**anti anti vm dll project**

Executive Summary:

Main goal: Anti anti vm dll, used to hide VMWare characteristics as files, processes, services, registry values

The method used in this project is by hooking the relevant functions in OS, I'm making use in "MinHook" native c library which make my life easier a lot.

The current version aim to win7 32 bit.

One of the main goals is that the dll will be easy to configure, in order to let one to hide specific program.

The way to use the dll is to write its path to AppInit\_DLLs registry value, and then every process that load user32.dll will load my dll as well.

There are also 2 black list files: registry\_blackList.txt, files\_blackList.txt.  
Those files define which files and registry key to hide.

In order to make the use in the project easier I wrote exe file that change the necessary registry values and also copy the black list files to the right location.

Another goal of the exe file in the next stages of the project is to change VM footprints that can't be cleaned with hooking such as MAC number that use by vmWare VMs.

The functions I decided to hook and the way to check performance of my tool is based on - <https://github.com/AlicanAkyol/sems> - an open source project that is used to do the next: "sems is a tool which is created to help malware researchers by checking their environments for the signatures of any virtualization techniques, malware sandbox tools or well know malware analysis tools."

list of win32api calls hook that was done:

registry: RegOpenKeyExA.

files: GetFileAttributesA, CreateFileW

how to use:

1. create win7 32bit vmware machine.
2. Download <https://github.com/AlicanAkyol/sems> and run sems.exe to view vm detection result.
3. Copy runFiles directory to vm and run editReg.exe
4. Run again sems.exe and compare results to previous run results.

to-do list - Order of importance:

1. hook other functions:   
   processes: Process32First, Process32Next.  
   registry: RegQueryValueExA.
2. Make more clean and Reliability code, write code documentation.
3. Feet project to windows 7 64 bit.
4. Feet project to xp, windows 8, windows 10 – 32/64 bit.
5. Write project document with detailed explanation.
6. Hide other VM characteristics with exe file.
7. Search for another relevant files/processes/registry.

refrences:

1. AppInit\_DLLs: <https://support.microsoft.com/he-il/kb/197571>
2. anti vm\sandbox techniques:  
    [https://sentinelone.com/blogs/sfg-furtims parent/](https://sentinelone.com/blogs/sfg-furtims%20parent/)   
   <http://blog.cyberbitsolutions.com/anti-vm-and-anti-sandbox-explained/>   
   <https://www.sans.org/reading-room/whitepapers/forensics/detecting-malware-sandbox-evasion-techniques-36667>
3. MinHook library: <http://www.codeproject.com/Articles/44326/MinHook-The-Minimalistic-x-x-API-Hooking-Libra>
4. anti vm\sandbox malware samples\PoC : <https://github.com/AlicanAkyol/sems>