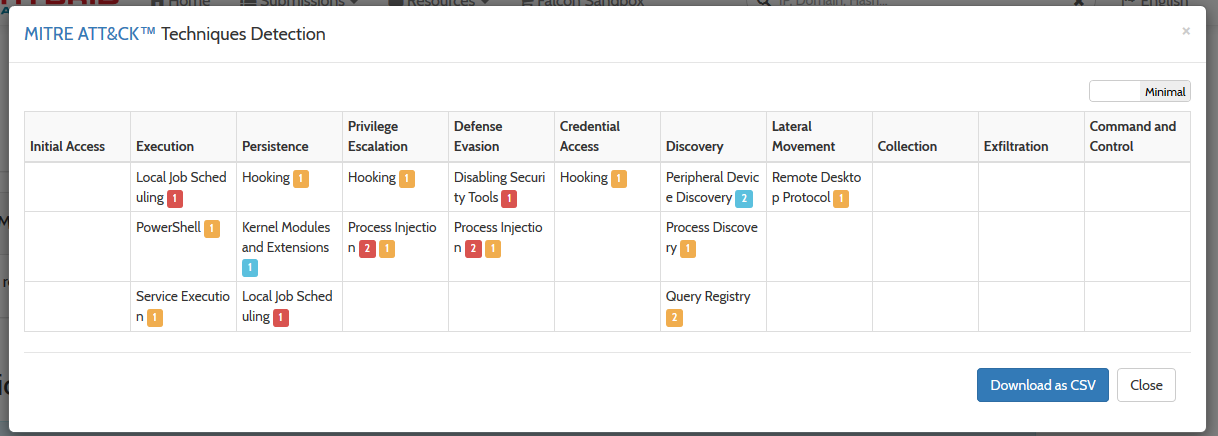
Hybrid: <https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100>



* Created Alternate data stream file: created file "%APPDATA%\VsCard\9b7ff7f7f46a19bf3d06bba19946a93da2adfbe7e340a79d3f729c4b99b243a9.exe:Zone.Identifier". ***So what is in this file?***
* Dropped file "9b7ff7f7f46a19bf3d06bba19946a93da2adfbe7e340a79d3f729c4b99b243a9.exe" as malicious (classified as "BehavesLike.PWSZbot" with 12% detection rate). Waduhek does this do?. Also spawned this as well. ***What does this file Do?***
* Vritual Memory Alocation : "<Input Sample>.exe" allocated memory in "%WINDIR%\System32\cmd.exe"  
  "<Input Sample>.exe" allocated memory in "\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale"  
  "<Input Sample>.exe" allocated memory in "C:\9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8.exe"
* Disabling monitor tools: Process "cmd.exe" with commandline "/c powershell Set-MpPreference -DisableRealtimeMonitoring $true" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))  
  Process "powershell.exe" with commandline "powershell Set-MpPreference -DisableRealtimeMonitoring $true" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))

Process "sc.exe" with commandline "sc stop WinDefend" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))  
Process "sc.exe" with commandline "sc delete WinDefend" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))

***What does disabling these do?***

* List of spawned process

Spawned process "<Input Sample>.exe" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))  
Spawned process "cmd.exe" with commandline "/c sc stop WinDefend" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))  
Spawned process "cmd.exe" with commandline "/c sc delete WinDefend" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))  
Spawned process "sc.exe" with commandline "sc stop WinDefend" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))  
Spawned process "cmd.exe" with commandline "/c powershell Set-MpPreference -DisableRealtimeMonitoring $true" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))  
Spawned process "sc.exe" with commandline "sc delete WinDefend" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))  
Spawned process "9b7ff7f7f46a19bf3d06bba19946a93da2adfbe7e340a79d3f729c4b99b243a9.exe" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))  
Spawned process "powershell.exe" with commandline "powershell Set-MpPreference -DisableRealtimeMonitoring $true" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))

* Slept many times : "9b7ff7f7f46a19bf3d06bba19946a93da2adfbe7e340a79d3f729c4b99b243a9.exe" (Thread ID: 3440) slept "520" times (threshold: 500)
* RDP Keys : "<Input Sample>.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER"; Key: "TSUSERENABLED")  
  "9b7ff7f7f46a19bf3d06bba19946a93da2adfbe7e340a79d3f729c4b99b243a9.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER"; Key: "TSUSERENABLED")

***So can we RDP? Which function does this?***

* Process Spawned:

Spawned process "cmd.exe" with commandline "/c sc stop WinDefend" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))  
Spawned process "cmd.exe" with commandline "/c sc delete WinDefend" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))  
Spawned process "sc.exe" with commandline "sc stop WinDefend" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))  
Spawned process "cmd.exe" with commandline "/c powershell Set-MpPreference -DisableRealtimeMonitoring $true" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))  
Spawned process "sc.exe" with commandline "sc delete WinDefend" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))  
Spawned process "9b7ff7f7f46a19bf3d06bba19946a93da2adfbe7e340a79d3f729c4b99b243a9.exe" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))  
Spawned process "powershell.exe" with commandline "powershell Set-MpPreference -DisableRealtimeMonitoring $true" ([Show Process](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100))

***What does these commands do?***

Analysed 8 processes in total.

* C:\Users\dell\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\5D3CE49D.tmp[*Input Sample*](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100#00022812-00003716) (PID: 3716) https://www.hybrid-analysis.com/img/process_flag/multiscan_match_white.png8/64
  + https://www.hybrid-analysis.com/images/icon_dummy.png[cmd.exe](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100#00023575-00002144) /c sc stop WinDefend (PID: 2144) https://www.hybrid-analysis.com/img/process_flag/reduced_monitoring.png
    - https://www.hybrid-analysis.com/images/icon_dummy.png[sc.exe](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100#00023601-00002684) sc stop WinDefend (PID: 2684) https://www.hybrid-analysis.com/img/process_flag/reduced_monitoring.png
  + https://www.hybrid-analysis.com/images/icon_dummy.png[cmd.exe](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100#00023586-00002384) /c sc delete WinDefend (PID: 2384) https://www.hybrid-analysis.com/img/process_flag/reduced_monitoring.png
    - https://www.hybrid-analysis.com/images/icon_dummy.png[sc.exe](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100#00023609-00002992) sc delete WinDefend (PID: 2992) https://www.hybrid-analysis.com/img/process_flag/reduced_monitoring.png
  + https://www.hybrid-analysis.com/images/icon_dummy.png[cmd.exe](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100#00023608-00002568) /c powershell Set-MpPreference -DisableRealtimeMonitoring $true (PID: 2568) https://www.hybrid-analysis.com/img/process_flag/reduced_monitoring.png
    - https://www.hybrid-analysis.com/images/icon_dummy.png[powershell.exe](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100#00023654-00003400) powershell Set-MpPreference -DisableRealtimeMonitoring $true (PID: 3400) https://www.hybrid-analysis.com/img/process_flag/logged_stdout.pnghttps://www.hybrid-analysis.com/img/process_flag/reduced_monitoring.png
  + https://www.hybrid-analysis.com/images/icon_dummy.png[9b7ff7f7f46a19bf3d06bba19946a93da2adfbe7e340a79d3f729c4b99b243a9.exe](https://www.hybrid-analysis.com/sample/9b6ff6f6f45a18bf3d05bba18945a83da2adfbe6e340a68d3f629c4b88b243a8?environmentId=100#00023634-00002432) (PID: 2432) https://www.hybrid-analysis.com/img/process_flag/multiscan_match_white.png8/64

**Questions to answer in order:**

1. ***What does these commands do?***
2. ***So what is in this ADS file?***
3. ***So can we RDP? Which function does this?***

**Answer to 1:**

* /C Carries out the command specified by the string and then terminates. sc stop WinDefend stops windows defender
* Sc (Service control). sc delete WinDefend will delete the servicez
* You can exclude certain files, folders, processes, and process-opened files from Windows Defender Antivirus scans. powershell Set-MpPreference -DisableRealtimeMonitoring $true, Disable already excluded files, and use manual exclusion

Linl: <https://www.peerlyst.com/posts/using-powershell-in-windows-defender-eli-shlomo>

**Setting Windows Defender Preferences** – The Set-MpPreference configures preferences for Windows Defender scans and updates. Just disable real time monitoring

* HKLM\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER enable RDP

**Running in VM:**

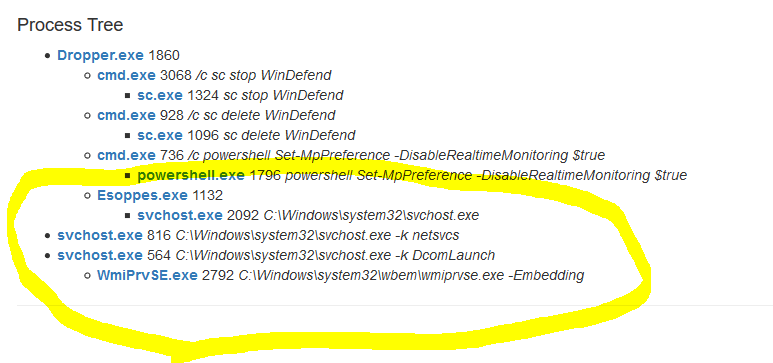
**->** Different file in my VM



Esposs.exe is perhaps similar?

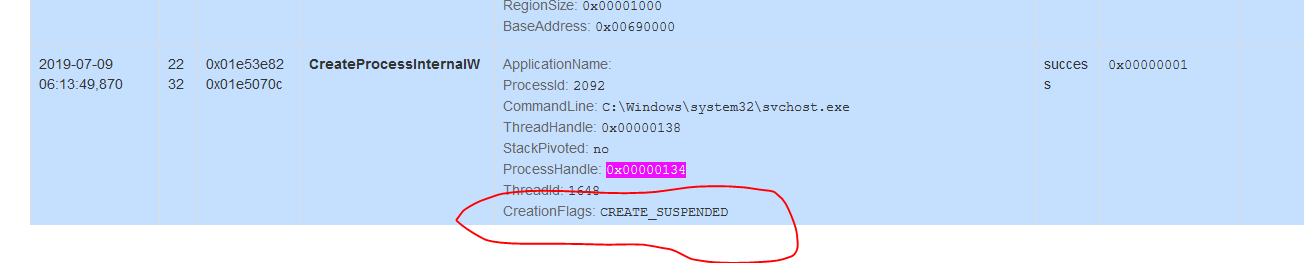
[https://cape.contextis.com/analysis/84882/#](https://cape.contextis.com/analysis/84882/)

**Look at these interesting stuffs**



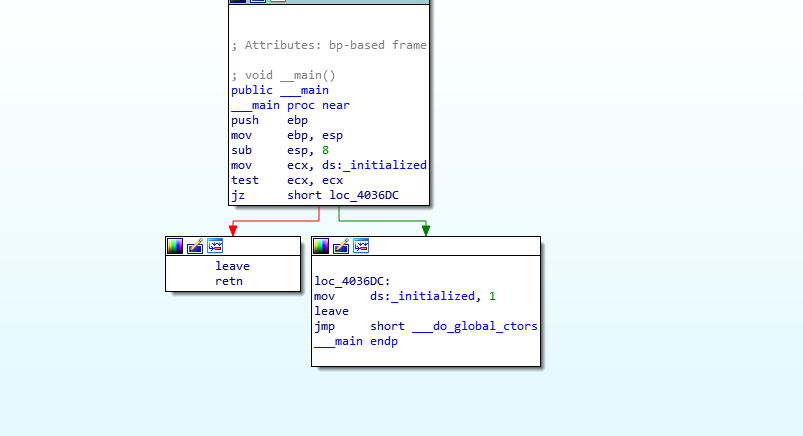
Process Injection?? Not Sure

CreateProcessInternalW in suspended mode



**Reversing:**

main just calls .ctor functions (.ctor array of pointers to constructor fuctions)



\_Z11EncryptDataPhiS\_Pm(ptr to "3<m5s@yghz/QfJX",0x10,ptr to raData (004041A0))

Function0040155D (ptr to AtxetnoCeriuqcAtpyrC) // Does some thing interesting

{

// Allocates memory, reverses the string, puts in allocated memory and gives back the // pointer to it

Edx = pointer to AtxetnoCeriuqcAtpyrC

Eax = 0

repne scasb // compares edx I guess until it gets what is in eax i.e. 0, and puts in ecx

ecx = sizeof(pointer to AtxetnoCeriuqcAtpyrC)

dec [ebp+Size\_to\_alloc]

mov eax, [ebp+var\_10]

mov edx, [ebp+Pointer\_to\_allocated\_memory]

add edx, eax ; Initially 0 + pointer\_to\_allocated\_memory

mov eax, [ebp+Size\_to\_alloc]

mov ecx, [ebp+Pointer\_to\_AtxetnoCeriuqcAtpyrC]

add eax, ecx

mov al, [eax]

mov [edx], al

inc [ebp+var\_10]

ex: ptr to allocated memory = 00001,

size = 6

ptr to reversestring = 000008

for (I := 0; I++; I > size\_of\_allocated; --size\_of\_allocated)

{

edx = ptr to allocated memory + I //

eax = size\_to\_alloc

ecx = ptr to reverse string

eax = eax + ecx // 1st case 5 + 0000008 // fifth element,, nex is 4 + .. as the size decreases we get earlier index

al = pointerd\_by\_eax

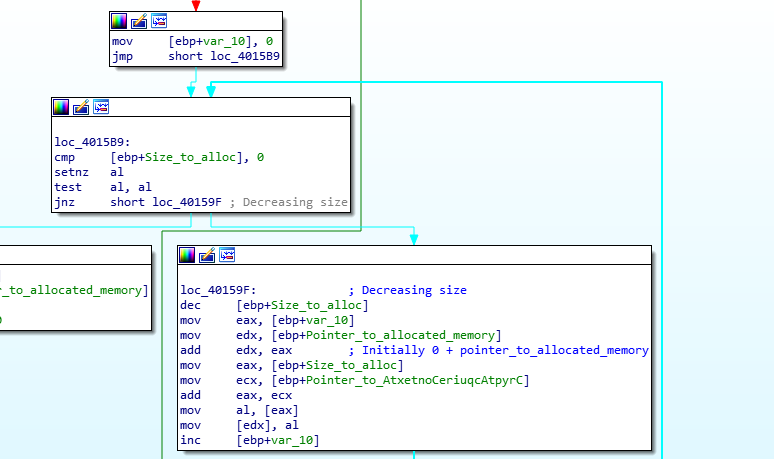
pointer\_byEdx = al

i

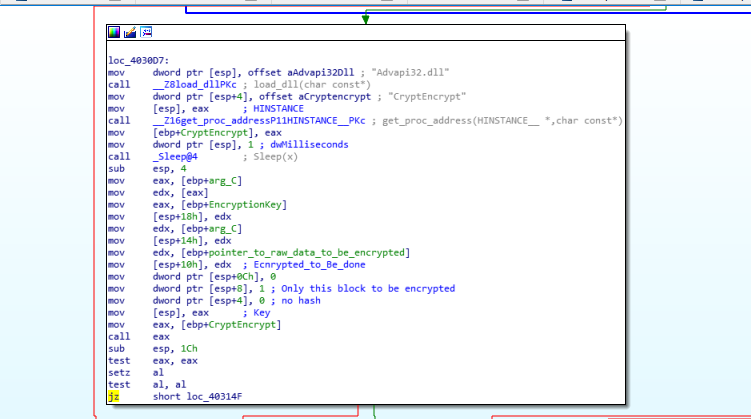
}

} // CryptAcquireContextA

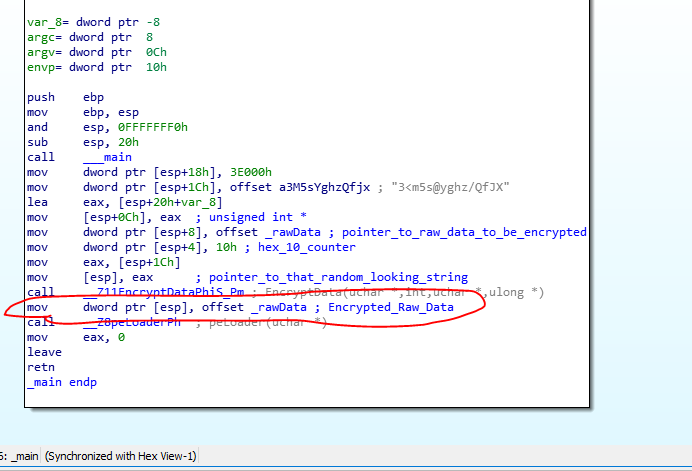
Setnz sets register to 1 if cmp was equal



Does a lot of cryptorelated stuffs, and finally encrypts some data



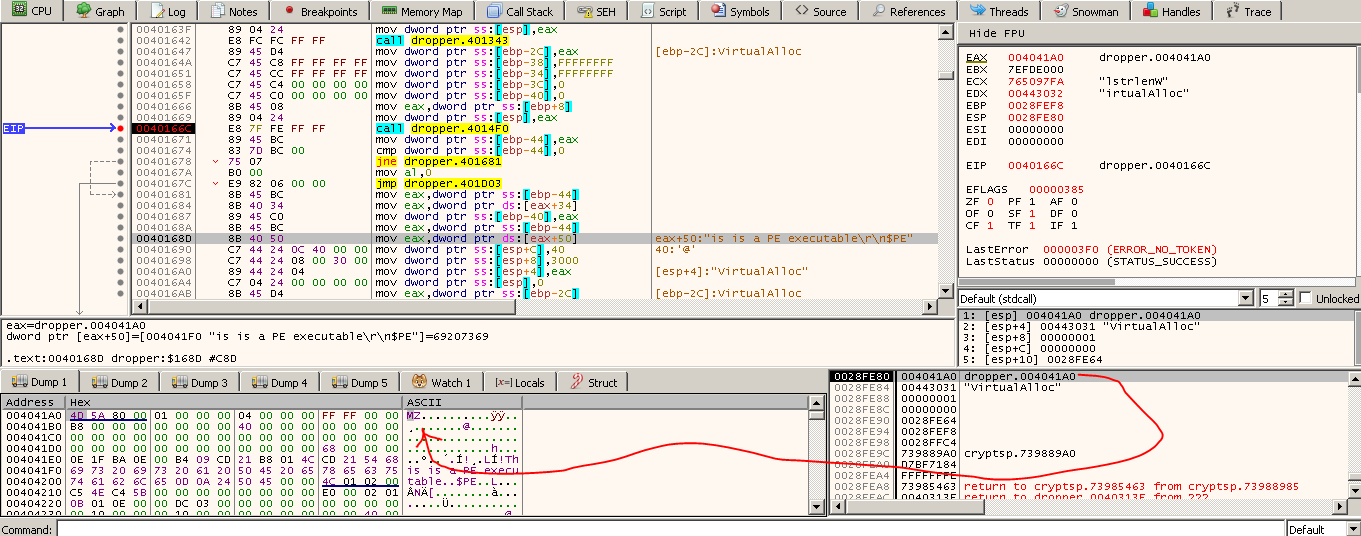
Pointer to the raw data is again passed to next function peloader(), so may be this is pefile



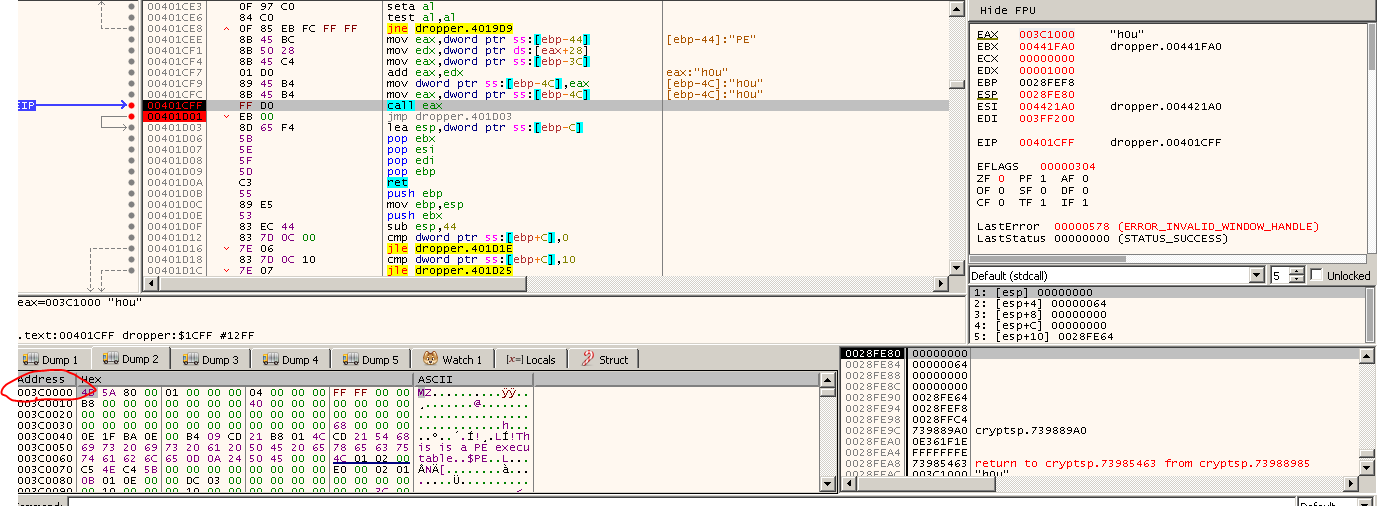
Does reverse stuff again for kernel32.dll and gets address of virtualalloc(). It later passes the encrypted raw data to getntHeaders()



While debugging, yes it is infact a PE Executable

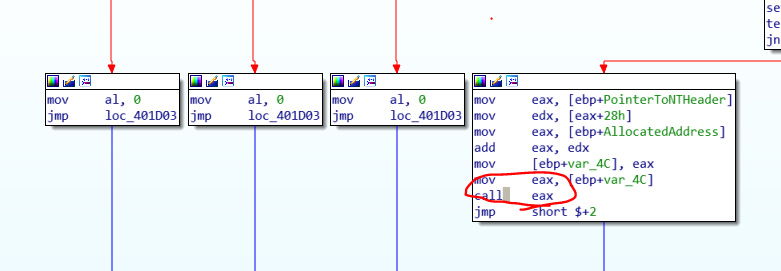


It then allocates address, A second PE file in next allocated address. Calls A function that was generated dynamically by calling the virtualalloc.



Calls function within this new PEfile

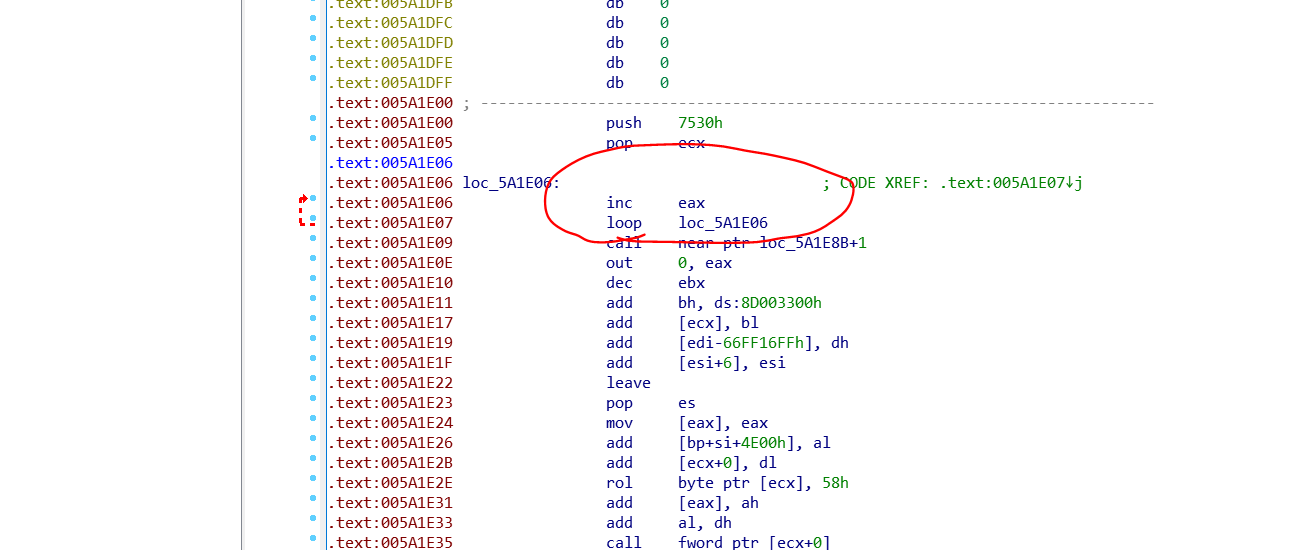
In IDA:



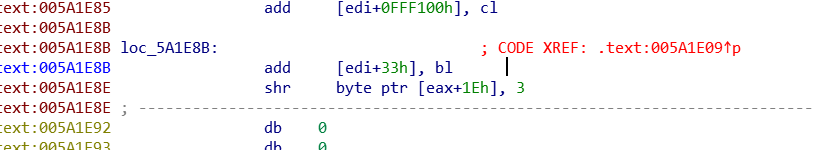
So all the calls happens after here, Some anti disassembly tricks here

I dumped the location into file using x64 dbg. It was not very helpful. So I debugged

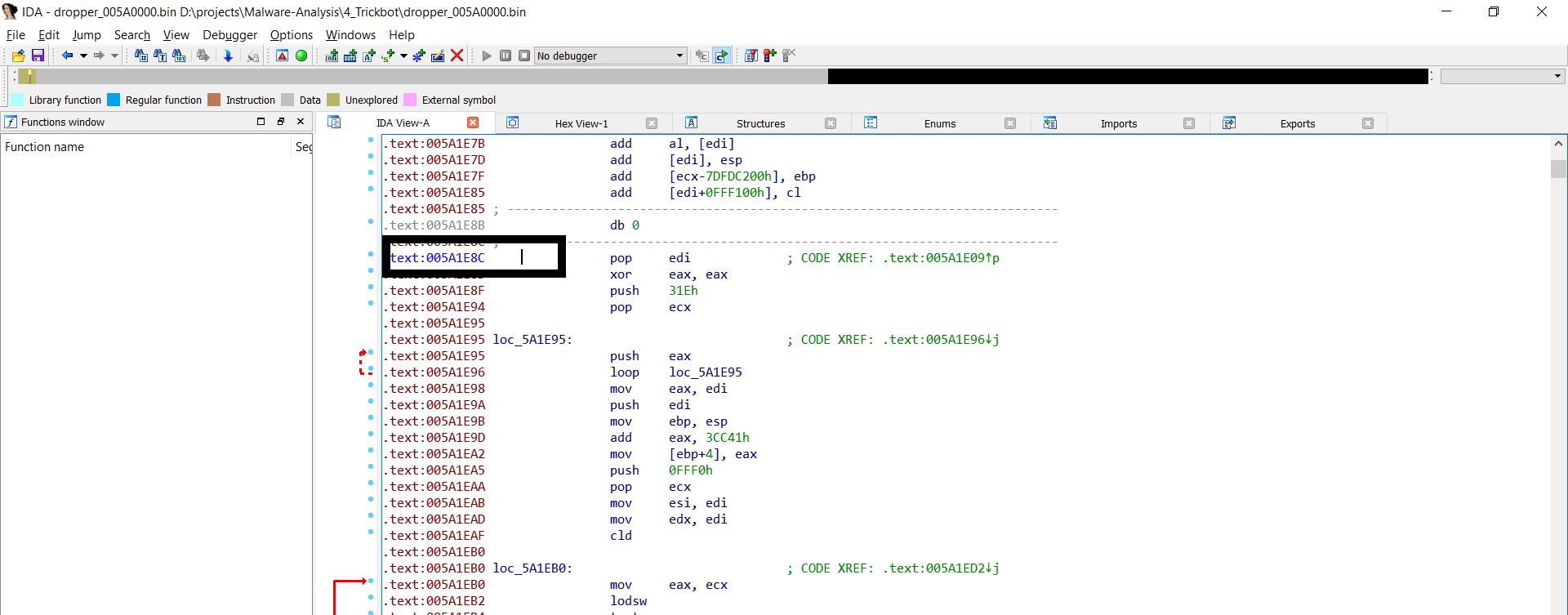
There is just a loop that keeps increasing the value of eax, which by the way when debugged seems to point at the address below.



So the loop instruction loops till ecx is zero, push pushed 0x7350 into stack then pops back to ecx, and does a trick, call someaddr + 1 address 5A1E8B is



But when I changed the section to data, changed the section 5A1E8B+1=5A1E8C to code, it changed to

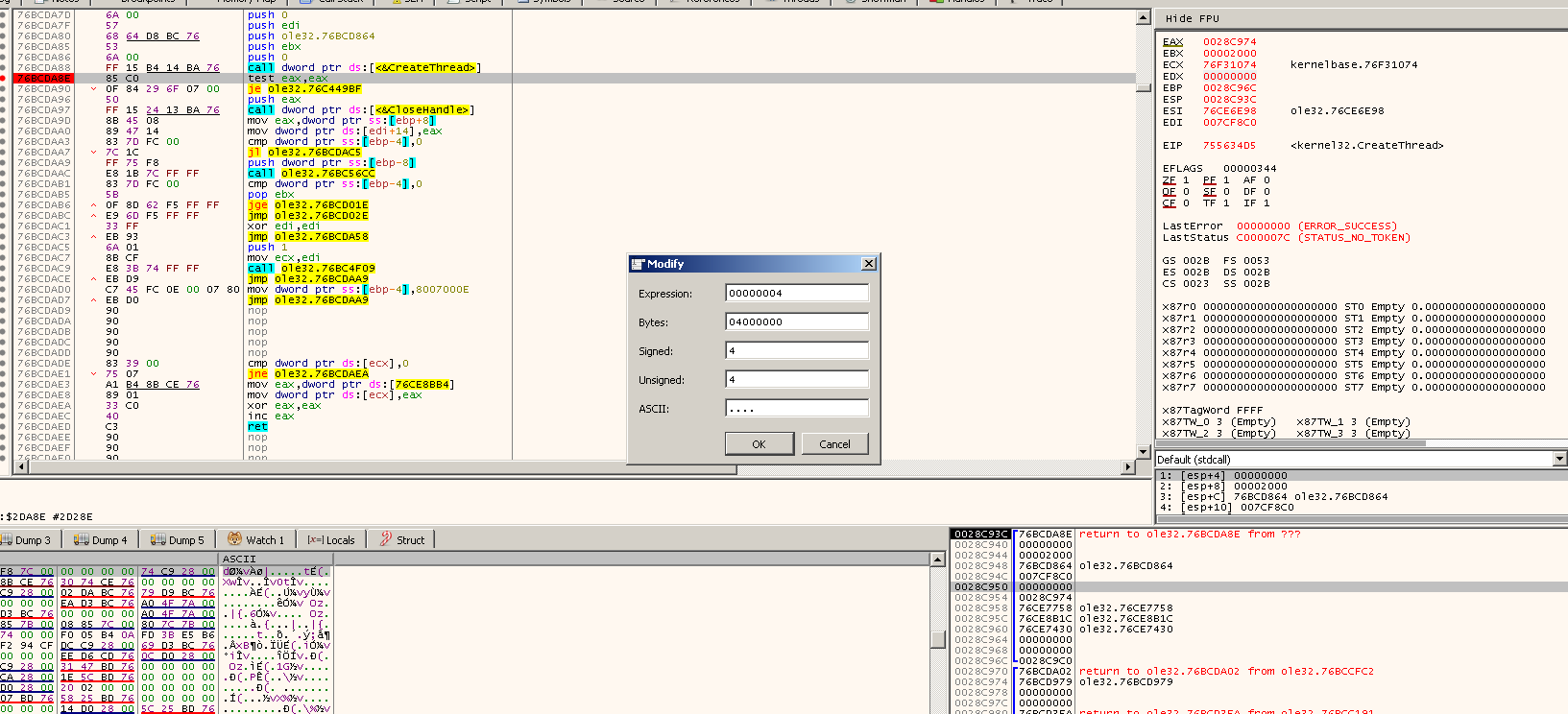


Then there is call eax, pointing to some code section that was initially treated as data

And this is what resolves and calls all of those create stuff, it exited, so let me set breakpoint in createthread then

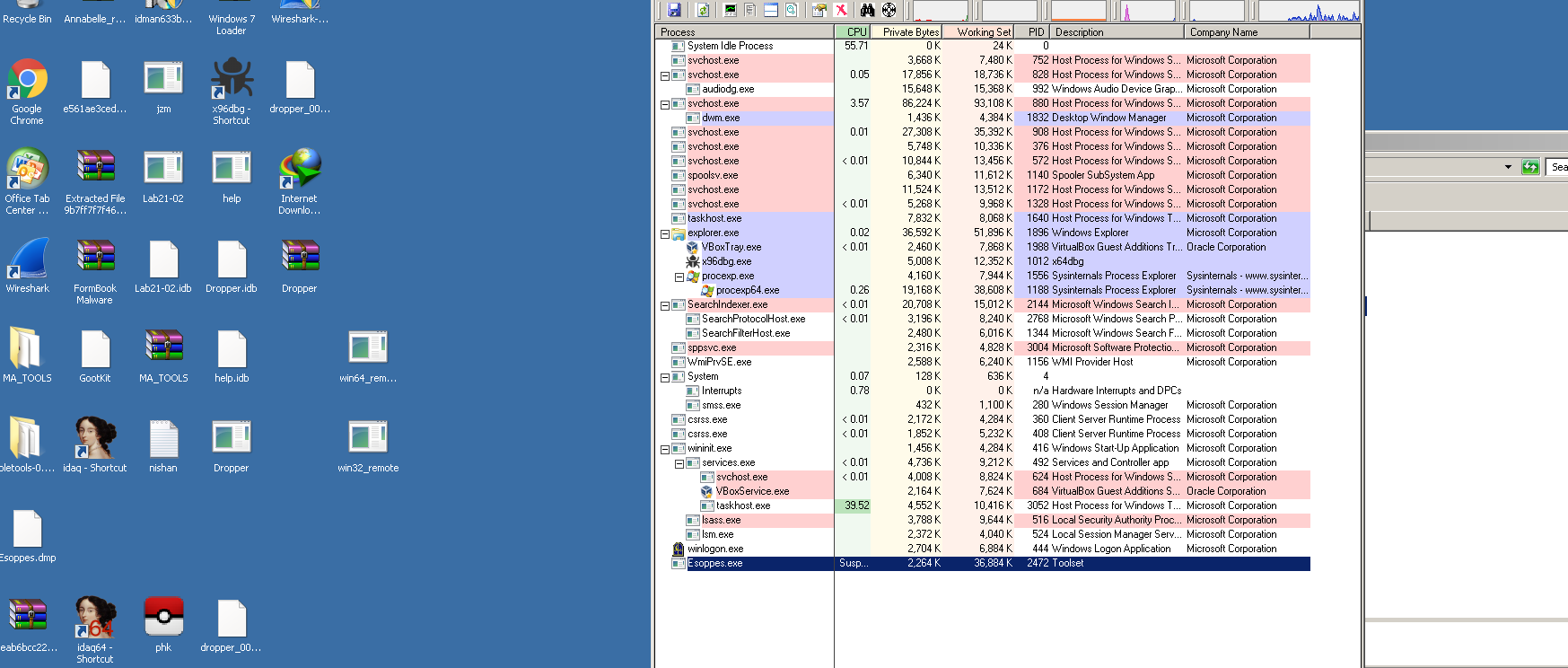
CreateFile, something that was not there, and yep after all that it tries to createthread

We change the creation flag to 0x0000004 to start in suspended mode



30th July 2019

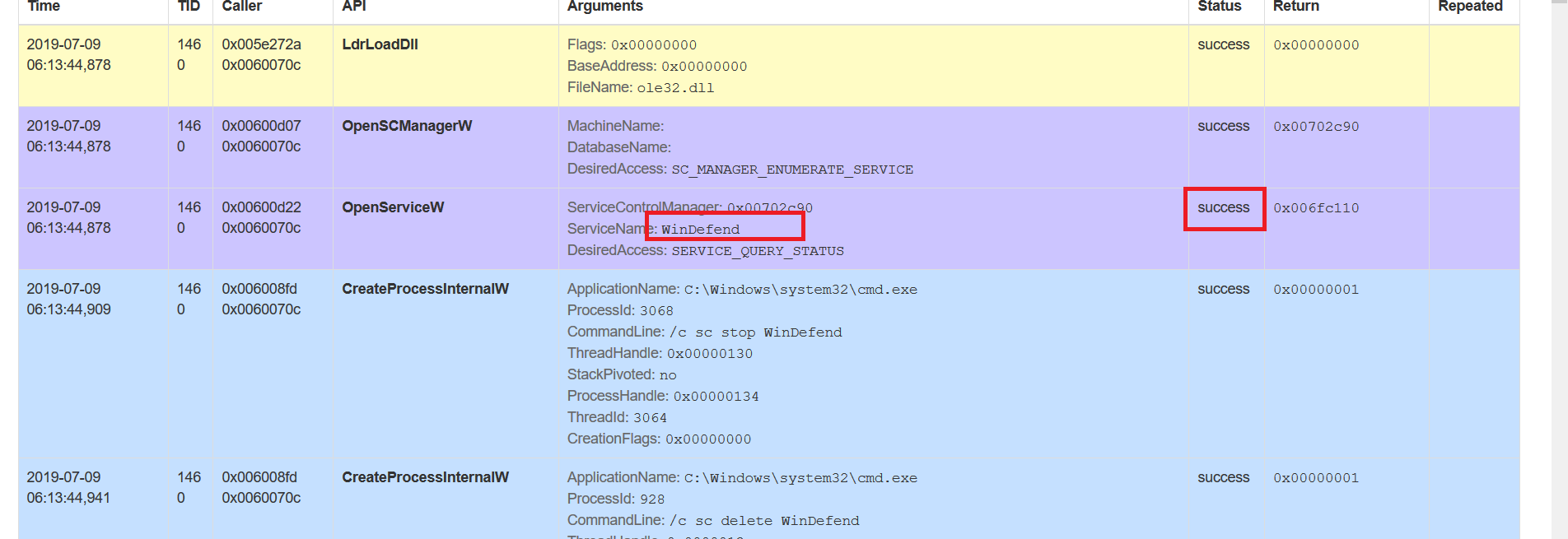
When debugger was not attached, esposs.exe was launched



So when the process copies and runs another process, it does process injection, but when I run it just does the copying agin.

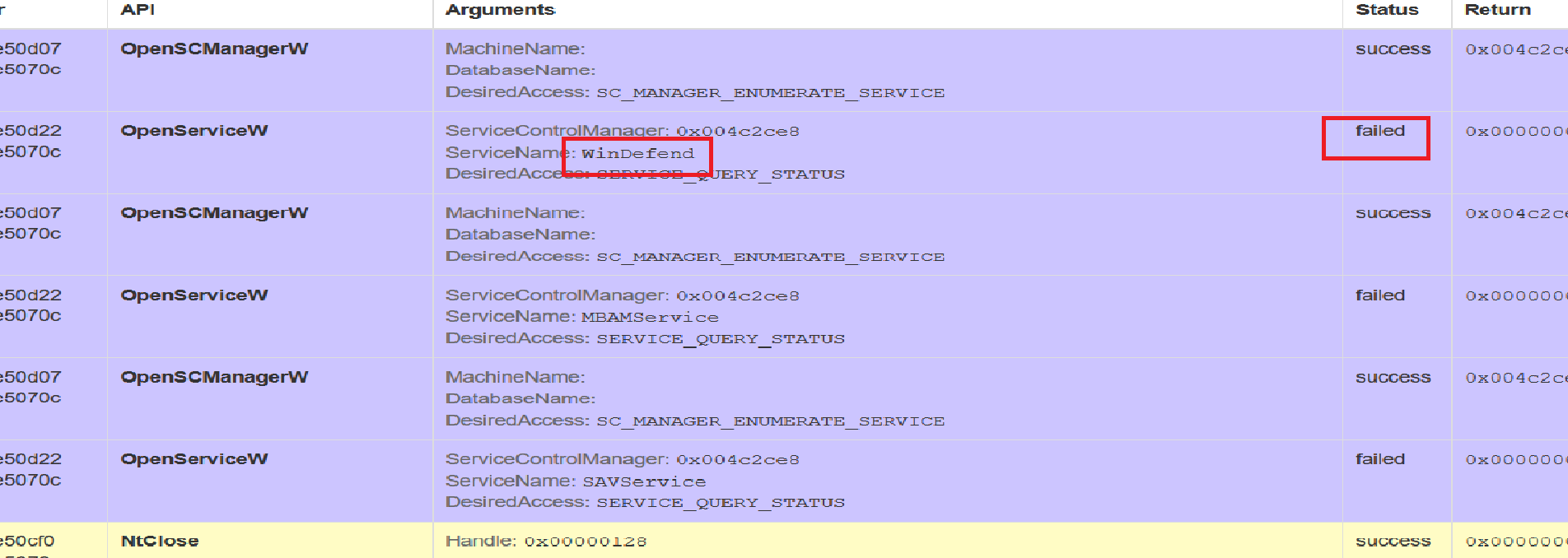
* Check Cape sandbox api calls to see what is causing this

Now I do understand, the cape sandbox,



Since winddefend service was not disabled, the openservicew is successful, dropeer goes on this route.

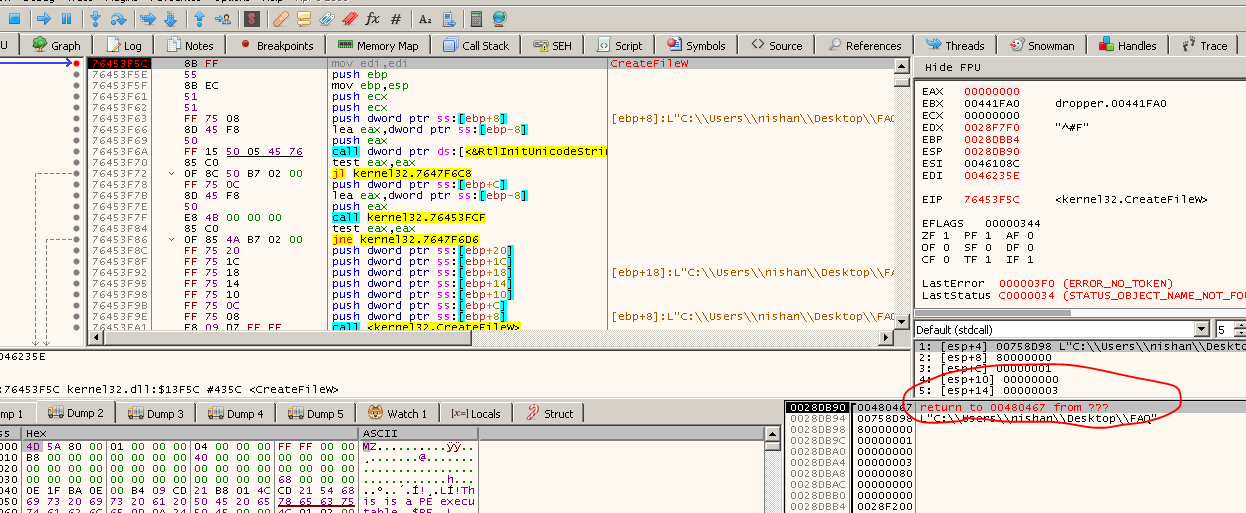
But for esoppes.exe goes different route.



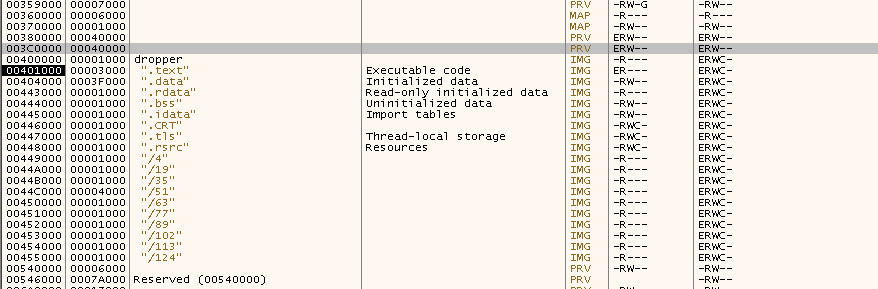
And I started the program changed the return value, then landed in the getfolderpathw and managed that as well, but exited, forgot to check if the createprocess was met, I set the breakpoint, but no breaks, will check again. I can not find shgetfolderpathw

I got there, a lot of decryption and stuff, difficult to get there,

After we exit, the same shit functions, there is a function call, dat function call is da one



And craeate thread



New processCreation inside the call to eax, and all of the systemdisable happens here as well.