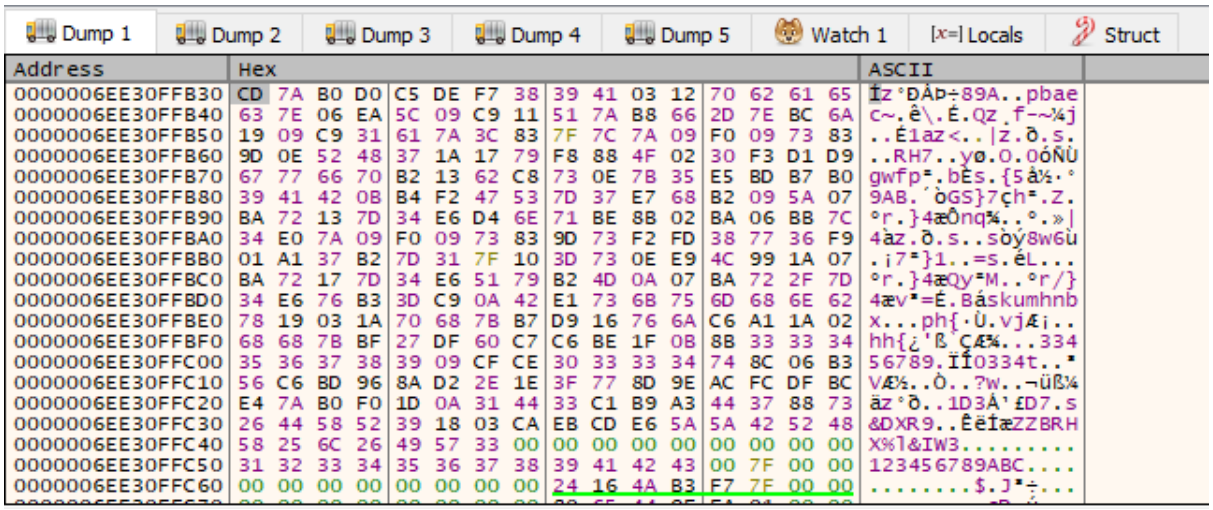
Analyzing XOR encrypted payload with xdbg

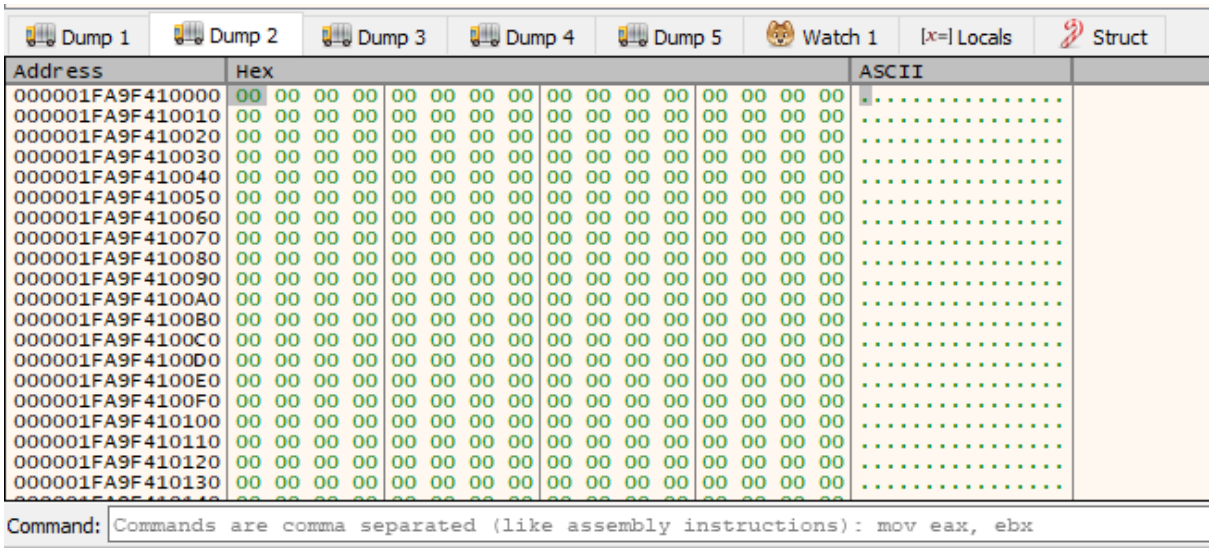
In this section, we will be analyzing, the .exe file, in which the payload is encrypted with XOR.

We must follow the same procedure we followed in the base64 case, so first run the program the cmd, then attach the program in xdbg, then from then analyze the program.

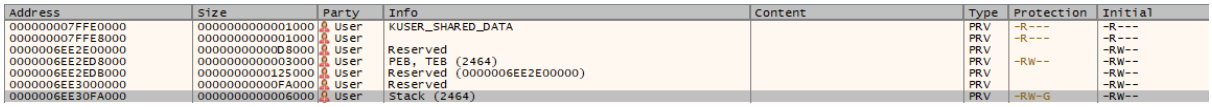
So, in the dump1, we can see the encrypted xor payload:



In dump2, we can see VirtualAlloc has allocated the space:

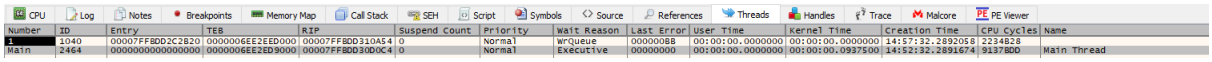


Here when we follow the address, which was there in dump1, if we follow that address in the memory map, we can see a thread value(stack)



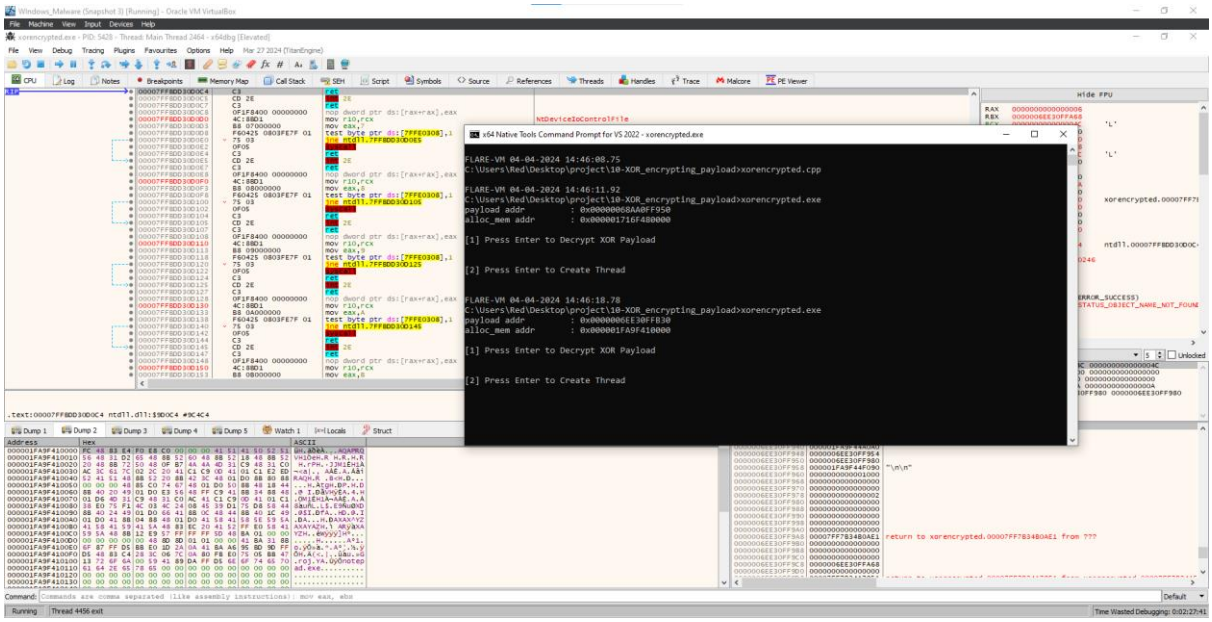
Address	Size	Party	Info	Content	Type	Protection	Initial
0000000007FFE0000	0000000000001000	User	KUSER_SHARED_DATA		PRV	-R---	-R---
0000000007FFE8000	0000000000001000	User			PRV	-R---	-R---
0000006EE2E00000	00000000000D8000	User	Reserved		PRV		-RW--
0000006EE2ED8000	0000000000003000	User	PEB, TEB (2464)		PRV	-RW--	-RW--
0000006EE2EDB000	0000000000125000	User	Reserved (0000006EE2E00000)		PRV		-RW--
0000006EE3000000	00000000000FA000	User	Reserved		PRV		-RW--
0000006EE30FA000	0000000000006000	User	Stack (2464)		PRV	-RW-G	-RW--

Even when following it in the threads, we can see that the same number pops up: “2464”



Number	ID	Entry	TEB	RIP	Suspend Count	Priority	Wait Reason	Last Error	User Time	Kernel Time	Creation Time	CPU Cycles	Name
1	1040	00007FF8DD2C2820	0000006EE2EED000	00007FF8DD310A54	0	Normal	WrQueue	000008B8	00:00:00.0000000	00:00:00.0000000	14:57:32.2892058	2234828	
Main	2464	0000000000000000	0000006EE2ED9000	00007FF8DD30DC4	0	Normal	Executive	00000000	00:00:00.0000000	00:00:00.0937500	14:52:32.2891674	9137BDD	Main Thread

So, now just press enter in the cmd, and we will see that in dump2, the ASCII column will be flooded with decrypted payload.



As we can see here, as soon as we hit enter, we can see the decrypted payload.

And we can see that even the protection got changed:

000001FA9F410000	0000000000001000	User		PRV	ER---	-RW--

Now if we further run the program, it will exit, and Notepad will be opened.