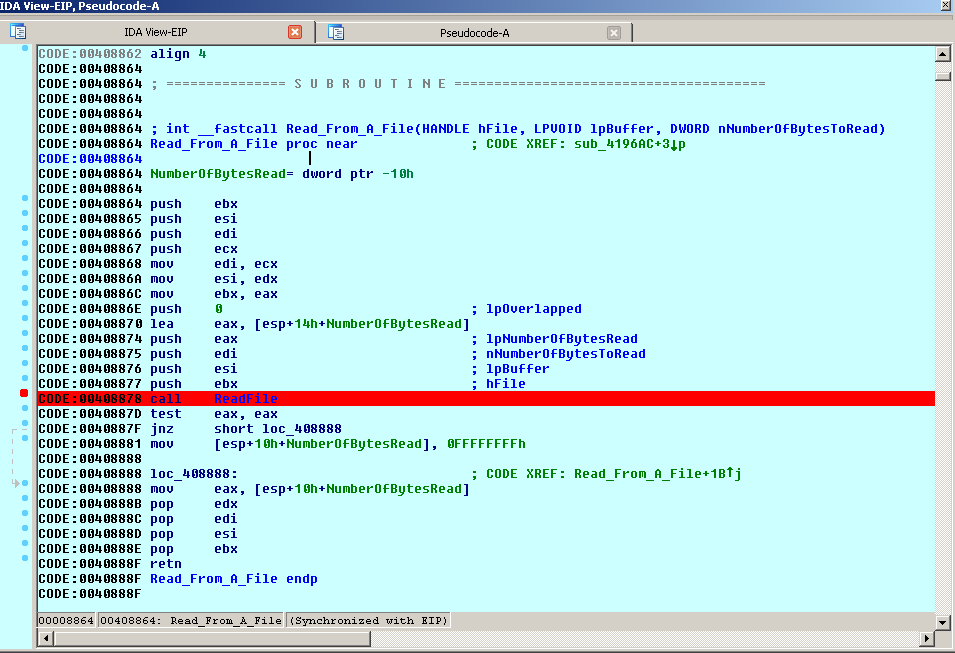
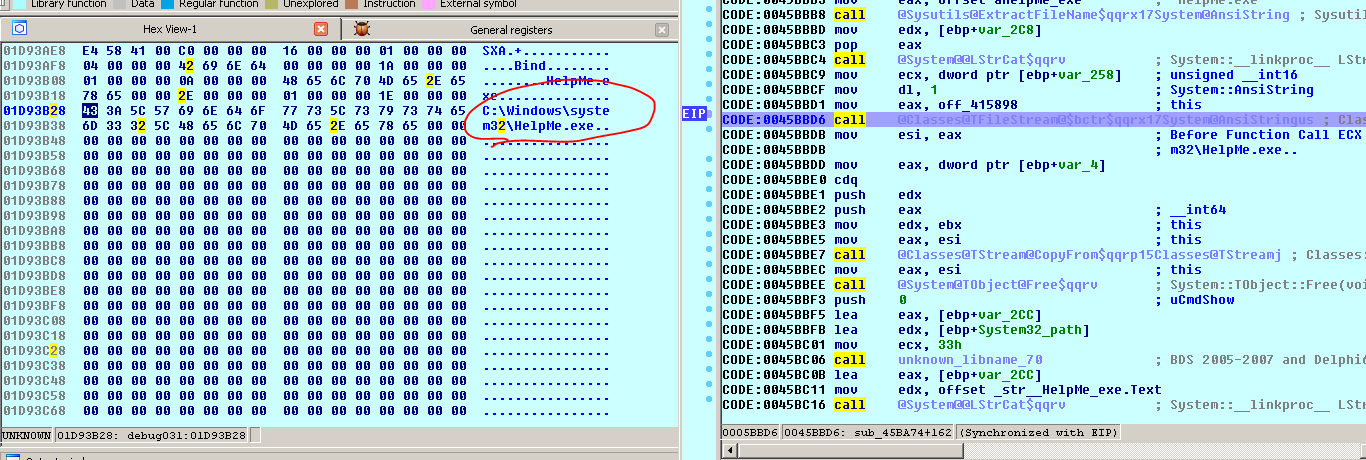
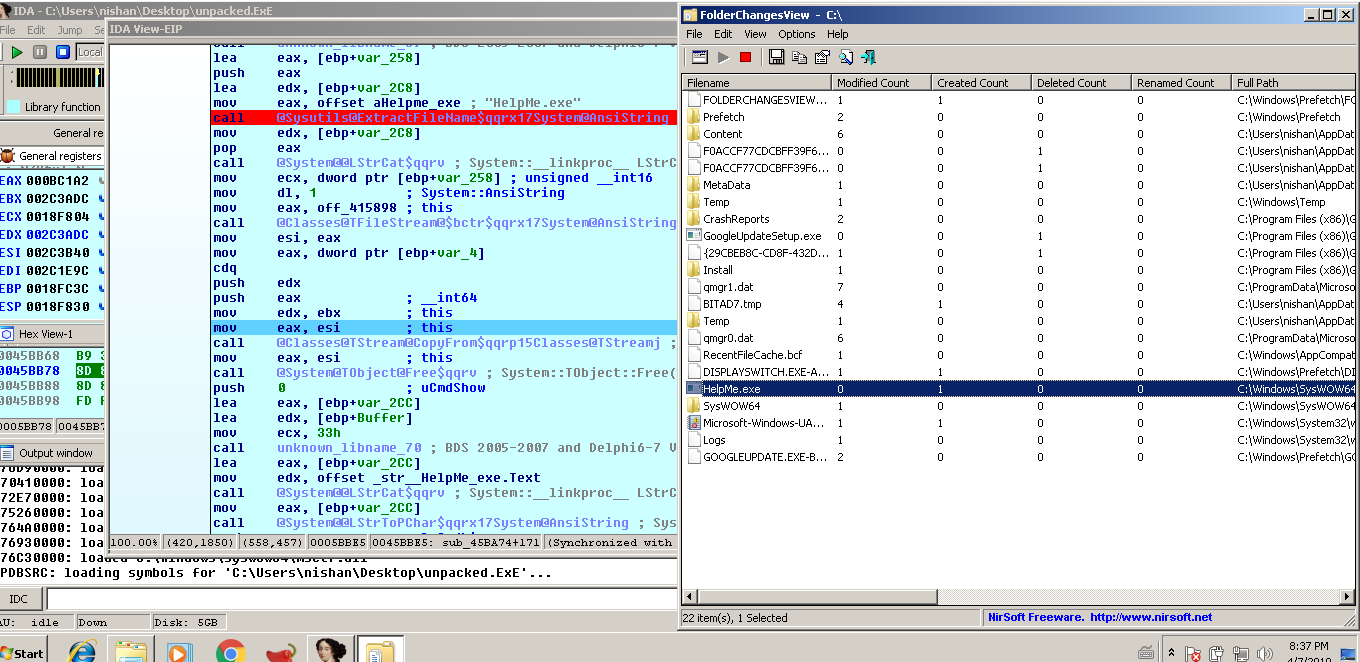


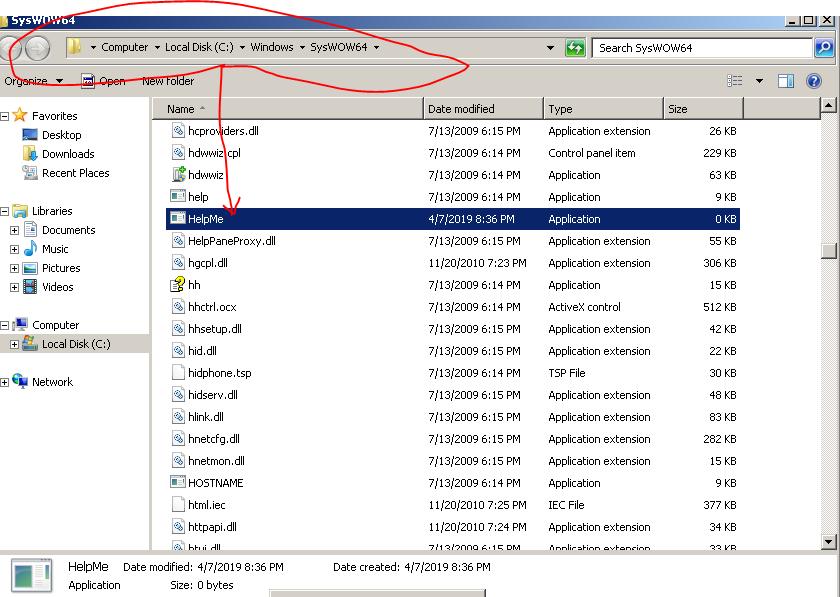
Now We know that the program tries to change registry key, and create file HelpMe.exe, so lets debug.



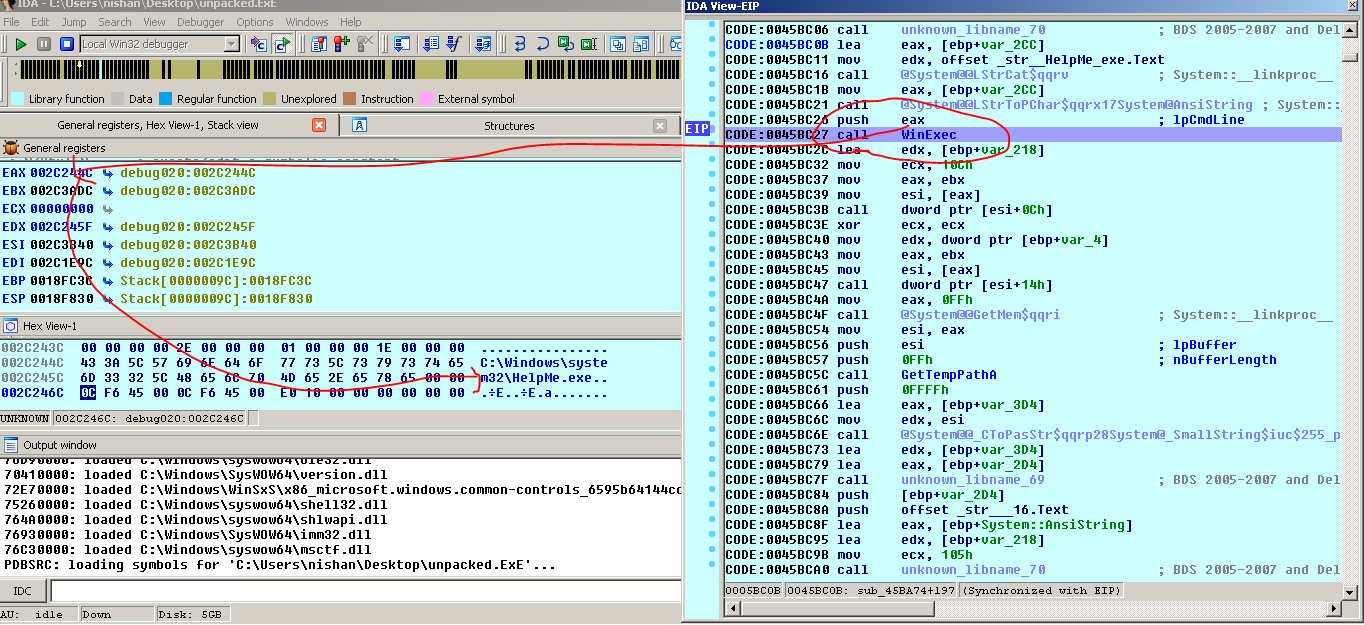
**Received Error, may be this is Access Deined one, lets run with admin priv.**



**But Since in 64 bit machine**



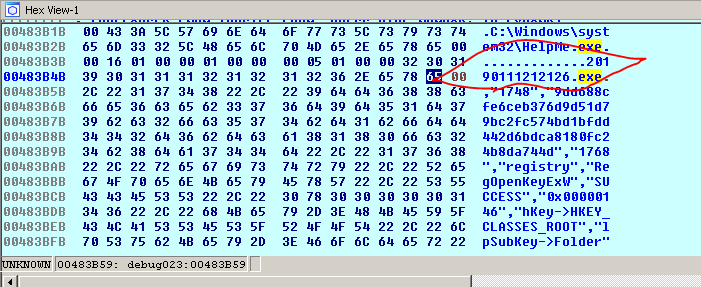
**After copying it runs it**



**Another File seems to be created, but extension too long error.**



**Change filename:**

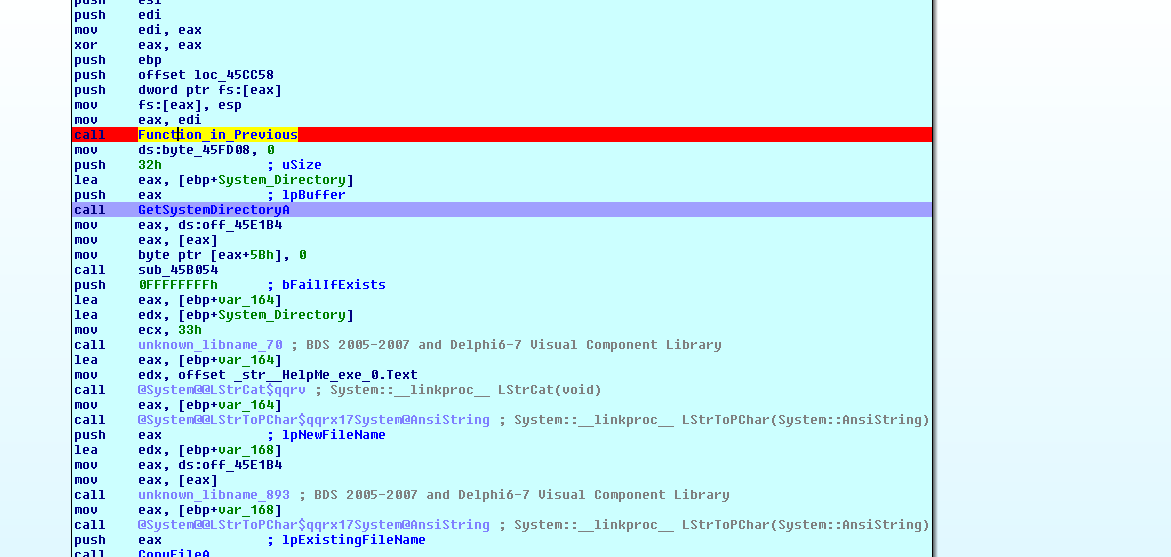


**But not an executable.**

**HelpMe.exe. Delphi compiled.**

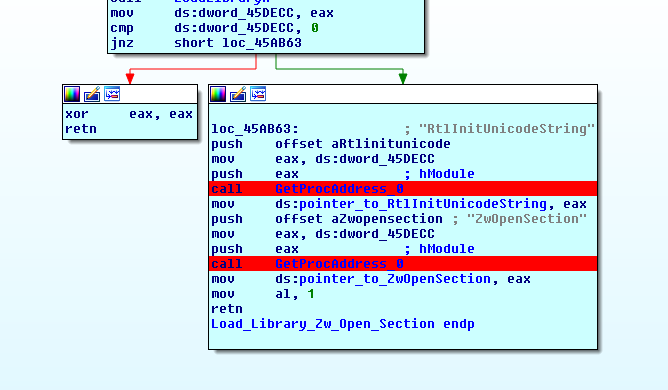
**Seems similar, WTF?, the same function does nothing and just exits,**

**Gets system directory**

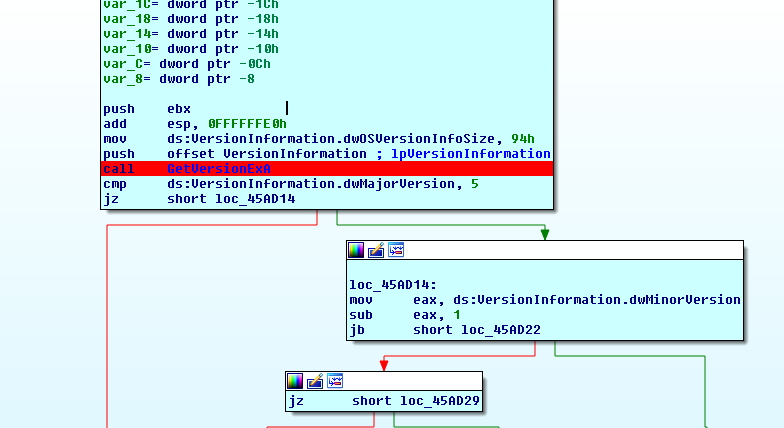


**sub\_45B054 calls function sub\_45AF60 which**

**calls 0045AB48 -> gets process address for RtlInitUnicodeString and ZwOpenSection**



**also calls 0045AF72 -> gets os version**



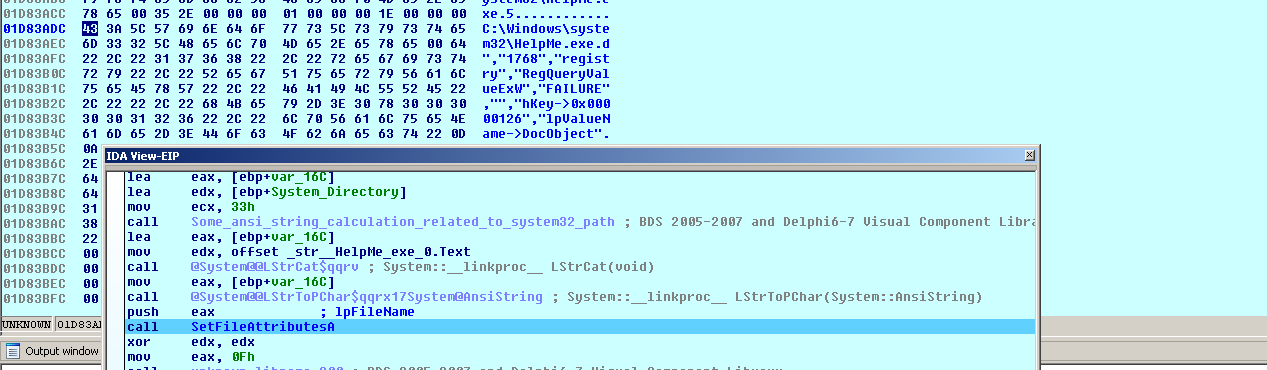
Compares if the os version is 5 i.e XP, in my case windows 7 i.e 6. Which does not match and just returns

A lot of calculation and eventually it called

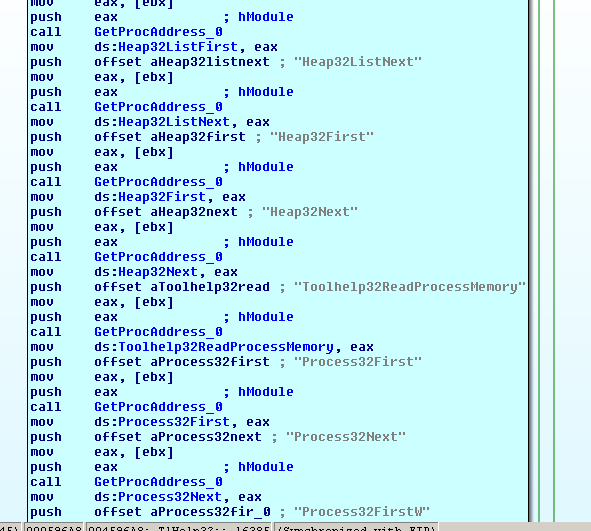
CopyFileA(C:\Users\nishan\Desktop\HelpMe.exe, C:\Windows\system32\HelpMe.exe)

Existing,new file

Again Changes Attribute of C:\Users\nishan\Desktop\HelpMe.exe



Function in 0045CABC and 0045CACB calls then same function TlHelp32::\_16385 which gets the process address of many functions manually.



The malware then takes snapshot of current process and then retrieves information about the process.

