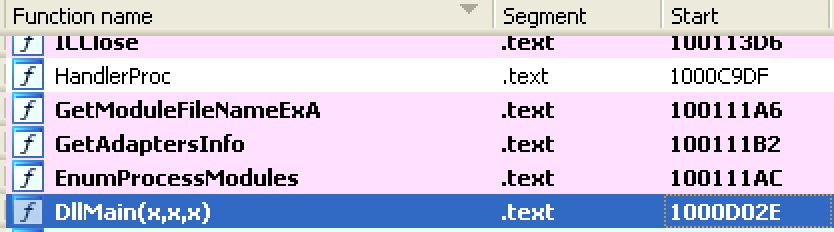
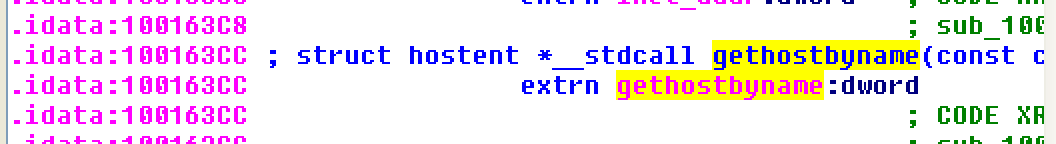
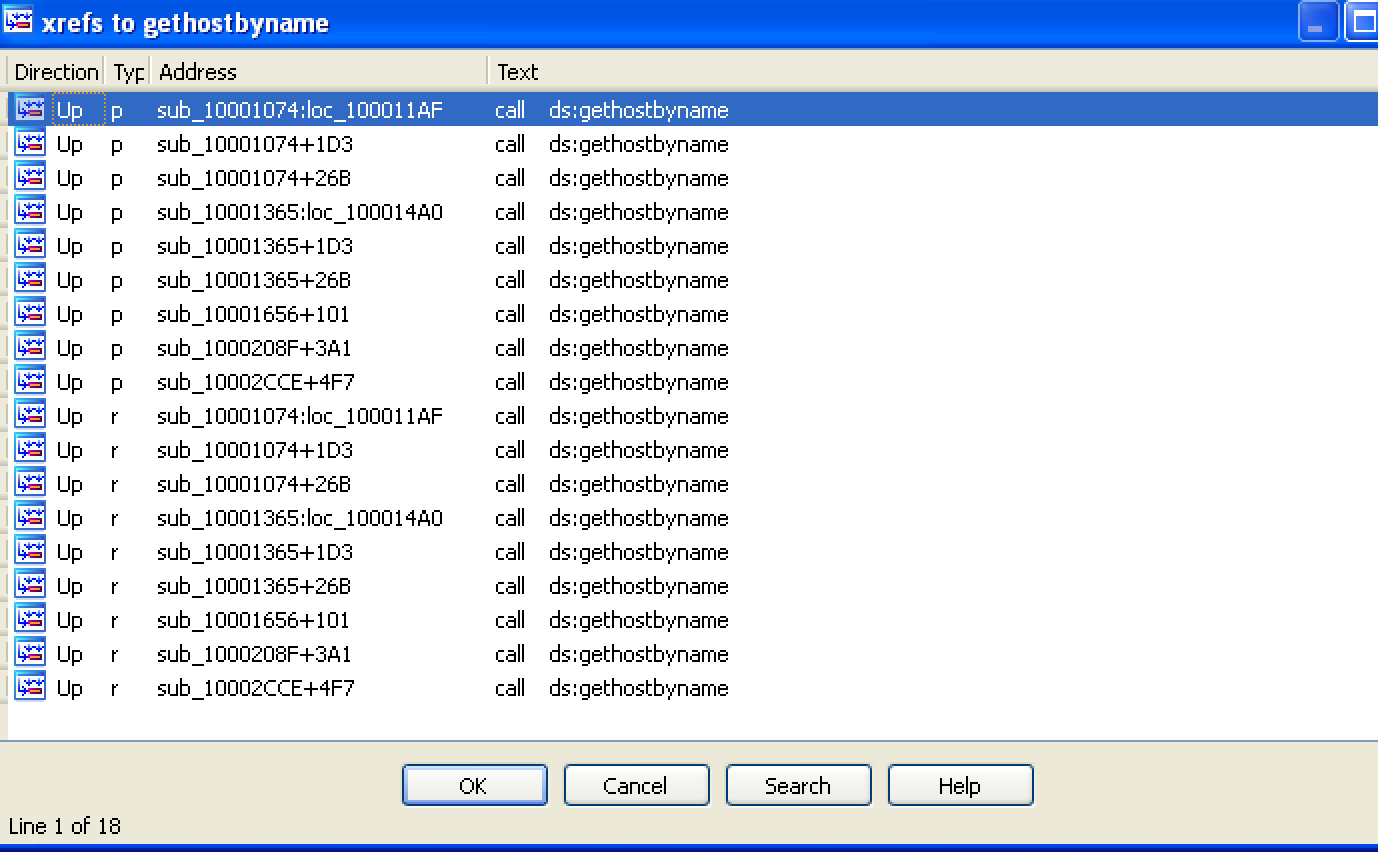
HW5

Xin Yang (xy213)

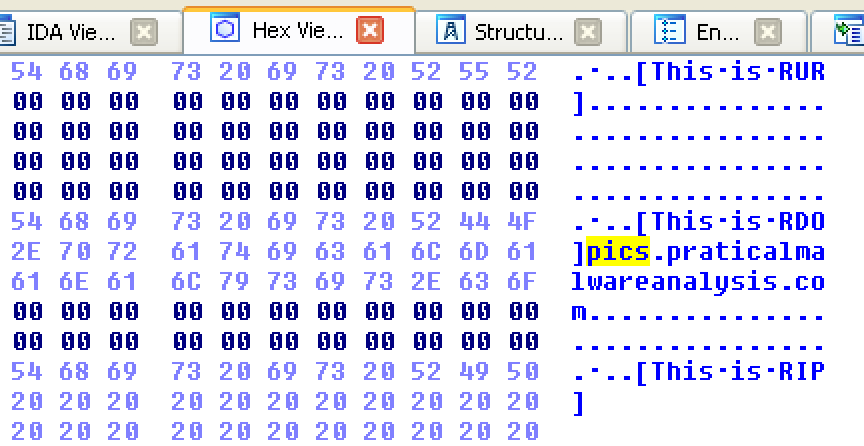
1. The address od DllMain is 1000D02E.
2. It’s located at the idata part.



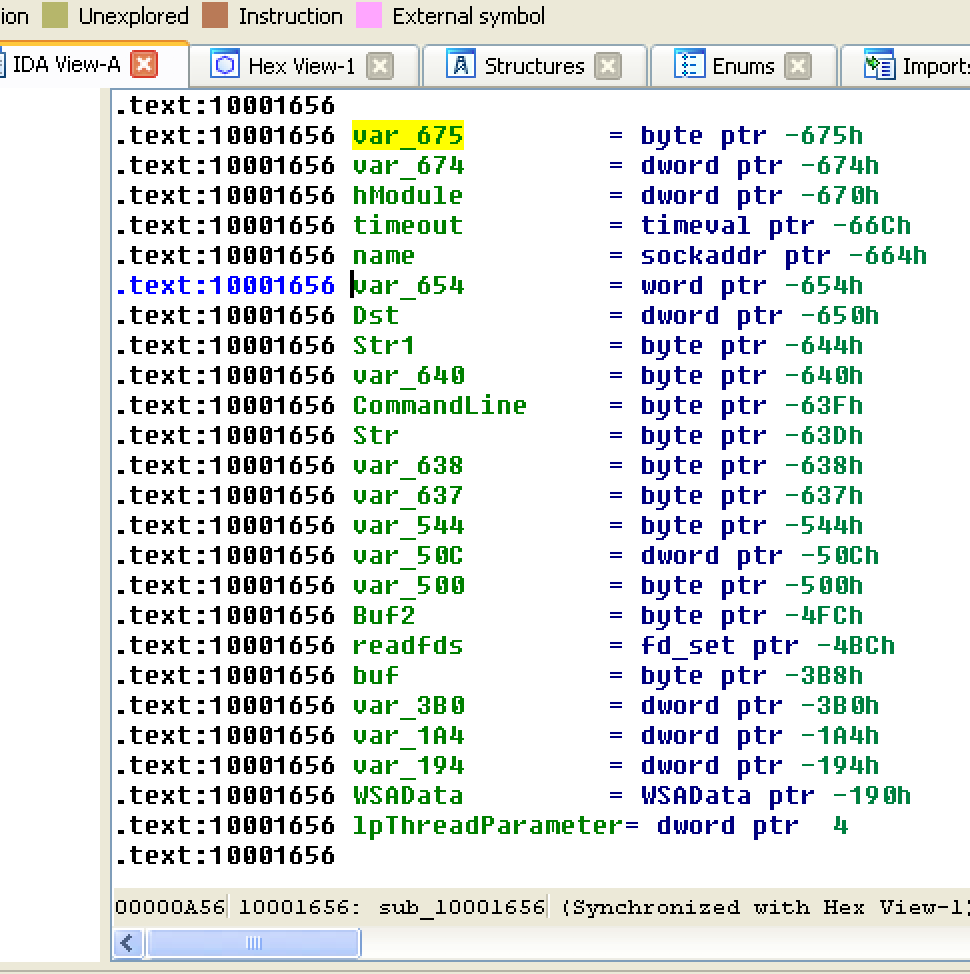
1. 18 functions call gethostbyname.



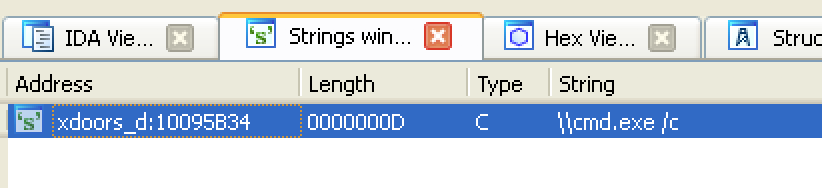
1. By finding address 0x10001757(0x10001656 + 101), we can see the mov instruction with off\_10019040 moved into eax register. When we click this offset, we can see this address in hex view: “pics.praticalmalwareanalysis.com”.



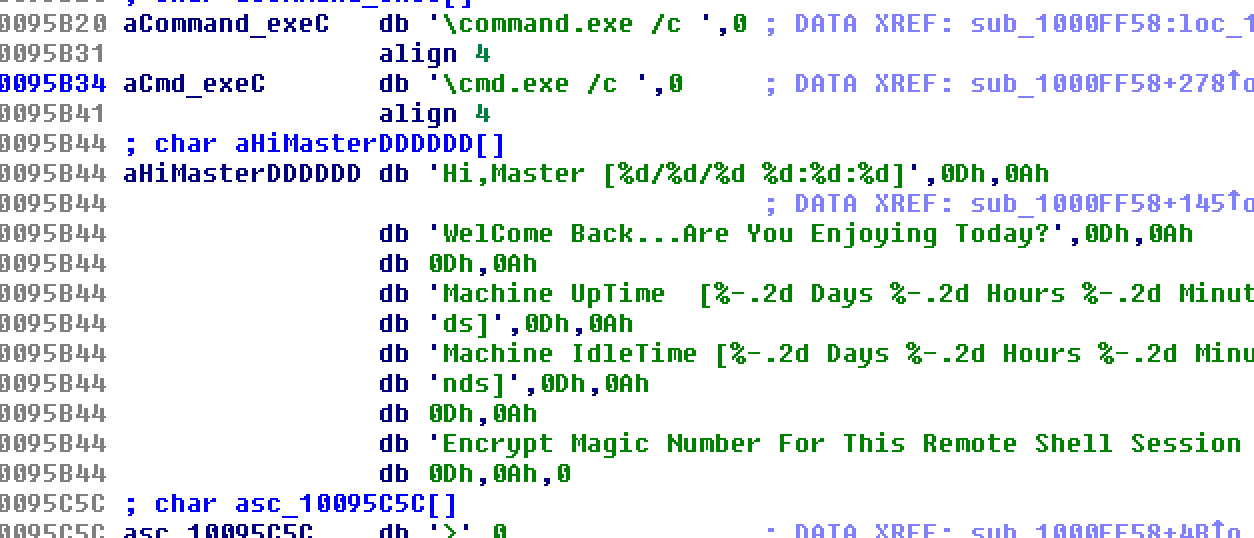
1. 12 local variables have been recognized by IDA pro.

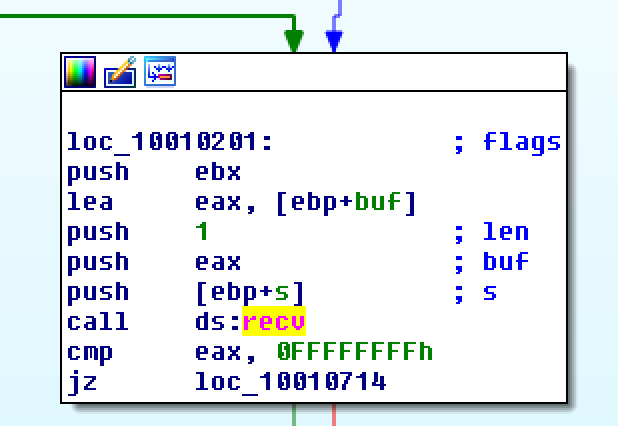


1. IDA Pro recognized only 1 parameter.
2. “\cmd.exe /c” is located at xdoors\_d: 10095B34

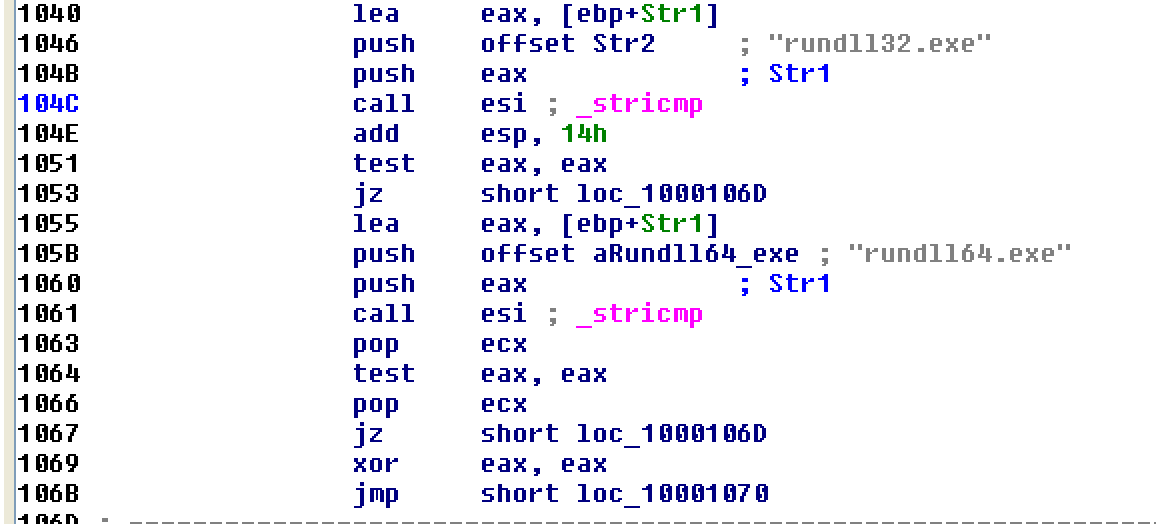


1. In the area of code that references \cmd.exe /c, command.exe or cmd.exe will be executed and display some information such as “Hi, Master” in an interface like a command line. Also it mentioned “Encrypt Magic Number For This Remote Shell Session”, which could mean that it’s a remote shell launching part. Also follow the control flow we can trace the recv function call, which is related to web socket.

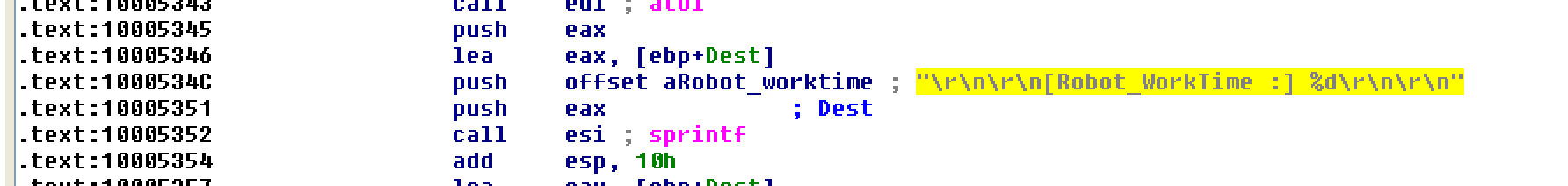


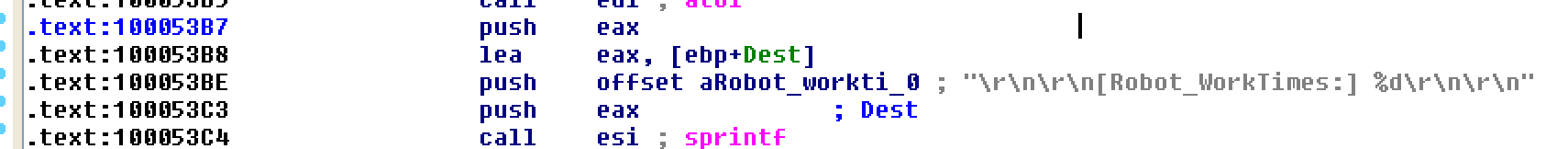


1. This malware would set dword\_1008E5C4 to 1 if this is a 64 bit system, which runs rundll64.exe instead of rundll32.exe.

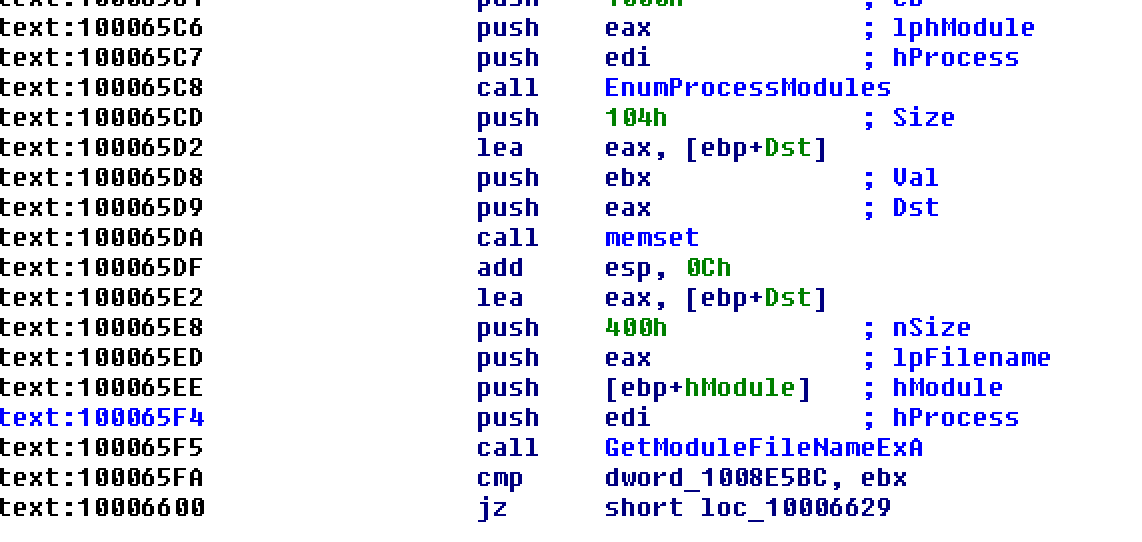


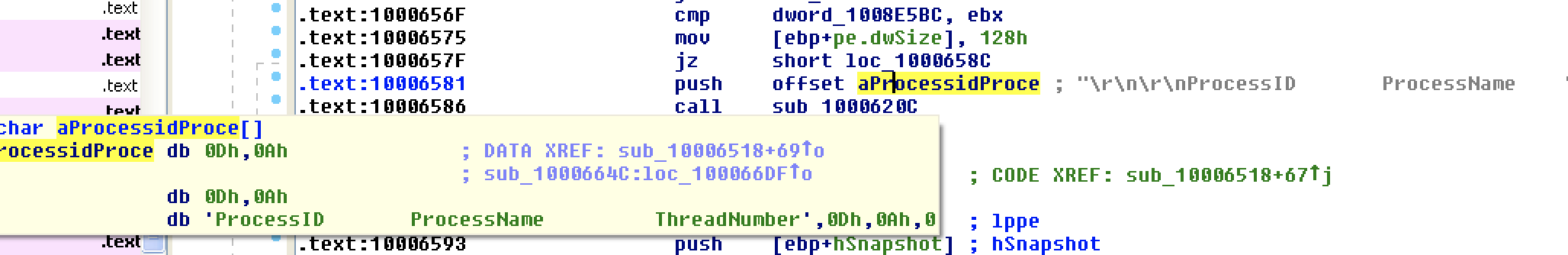
1. If the comparison is successful, the program will call 0x100052A2, then jump to loc\_10005309, and print “\r\n\r\n[Robot\_Worktime: ] %d\r\n\r\n” or “\r\n\r\n[Robot\_Worktimes: ] %d\r\n\r\n”.

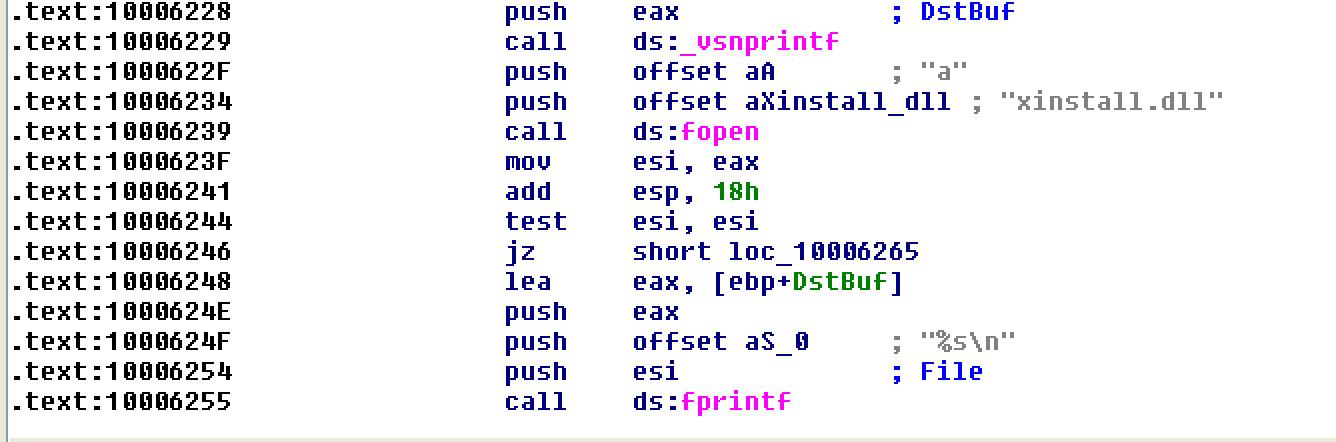




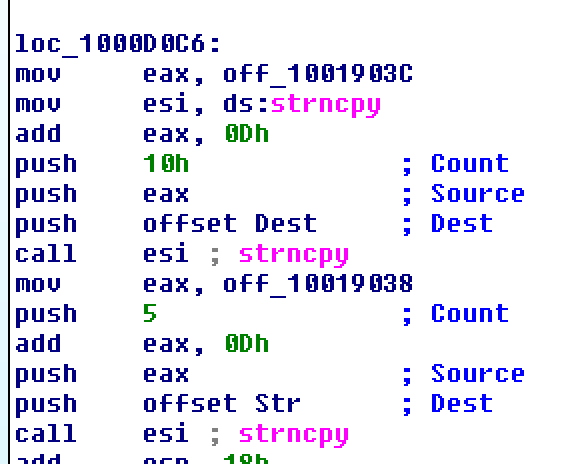
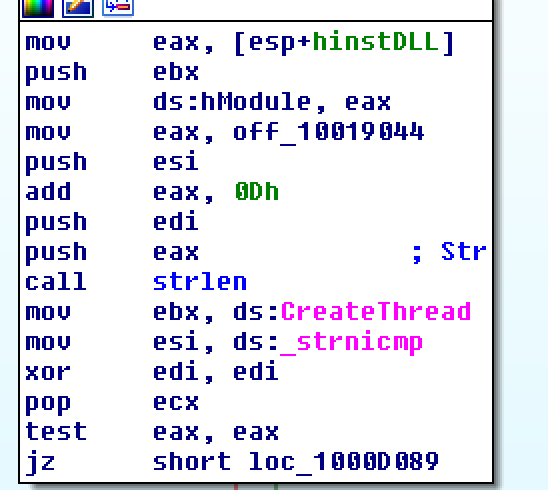
1. PSLIST would list related processes information including modules and thread number, then write them into xinstall.dll.



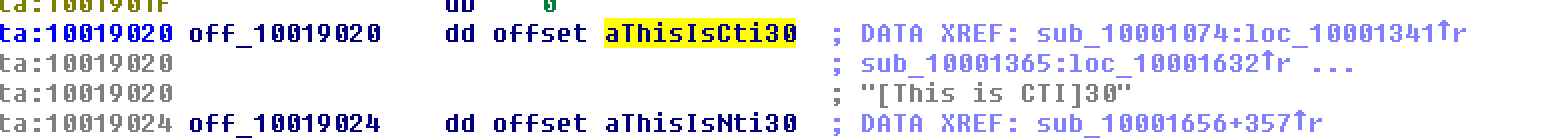


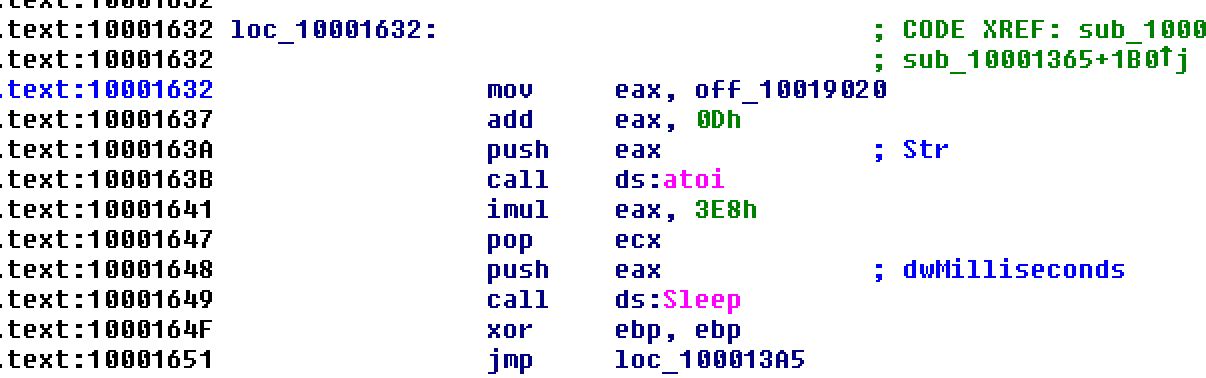


1. GetSystemDefaultLangID and sprintf could be called in this sub routine. We can rename it as send\_default\_languageid.
2. DLLMain calls CreateThread, \_strnicmp and strncpy directly, calls too many at the depth of 2 such as sprint, send, etc.

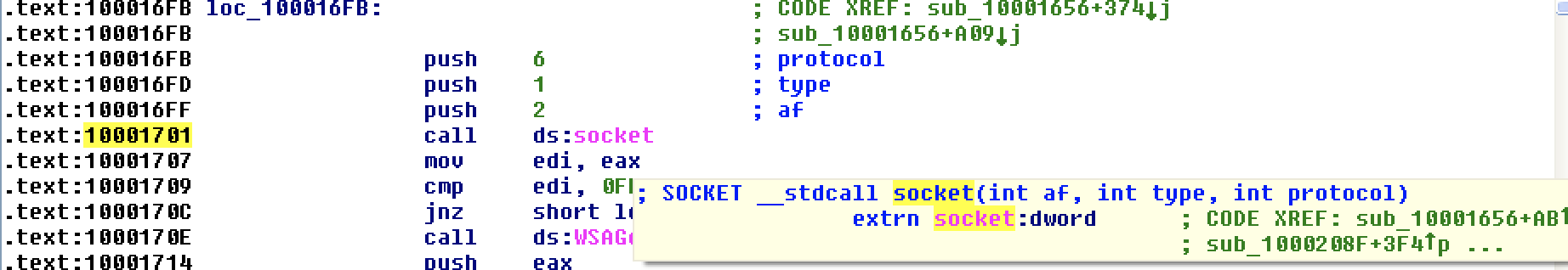


1. This program will sleep for 43 seconds.

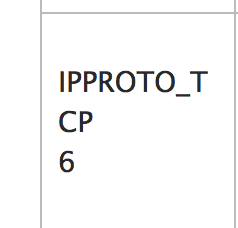
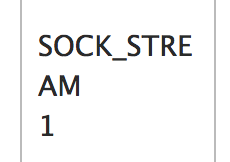
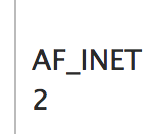




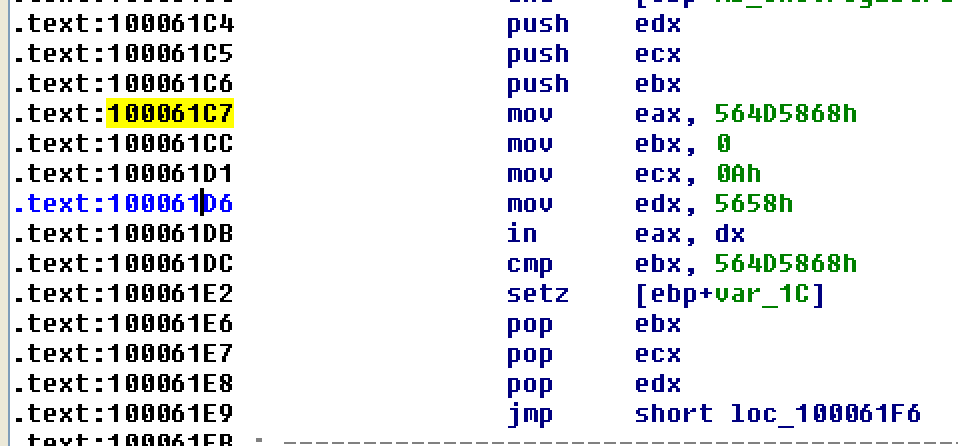
1. The parameters are 2, 1, 6 (af, type, protocal).

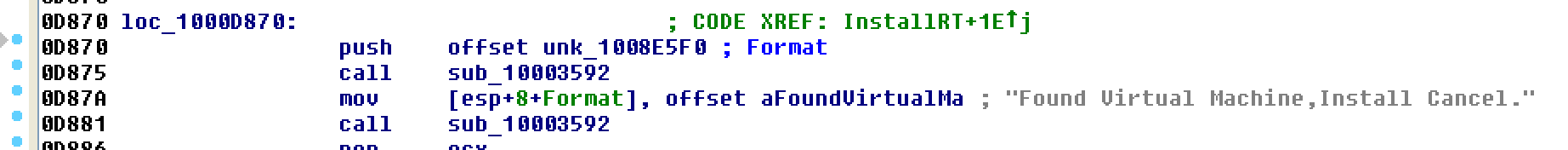


1. 2: AF\_INET, 1: SOCK\_STREAM: IPPROTO\_TCP

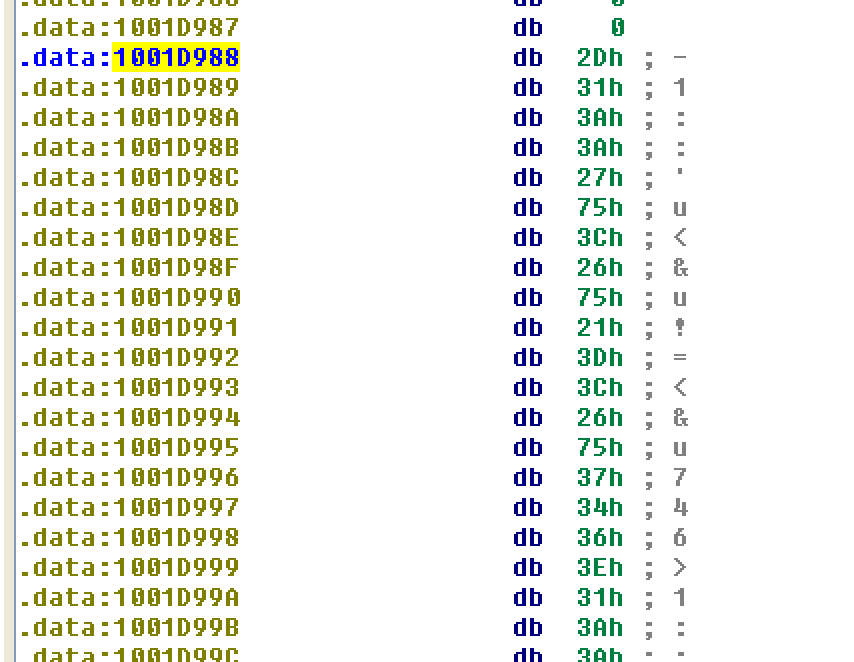


1. The “in” instruction is used at 100061DB with the string VMXh in sub routine 10006196. From the cross reference, we tried to enter the InstallRT, and we found there’s a sentence “Found Virtual Machine, Install Cancel.”, which proves there’s a vm detection.





1. There’re lots of single characters starting from 1001D988, which can be arguments for some certain commands.



2. Press A at 1001D988 or right click and select the strings option, which is set to be ASCII by default.
3. This