PROG8300-22F – Malware Project – John White (6714158)

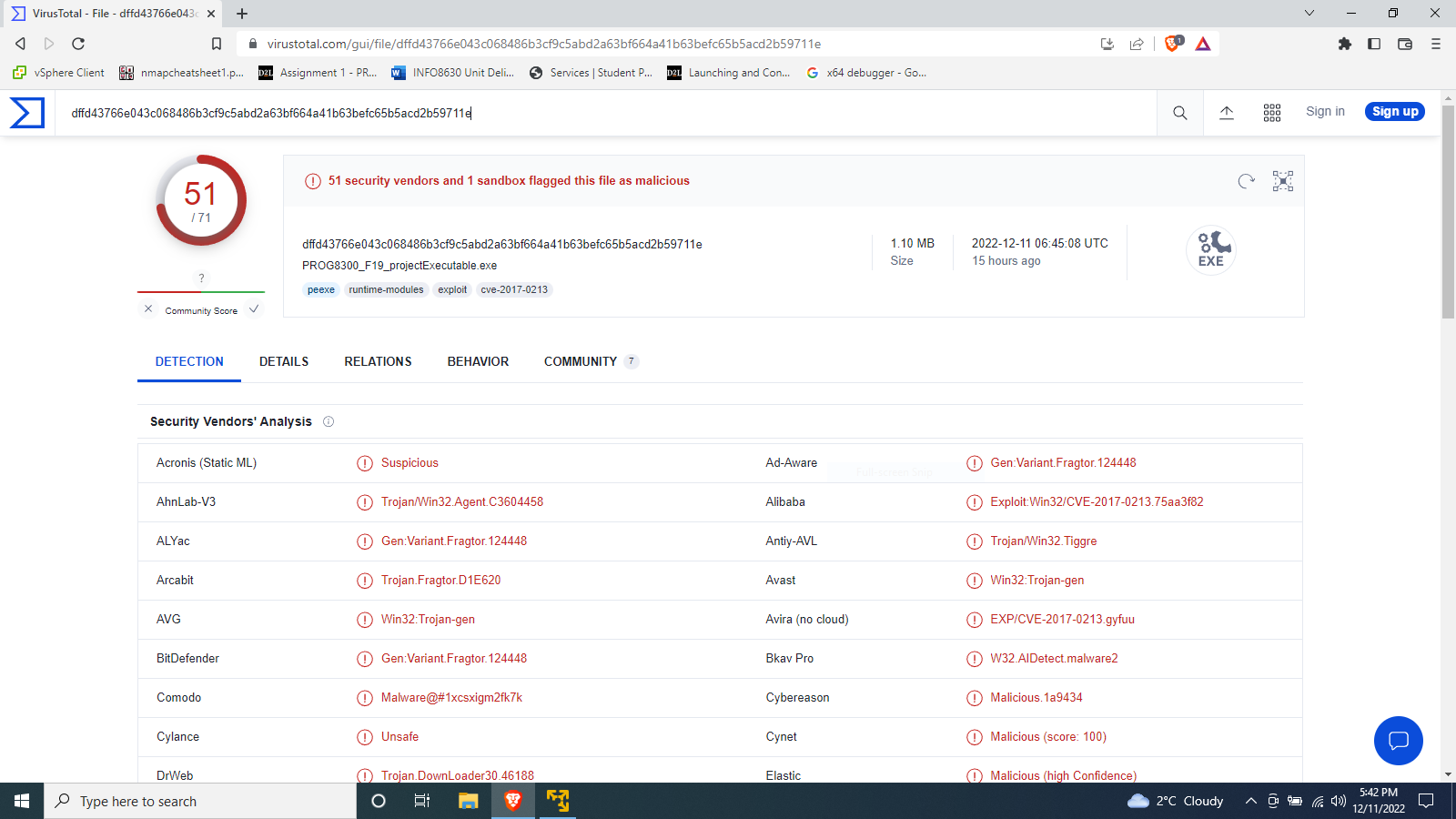
To begin the analysis, I uploaded the .exe file to VirusTotal.com to see if it matched any existing virus signatures (**Figure 1**). Many vendors did identify the .exe as malware and several of them suggested that the file could be a Trojan virus. I then continued with the static analysis using IDA. Based on the strings and imports, it seems like a large part of the program’s functionality involves creating, opening, and modifying files (**Figure 2** and **Figure 3**). I also analyzed the file using PEid and OllyDBG (**Figure 4** and **Figure 5**) but I did not find anything that I thought was useful. Using DependancyWalker (**Figure 6**), we can verify many of the imports that we found using IDA.

For the dynamic analysis, I started with RegShot (**Figure 7**). RegShot did indeed find that multiple registries were edited by the program. Many of these registries were also listed in Process Monitor (**Figure 8**). It also seems to have made modifications so several other files as well. When I ran the executable and input the password ‘PROG8300’, it created a file on my desktop called ‘AAAAAAAAAAA’ and the terminal closed. I am not sure what the purpose of this file is as of right now.

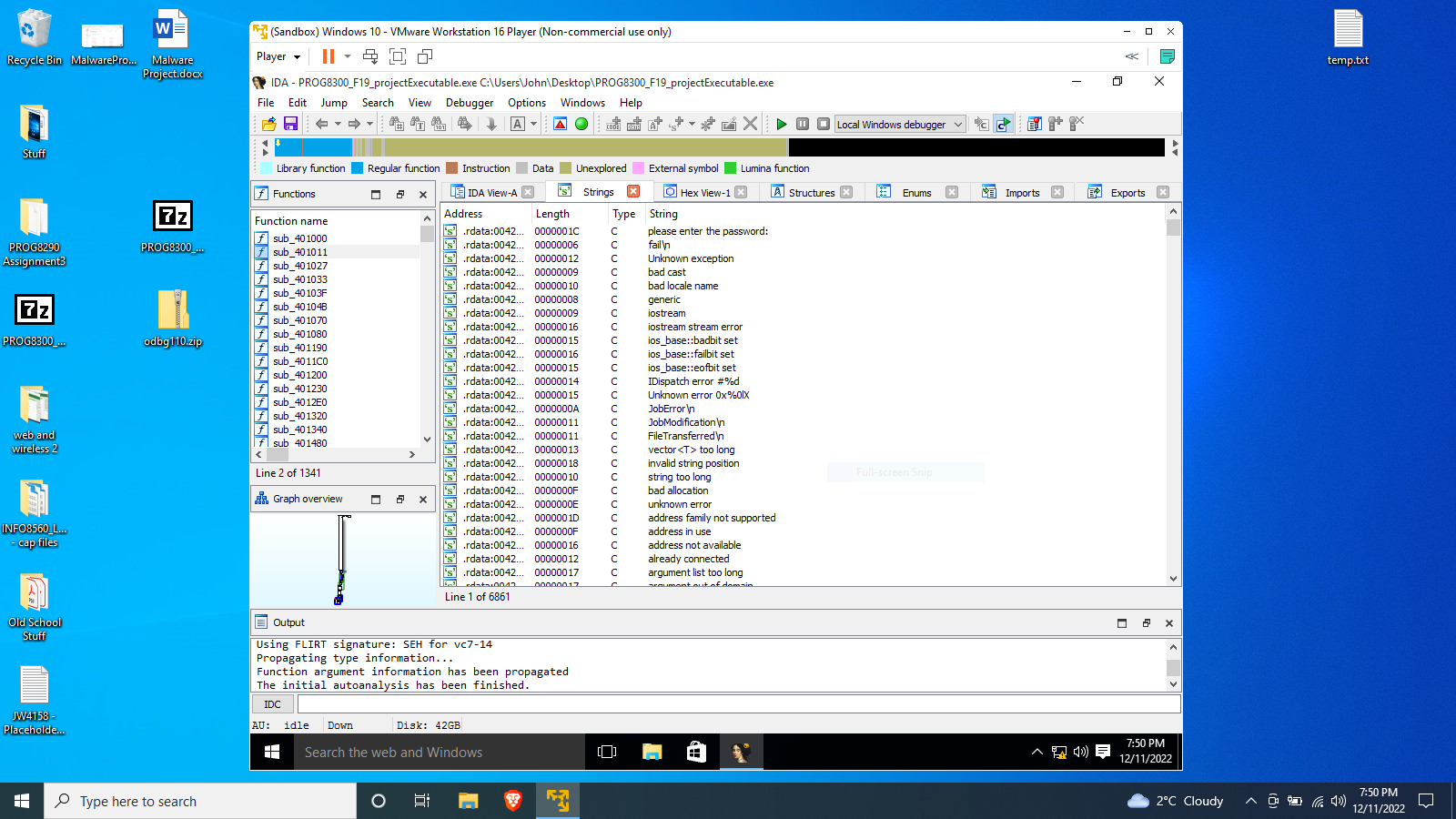
I could not get a network connection to work on my sandbox VM without sharing direct access to my network card, so I could not perform this portion of the analysis effectively. However, based on some of the imports and strings from IDA, it seems that this executable does have networking capabilities, most likely for the purpose of downloading files from somewhere.

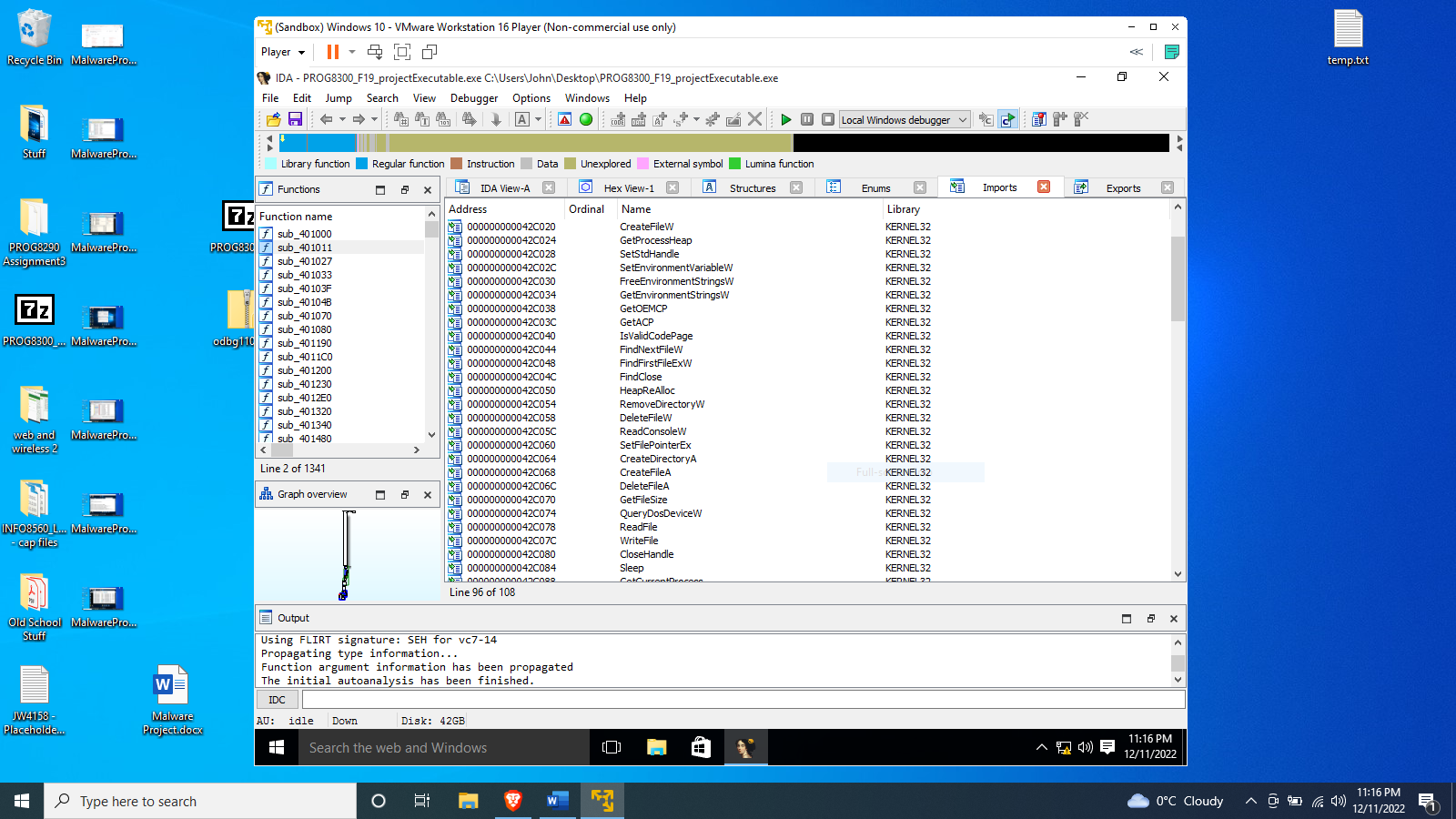
In conclusion, I believe that the purpose of this executable is to be a trojan virus downloader/installer. The program would be hidden in a seemingly-innocuous file and when run, it would install a virus on your computer that could log your keyboard activity or potentially act as a backdoor. It could also be very difficult to remove this virus once it’s been installed, because the installer can change the registry as well to make it appear as though the virus is not present. It is highly advised to take the precautions necessary to avoid this malware in the first place.

Screenshots

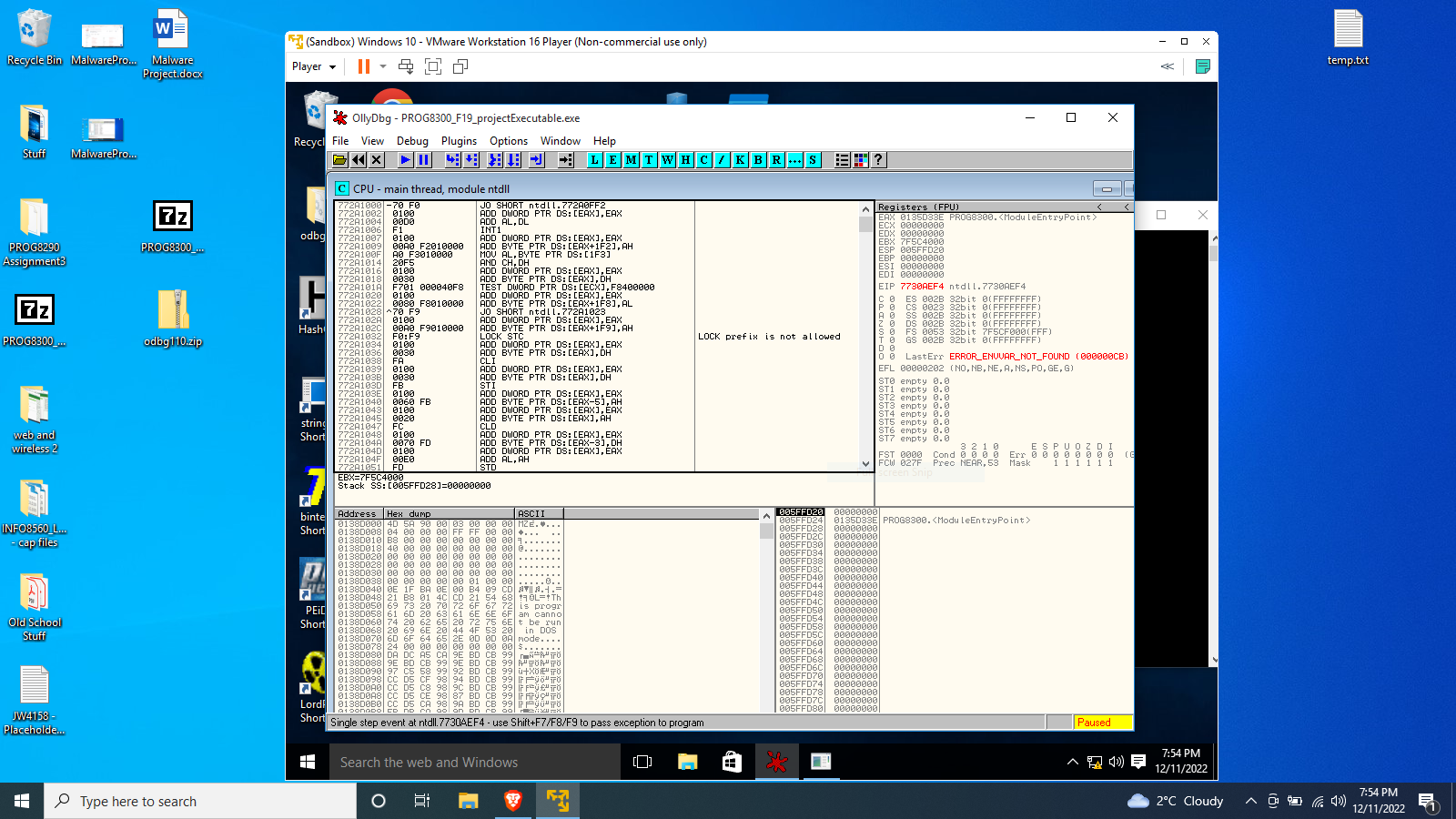


**Figure 1** – VirusTotal analysis

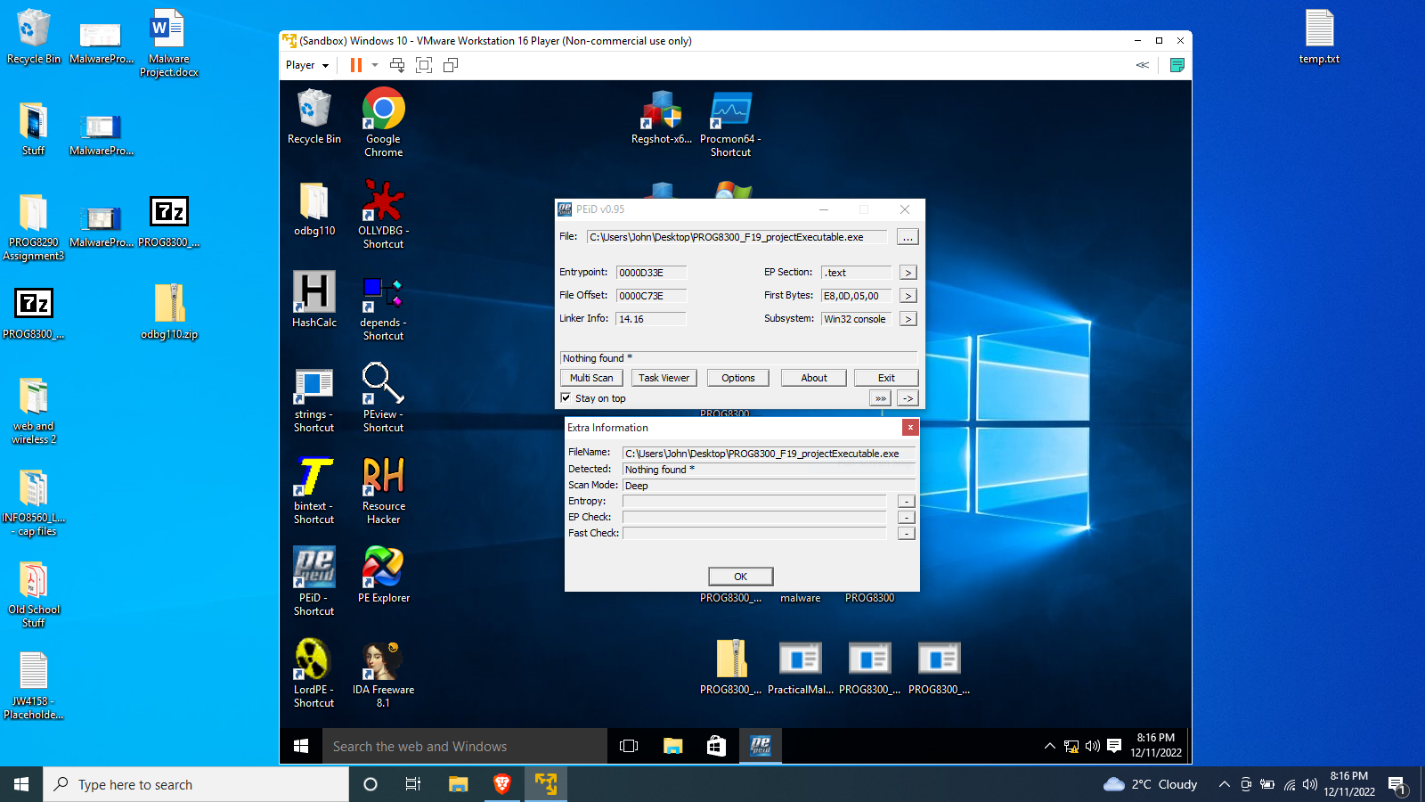
**Figure 2** – IDA analysis (strings)

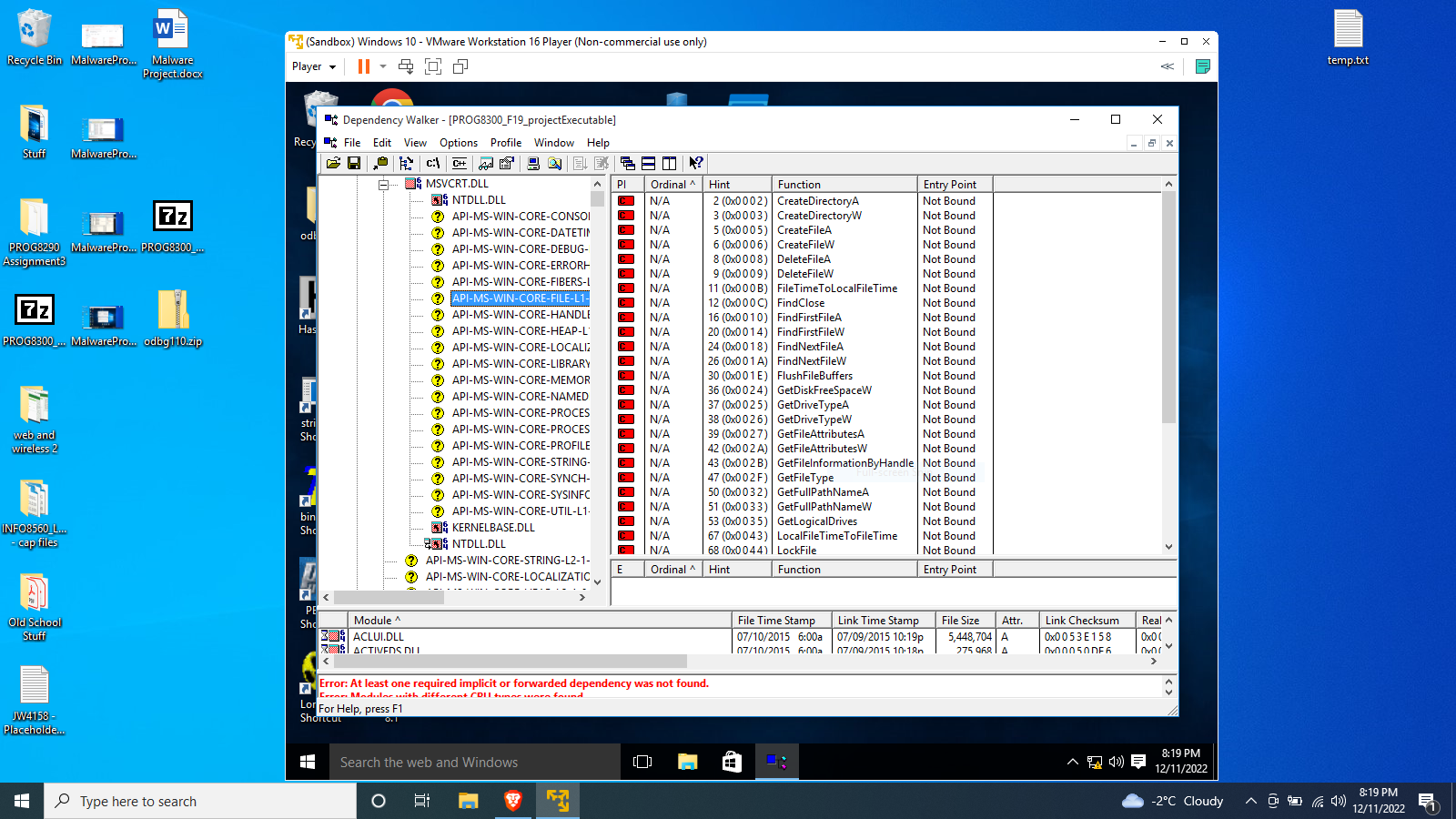


**Figure 3** – IDA analysis (imports)



**Figure 4** – OllyDBG analysis

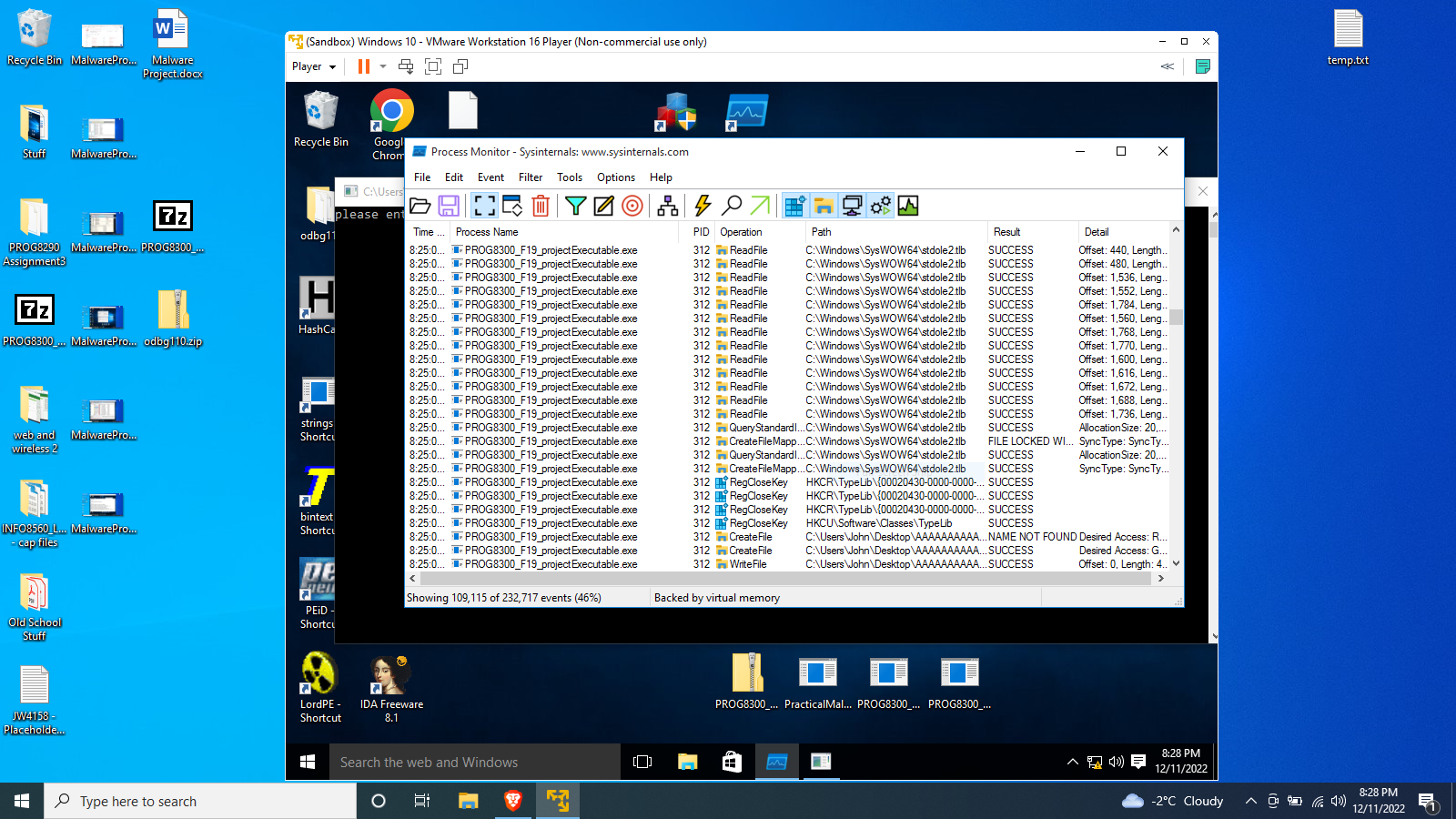
**Figure 5** – PEiD analysis



**Figure 6** – Dependency Walker analysis



**Figure 7** – Regshot analysis

**Figure 8** – Process Monitor analysis