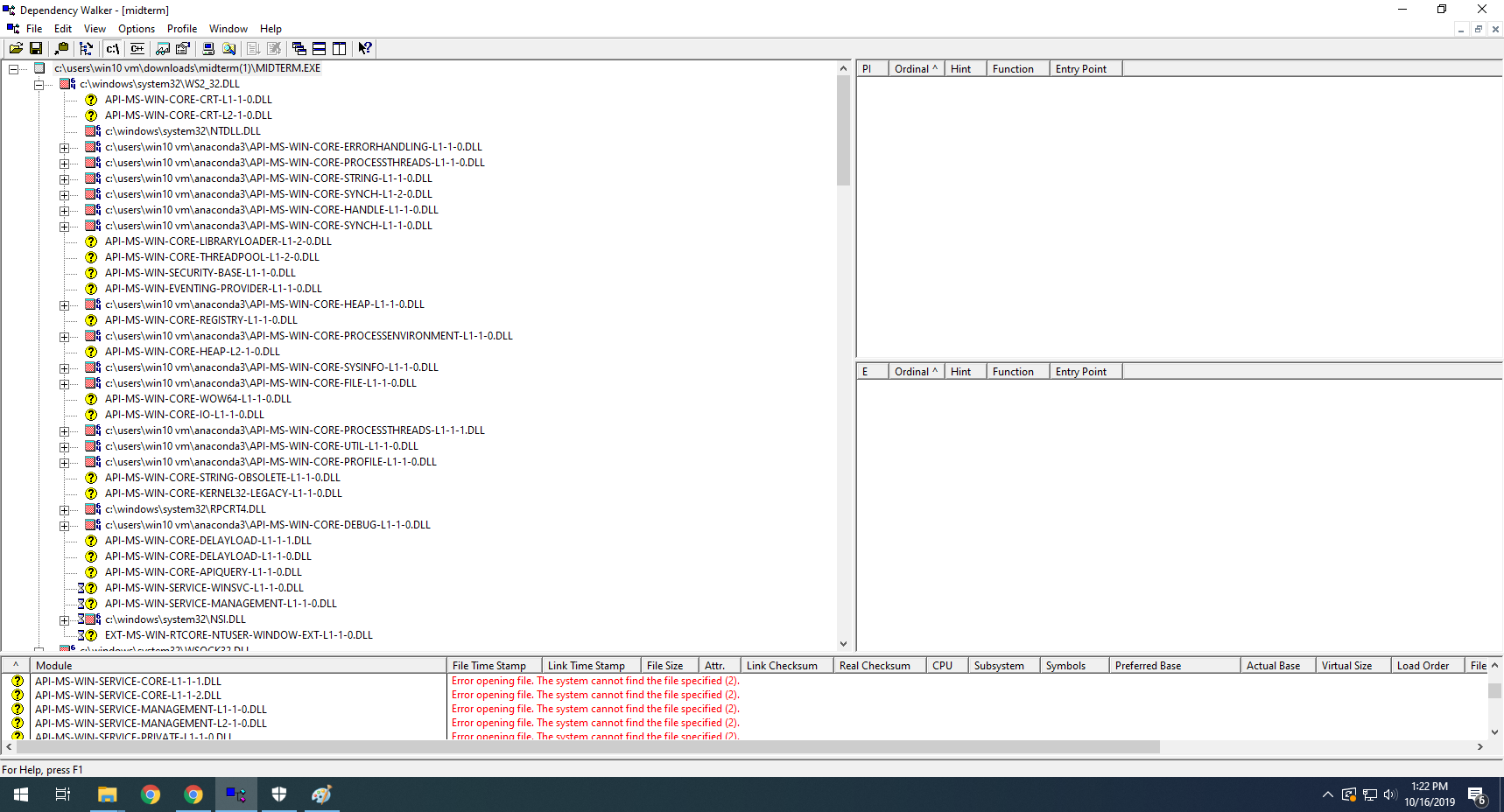
**CYB3011 Midterm**

|  |  |  |
| --- | --- | --- |
| **BACKGROUND** | | |
| **Date:**  10/16/19 | |  |
| **Your Name:**  Michael Huber | |  |
| **File Name:**  midterm.exe | |  |
| **File Location: C:\Users\Win10 VM\Downloads\midterm(1)** | | **N/A** |
| **File Timestamps:**  Creation Time:  2000-04-28 06:26:11  First Submission:  2007-08-28 18:43:49  Last Submission:  2019-08-29 10:32:02  Last Analysis:  2019-08-29 10:32:02 | |  |
| **Notification Vector:** | | **N/A** |
| **STATIC ANALYSIS** | | |
| **File Size (bytes):** | 28,704/32,768 (on disk) | |
| **Icon Graphic:** | **N/A** | |
| **Signed?:** | **N/A** | |
| **File Hash:** | E9fe9148a69a1b8f70996435787609c3 (MD5) | |
| **Imp Hash:** | 2d829b5c9f62f6971dd80406f4fc7f84 | |
| **PE Section Hashes:** | | |
| PE32 executable for MS Windows (GUI) Intel 80386 32-bit  PE file has unusual entropy sections  Details: .data with unusual entropies 7.63334150891  Source: Static Parser  Relevance: 10/10    PE file contains zero-size sections  Details: Raw size of ".bss" is zero  Source: Static Parser  Relevance: 10/10 | | |
| **Compile Time** (pescanner, PEView)**:** | | |
| 2000-04-28 06:26:11 | | |
| **File Properties** (PEStudio, PeView)**:** Description, version, file header characteristics | | |
| Target Machine:Intel 386 or later processors and compatible processors  Compilation Timestamp: 2000-04-28 06:26:11  Entry Point:4555  Contained Sections: 5 | | |
| **Strings** (strings, strings2, BinText)**:** Functions, domains, IP addresses, commands, error msgs | | |
|  | | |
| **Packed** (pescanner, PEiD, ExeInfo)**:** | | |
| LCC Win32 1.x -> Jacob Navia [Overlay] | | |
| **Entropy** (ByteHist, pescanner)**:** File, sections | | |
| N/A | | |
| **Imported/Exported Functions** (PEStudio, Dependency Walker)**:** | | |
| ADVAPI32.DLL  CRTDLL.DLL  KERNEL32.DLL  WS2\_32.DLL  wsock32.dll | | |
| **Open Source Research** (VirusTotal, search engines, malware repositories)**:** | | |
| Appears to be python-based, considering it goes and accesses python distribution on dependencies. Is a backdoor Remote Access Trojan according to Virustotal, connects to external EU domain. | | |

**Screenshots (Paste Below)**

****

****