# Rootkit VM analysis

## What was changed about the system

Automatic updates was off, after running rootkit revealer I could tell that files were being hidden. The machine felt slow but could have been the vm.

## What Files were responsible

Fat.bat which runs at start up runs fu to hide pid 4 and installs and starts mmpc then used fu to hide the msdirectx.sys and mmpc.sys drivers. It then runs sc delete mmpc.

Ctl.exe is used to hide fu.exe

## Tools and Techniques

First thing I did was run rootkit revealer. This pointed out hacker defender and two files fu.exe and _cool_beans

Tried looking at process explorer but processes were also hidden from it. Used Autoruns to look for programs that run at start up. Entry for FAT Filesystem Initialization in HKLM\Software\Microsoft\Current\Version\Run looked suspicious. Also suspicious were ctl.job, ctl2.job and ctl3.job in the task scheduler that all ran ctl.exe.

I used IDA to look at ctl.exe, it is He4Hook, ran ctl.exe –h to see the options then ctl.exe –s to see what files it was hiding. Ran ctl.exe –da to remove all files from protected list. Could then see fu.exe in the file system. Ran fu.exe –h to see options.

Just browsing around found the folder for vanquish and ran vanquish –remove but I couldn't tell if I'd uncovered any files or not. I couldn't find what was hiding the cool_beans directory.