

CONSEGNA U3 S10 L1

- **Librerie richiamate dal malware**

Malware_U3_W2_L1.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

1. KERNEL32.dll: è una Dynamic Link Library di Windows che permette il corretto funzionamento del kernel del sistema operativo. Le funzioni al suo interno si occupano della gestione della memoria (volatile), gestione dei processi (creazione e terminazione), dell'input/ output dei file e della gestione errori.
2. ADVAPI32.dll: è una raccolta di funzioni che si occupano di vari servizi di sistema come la sicurezza, l'accesso al registro, la registrazione degli eventi, e la gestione dell'account utente.
3. MSVCRT.dll: è una libreria contenete funzioni relative all'allocazione di memoria, operazioni di input/output dei file e alla gestione delle eccezioni.
4. WININET.dll: insieme di funzioni di importanza cruciale nella gestione delle connessioni internet, relativa ai protocolli HTTP, FTP, HTTPS. È fondamentale anche nella gestione dei cookies e della cache.

- **Sezioni del malware**

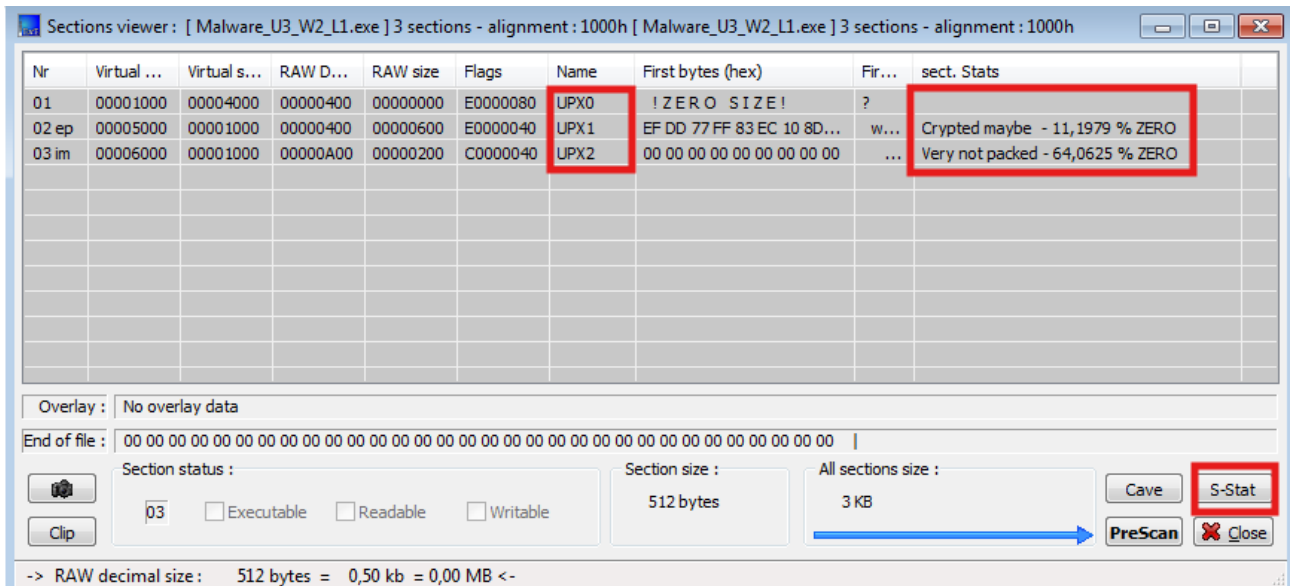
The screenshot shows the 'Sections viewer' window for the file [Malware_U3_W2_L1.exe]. It displays 3 sections with alignment 1000h.

Nr	Virtual ...	Virtual s...	RAW D...	RAW size	Flags	Name	First bytes (hex)	First Ascii 20h b...	sect. Stats
01	00001000	00004000	00000400	00000000	E0000080	UPX0	! Z E R O S I Z E !	?	
02 ep	00005000	00001000	00000400	00000600	E0000040	UPX1	EF DD 77 FF 83 EC 10 8D 44	w +D\$ 4o...	
03 im	00006000	00001000	00000A00	00000200	C0000040	UPX2	00 00 00 00 00 00 00 00	` d` ...	

Below the table, the 'Overlay' section shows 'No overlay data'. The 'End of file' section shows a series of null bytes. The 'Section status' section shows '03' and checkboxes for Executable, Readable, and Writable. The 'Section size' is 512 bytes. The 'All sections size' is 3 KB. There are buttons for 'Cave', 'S-Stat', 'PreScan', and 'Close'. At the bottom, it says '-> RAW decimal size : 512 bytes = 0,50 kb = 0,00 MB <-'

Il malware in analisi si compone di tre sezioni. Per verificarlo ho usato sia **CFFExplorer** che **Exeinfo PE**.

Malware_U3_W2_L1.exe							
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000



Purtroppo il malware ha al suo interno una protezione per nascondere il funzionamento delle varie sezioni, detto **Anti-UPX Unpacking**. Ogni sezione viene quindi nominata con la sigla **UPX** seguita da un numero (ad esempio 0,1,2...). Si tratta di un comune software per la compressione di tipo legittimo per ridurre la dimensione di un file. Spesso però capita che questi tools si occupino di offuscare e criptare il contenuto del malware per rendere più difficile l'analisi statica e il reverse engineering dello stesso.

Ci si accorge di ciò, oltre che dalla colonna **Name**, dove le varie sezioni vengono nominate a partire dalla nomenclatura **UPX0** a salire (**UPX1, UPX2...**) anche da ciò che compare alla colonna **sect. Stat** dopo aver premuto il pulsante **S-Stat**. Alcuni dei più popolari sono **UPX, ASPack, Themida, Exe Packer, MPRESS, Morphine**.

KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090
OFTs	FTs (IAT)	Hint	Name			
Dword	Dword	Word	szAnsi			
N/A	000060C8	0000	LoadLibraryA			
N/A	000060D6	0000	GetProcAddress			
N/A	000060E6	0000	VirtualProtect			
N/A	000060F6	0000	VirtualAlloc			
N/A	00006104	0000	VirtualFree			
N/A	00006112	0000	ExitProcess			

Un altro segnale del fatto che sia stato usato un metodo di offuscamento, sono alcune funzioni che vengono rilevate tra quelle presenti nelle librerie (ad esempio nella KERNEL32.dll) adoperate, dal software malevolo: **VirtualProtect** (modifica la protezione di un'area di pagine memoria di cui è stato eseguito il commit nello spazio degli indirizzi virtuali del processo che l'ha invocata), **GetProcAddress** (recupera l'indirizzo di una funzione esportata o variabile della libreria dinamica specificata), **LoadLibraryA** (si occupa di caricare in memoria il modulo specificato nello spazio indirizzi del processo che la ha chiamata).

Memory map

Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00010000				Map	RW	RW	
00020000	00010000				Map	RW	RW	
00030000	00001000				Priv	RW	RW	
00040000	00001000				Imag	R	RWE	
00089000	00007000				Priv	RW	RW	
0018D000	00001000				Priv	RW	RW	
0018E000	00002000				Priv	RW	RW	
00190000	00004000				Map	R	R	
001A0000	00001000				Priv	RW	RW	
001B0000	00001000				Priv	RW	RW	
001D0000	00006000				Priv	RW	RW	
00270000	00012000				Priv	RW	RW	
00370000	00067000				Map	R	R	
00400000	00001000	Malware_		PE header	Imag	R	RWE	\\Device\\HarddiskVolume2\\Windows\\System32\\local
00401000	00004000	Malware_	UPX0		Imag	R	RWE	
00405000	00001000	Malware_	UPX1	code	Imag	R	RWE	
00406000	00001000	Malware_	UPX2	data, import	Imag	R	RWE	
00410000	00000000				Map	R	R	
00590000	00003000				Map	R	R	
005B0000	00003000				Priv	RW	RW	
005C0000	00181000				Map	R	R	
00750000	0008A000				Map	R	R	
756E0000	00008000				Imag	R	RWE	
756F0000	00005C00				Imag	R	RWE	
75750000	00003F00				Imag	R	RWE	
75880000	00001000	CRVPTBAS		PE header	Imag	R	RWE	
75881000	00008000	CRVPTBAS	.text	code, import	Imag	R	RWE	
75889000	00001000	CRVPTBAS	.data		Imag	R	RWE	
7588A000	00001000	CRVPTBAS	.rsrc	resources	Imag	R	RWE	
7588B000	00001000	CRVPTBAS	.reloc	data, relocat	Imag	R	RWE	
75890000	00001000	SspiClli		PE header	Imag	R	RWE	
758A0000	00016000	SspiClli	.text	code, import	Imag	R	RWE	
758C0000	00001000	SspiClli	.data	data	Imag	RW	RWE	
758D0000	00001000	SspiClli	.rsrc	resources	Imag	R	RWE	
758E0000	00002000	SspiClli	.reloc	relocations	Imag	R	RWE	
75980000	00001000	GDI32		PE header	Imag	R	RWE	
75990000	00049000	GDI32	.text	code, import	Imag	R	RWE	

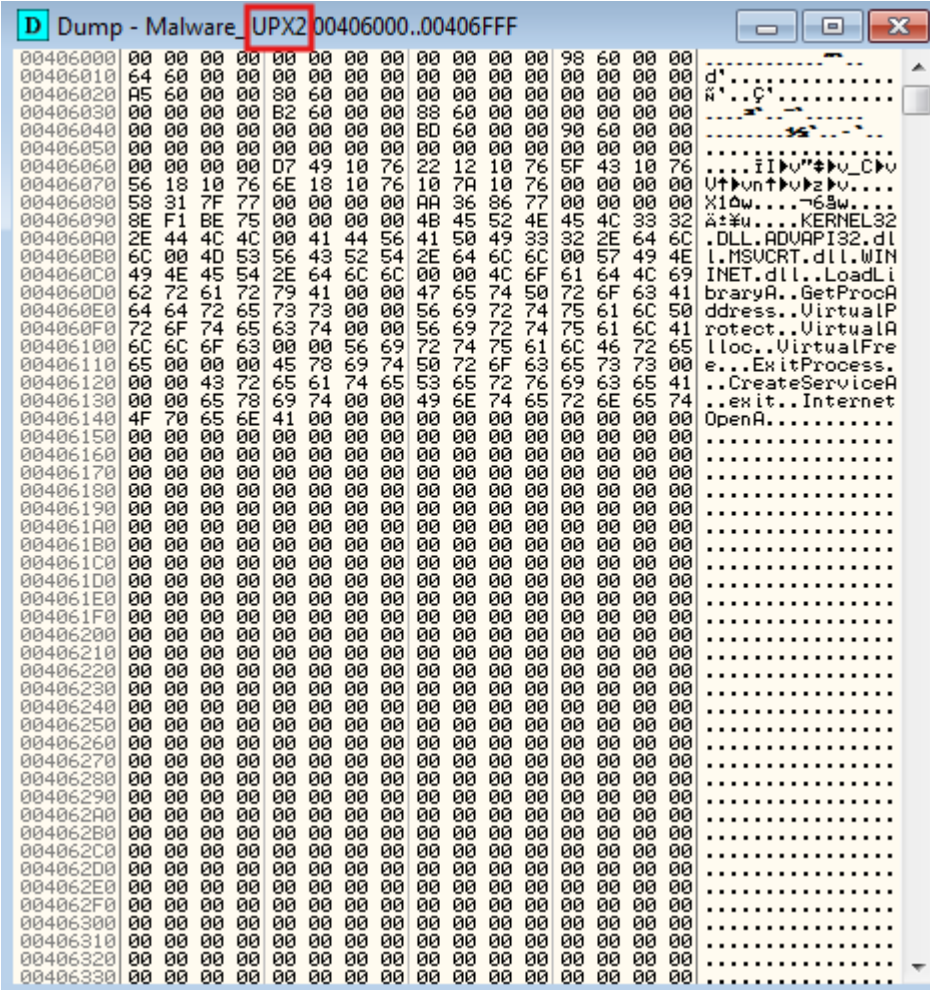
Dump - Malware UPX0.00401000..00404FFF

Name	Size	Type	Location
UPX0.00401000..00404FFF	0 bytes	Application extension	C:\Program Files\Windows Defender\Engine\Signature

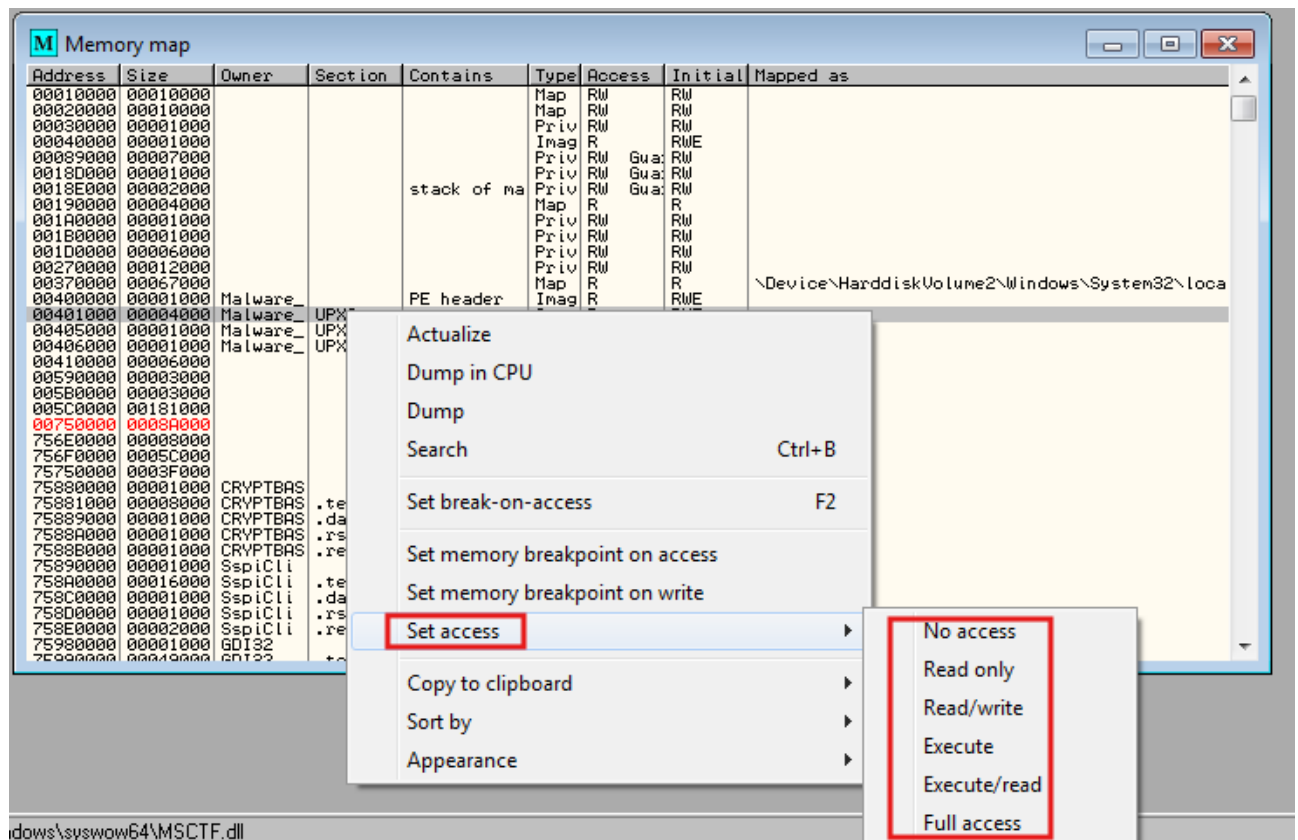
Facendo lo stesso sulla voce **UPX2** si ottiene invece questa finestra contenente delle istruzioni in assembly.

Address	Hex	Assembly	Comment
00405000	EF	OUT DX,EAX	I/O command
00405001	DD77 FF	FSAVE (108-BYTE) PTR DS:[EDI-1]	
00405004	83EC 10	SUB ESP,10	
00405007	8D4424 00	LEA EAX,DWORD PTR SS:[ESP]	
00405008	C703 10304000	MOV DWORD PTR DS:[EBX],Malware_.00403010	
00405011	50	PUSH EAX	
00405012	0808	OR BYTE PTR DS:[EAX],CL	
00405014	40	INC EAX	
00405015	1040 10	ADC BYTE PTR DS:[EAX+10],AL	
00405018	B7 FD	MOV BH,0FD	
0040501A	E9 DC0C0000	JMP Malware_.00405CFB	
0040501F	07	POP ES	Modification of segment register
00405020	10FF	ADC BH,BH	
00405022	15 0420156A	ADC EAX,6A152004	
00405027	01BD FDFB5DE8	ADD DWORD PTR SS:[EBP+E85DFBFD],EDI	
0040502D	0D 3C83C418	OR EAX,18C4833C	
00405032	C3	RETN	
00405033	90	NOP	
00405034	0081 EC00040F	ADD BYTE PTR DS:[ECX+F0400EC],AL	
0040503A	68 2830E9BE	PUSH BEE93028	
0040503F	E9 FE1C6801	JMP 01A86042	
00405044	001F	ADD BYTE PTR DS:[EDI],BL	
00405046	2920	SUB DWORD PTR DS:[EAX],ESP	
00405048	85C0	TEST EAX,EAX	
0040504A	74 08	JE SHORT Malware_.00405054	
0040504C	6A 0B	PUSH 0B	
0040504E	1C 67	SBB AL,67	
00405050	DF17	FIST WORD PTR DS:[EDI]	
00405052	AC	LODS BYTE PTR DS:[ESI]	
00405053	56	PUSH ESI	
00405054	1E	PUSH DS	
00405055	0F2C45 03	CUTTPS2PI MM0,DWORD PTR SS:[EBP+3]	
00405059	0B08	OR ECX,DWORD PTR DS:[EAX]	
0040505B	F66D EF	IMUL BYTE PTR SS:[EBP-11]	
0040505E	3E:8BF0	MOV ESI,EAX	Superfluous prefix
00405061	7E 1C	JLE SHORT Malware_.0040507F	
00405063	68 E8034450	PUSH 504403E8	
00405068	131465 76B7FD0B	ADC EDX,DWORD PTR DS:[BFDB776]	
0040506F	018D 4C242C05	ADD DWORD PTR SS:[EBP+52C244C],ECX	
00405075	51	PUSH ECX	
00405076	0A02	OR AL,BYTE PTR DS:[EDX]	
00405078	6A 10	PUSH 10	
0040507A	03D9	ADD EBX,ECX	
0040507C	6C	INS BYTE PTR ES:[EDI],DX	I/O command
0040507D	63EE	ARPL SI,BP	
0040507F	68 1C450456	PUSH 5604451C	
00405084	3B00	CMF EAX,DWORD PTR DS:[EAX]	
00405086	33D2	XOR EDX,EDX	
00405088	66:B7 EB	MOV BH,0EB	
0040508B	BE 14895424	MOV ESI,24548914	
00405090	04 29	ADD AL,29	
00405092	04 07	ADD AL,7	
00405094	0850 04	OR BYTE PTR DS:[EAX+4],DL	
00405097	1051 6C	ADC BYTE PTR DS:[ECX+6C],DL	
0040509A	49	DEC ECX	
0040509B	B6 DF	MOV DH,0DF	

Qui ciò che si ottiene aprendo la voce **UPX2.**

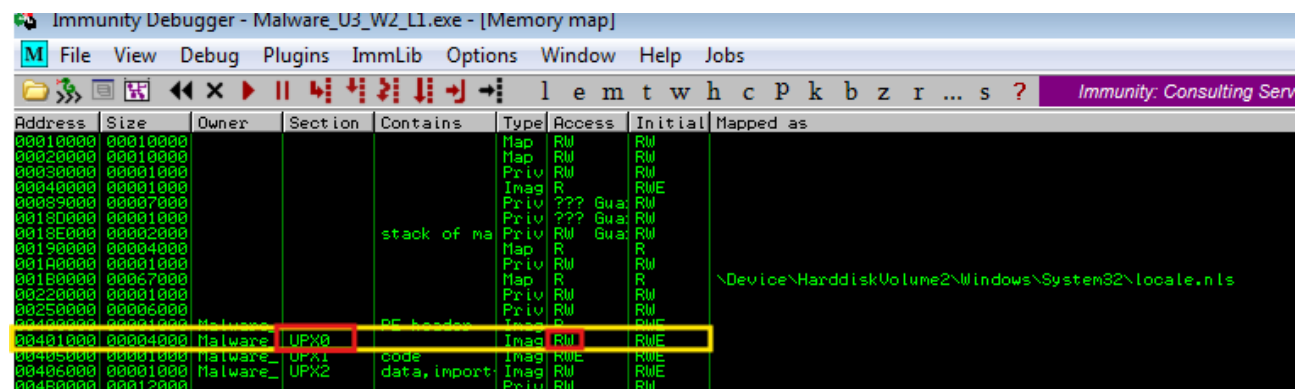


Si devono ora settare i permessi della sezione **UPX0** in sola lettura e scrittura.

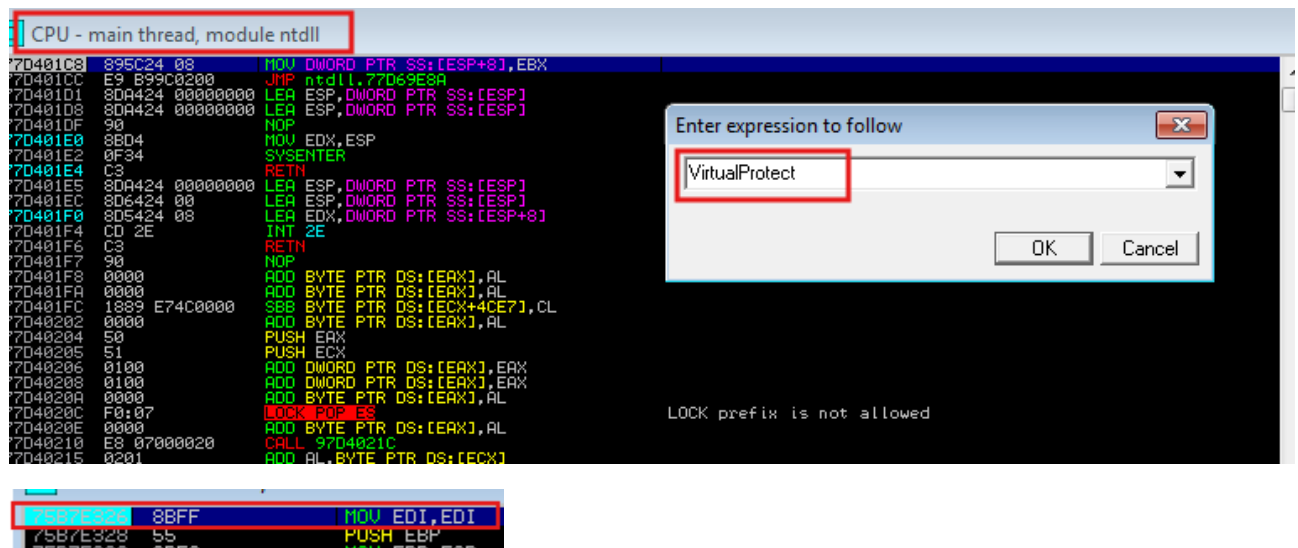


Per Effettuare la modifica dei permessi ho usato un altro tool chiamato **Immunity Debugger**, dato che il precedente non riusciva ad applicare le modifiche. Quindi ho impostato i permessi di lettura e scrittura alla sezione **UPX0**.

00401000	00004000	Malware_	UPX0		Image	RWE	RWE
00405000	00001000	Malware_	UPX1	code	Image	RWE	RWE
00406000	00001000	Malware_	UPX2	data, import	Image	RW	RWE



Nella finestra “CPU – main thread”, con **Ctrl+G** si apre questa finestra. Digitando il comando **VirtualProtect**, si raggiunge la funzione che ha questo nome, che viene evidenziata nella finestra che mostra l’esecuzione del codice. Serve inserire un **breakpoint** proprio in corrispondenza di questa funzione usando il tasto **F2**.



Purtroppo dopo vari tentativi e ricerche non sono riuscito a far funzionare correttamente il programma per estrarre le sezioni del malware.

Dopo aver continuato l'esecuzione del programma con il tasto **F9**, si è raggiunto il **breakpoint** in corrispondenza della funzione **VirtualProtect**.

The screenshot shows a debugger window titled "CPU - main thread, module KERNELBA". The assembly list displays instructions from address 75B7E328 to 75B7E39E. A red box highlights the instruction at address 75B7E328: `MOV EDI,EDI` with a comment `Malware_.00400000`. Below the assembly list, the register window shows `EDI=00400000 (Malware_.00400000)`. At the bottom, a status bar indicates a breakpoint at `KERNELBA.VirtualProtect`.

Address	Hex dump	ASCII
00400000	00 00 00 00 00 00 00 00
00400008	00 00 00 00 90 60 00 00
00400010	64 60 00 00 00 00 00 00	d'.....
00400018	00 00 00 00 00 00 00 00
00400020	A5 60 00 00 80 60 00 00	A'..Q'...
00400028	00 00 00 00 00 00 00 00
00400030	00 00 00 00 B2 60 00 00	...B'...

