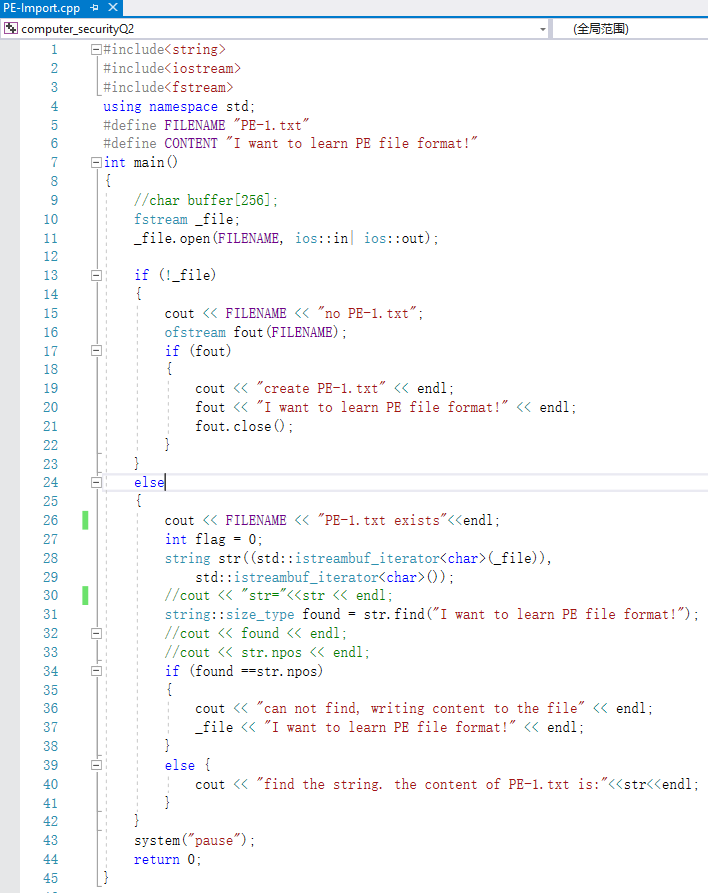
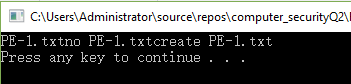
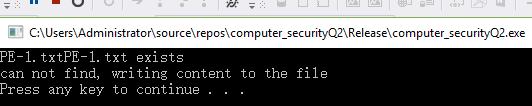
The original program is **PE-Import.exe**, the version that packed by virtual machine tool (VCprotect) is **PE-Import-vc+.exe**, the version that packed by VCprotect and UPX is **PE-Import-vc+upx.exe.**

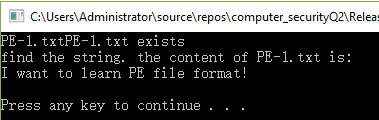
Step1:

Code:









Step2:

**In msvcp140.dll:**



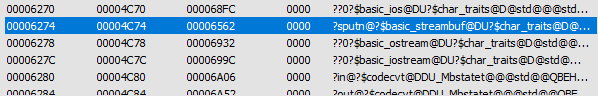
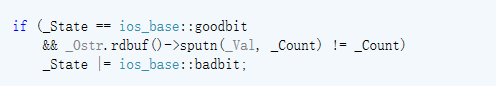
*cout:*



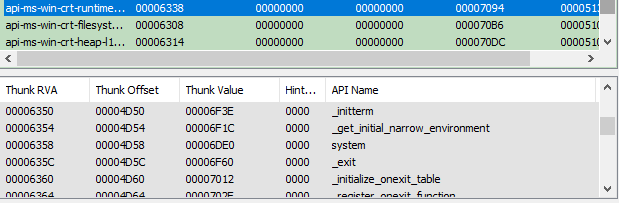
*<<(+14 overload)*



(the code friction that define “<<”)

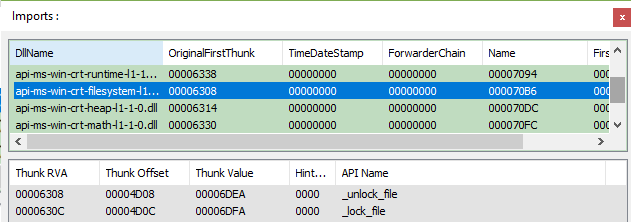


*System(“pause”)*

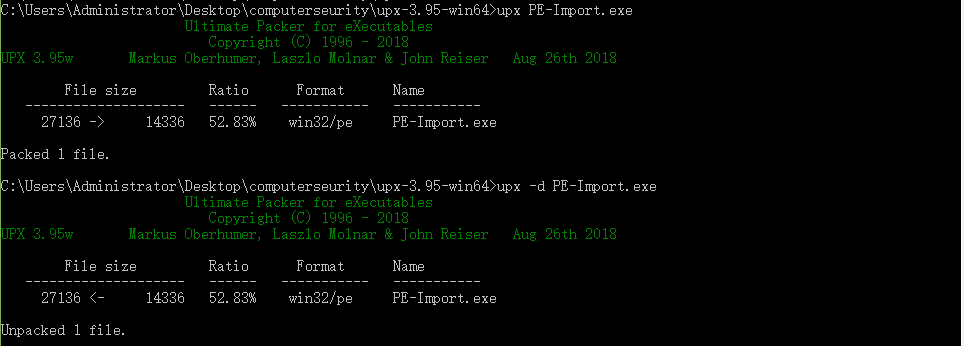


Note: AS the program was written by C++, most API in my code can not be found in Imports. The reason may because msvcp140.dll is not shown correctly in exeinfo.

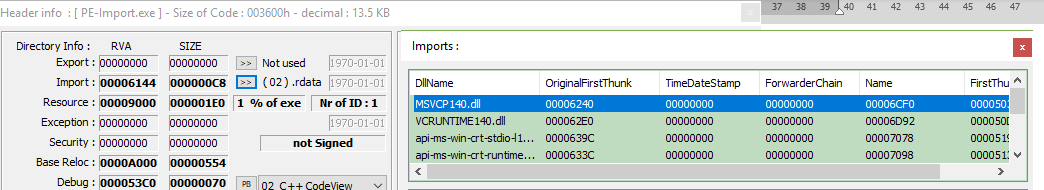
I also found two API may related to my program as I use the file, but I didn’t find the place where directly call those two function in the definition of the function and symbol in my code:

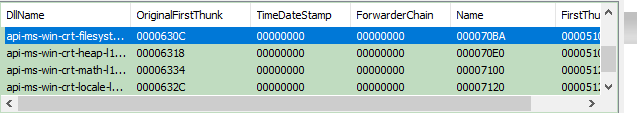


Packing and unpacking(step 3.1&3.3)



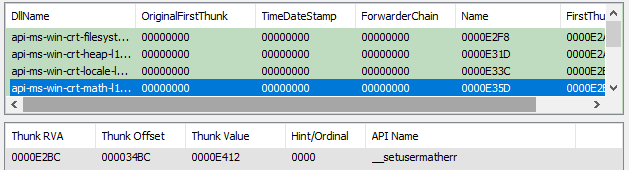
Before pack:

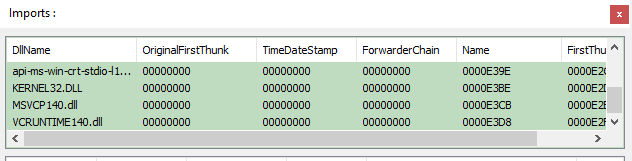






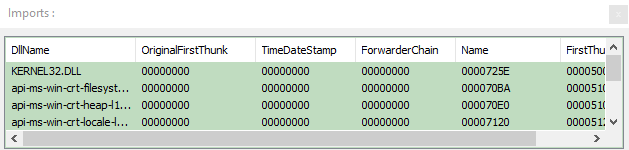
After pack(step 3.2):

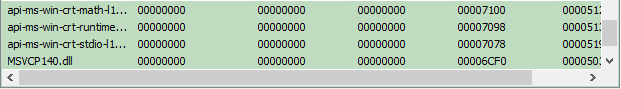






Unpack(step 3.3):







Discuss:

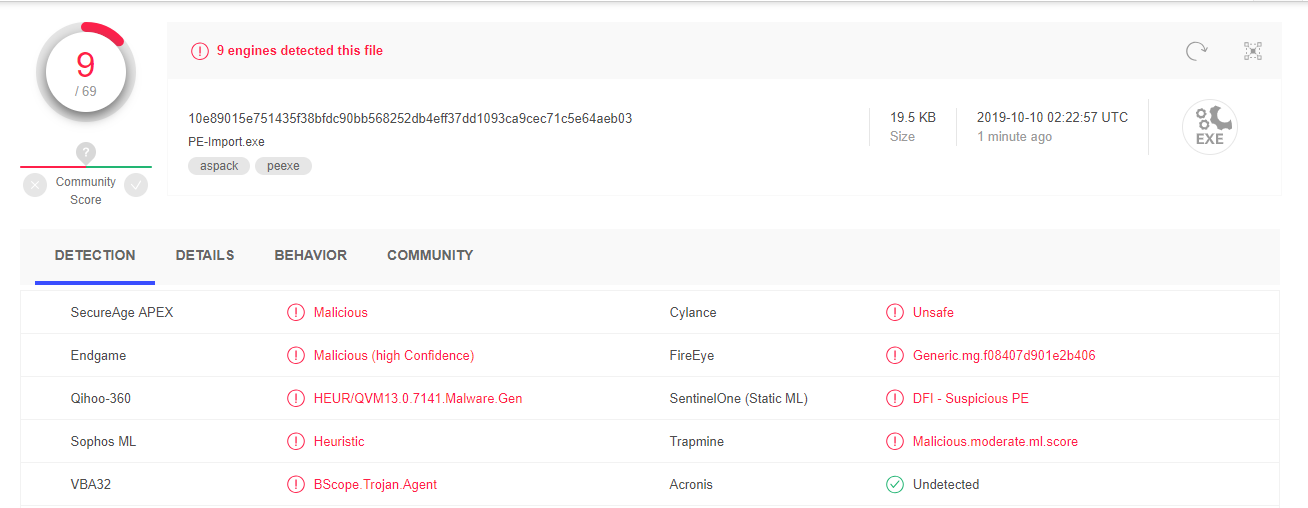
Compress the file will loose the information on OriginalFirstThunk and change the name. Decompress can not recover the information at OriginalFirstThunk but can recover the name. Also, the unpack operation is unsuccessful which broken my binary code, I check the information in the Hex view, it is same as the original code, but it can’t run.

Step4

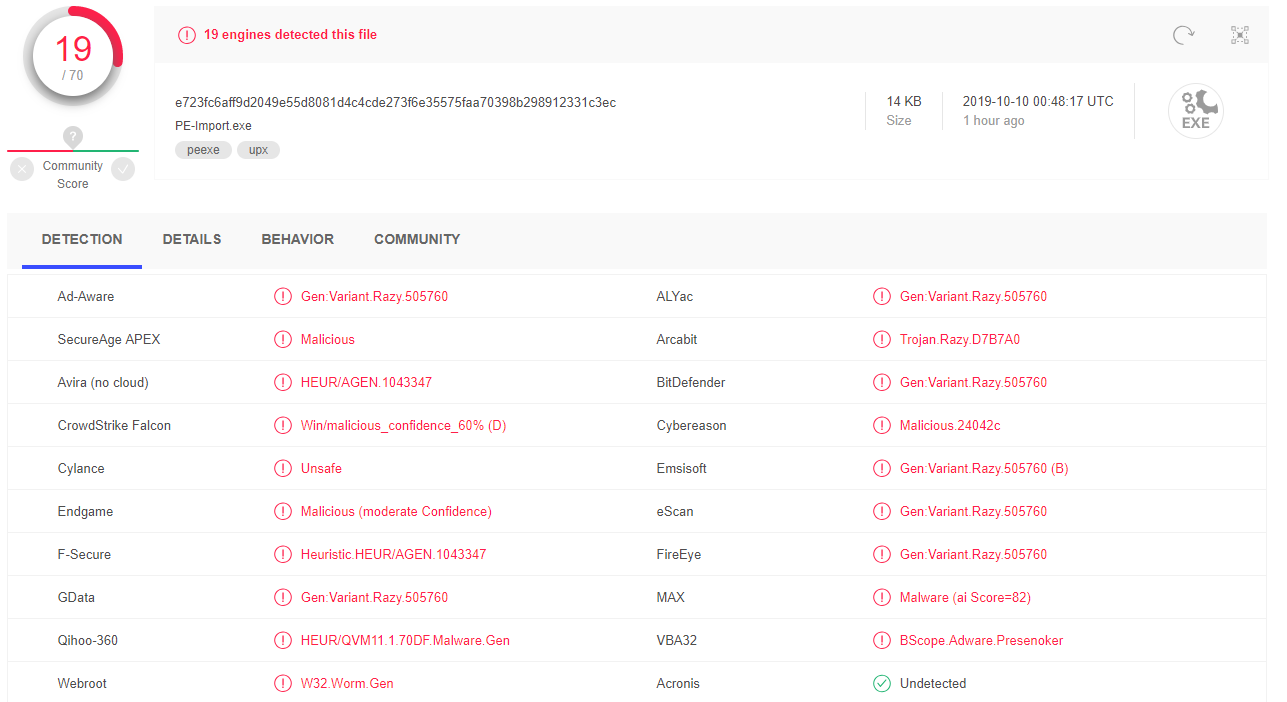
ADD the feather code of one particular virus to the PE header, but it’s not working.....



Packed by Aspack:

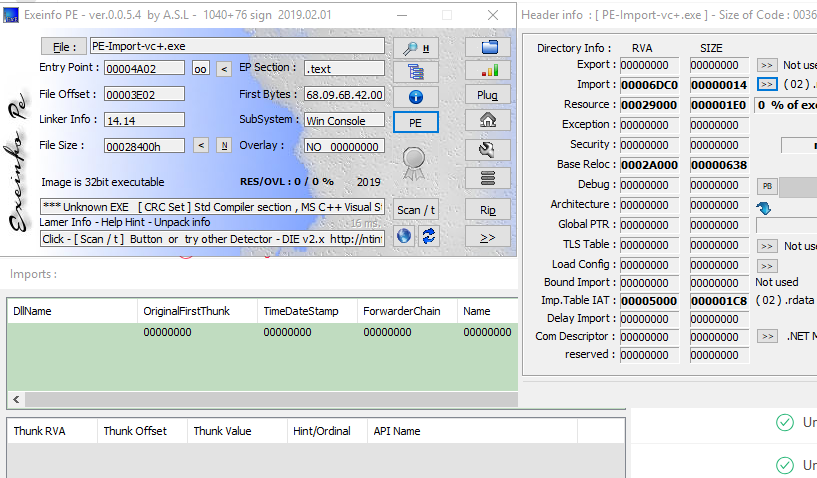


Packed by UPX:

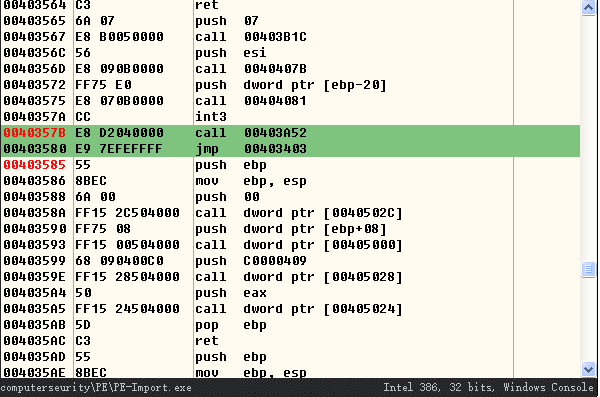


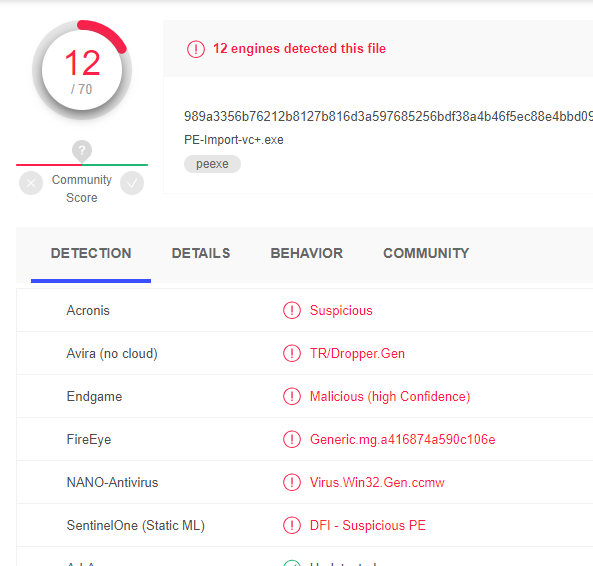
Change by VCprotect Virtualization tool (http://www.vcprotect.com):

Hide the import table:



This tool also encrypted the Register and metamorphose the code.





Packed by VCprotect then packed by upx

