

🛛 > Programa	ASPACK
>> Versión	2.12
> Herramientas	OLLYDBG 1.10 IMPORT REC. PEID
> Compilador	Borland Delphi Heuristic Mode
> Objetivos	DESEMPACAR EL EJECUTABLE
>> Cracker	AGUML

Antes de nada conozcamos a nuestro enemigo. Abrimos PEID y miramos a ver con que esta empacado y:

🕮 PEiD v0.9				
File: C:\Archiv	os de programa\ASPack\ASPac	:k.exe		
Entrypoint: 00	001000	EP Section:		
File Offset: 00	000400	First Bytes: 68,01,	,80,46	
Linker Info: 2.2	25	Subsystem: Win32	GUI	GenOEP 🛛 🔀
ASProtect 1.22	- 1.23 Beta 21 -> Alexey Solo	dovnikov		Found OEP: 0044289C
Multi Scan	Task Viewer Options	About	E <u>×</u> it ->	Aceptar

Ufff, con lo poco que me gusta ese packer, jejeje. Bueno pues carguémoslo en Olly a ver que pasa:

💥 - [CP	U - main th	read, n	nodule A	SPack]													
C File	View Debug	Plugins	Options	Window	Help	1											
🗁 📢 X	< > 	4 +	}:	→] →	: I	LE	Μ	TW	7	H C	1	K	B	R	S	i	
00401000 00401005 0040100A	68 018046 E8 010000 C3	.00 P	USH 46800 ALL 00401 ETN	01 .008						ASPa	ick.0	040	1008	3	_		
00401008 0040100C 00401012 00401014	04 84 3D 621108	E04E C 89 C	MP EDX,DW DD AL,84 MP EAX,89	0RD PTR 081162	DS:CE	EDX+4I	EE024	1773									
00401019 0040101F 00401020 00401022	1905 9080 45 ~ E1 09 2301	19438 S I A	BB DWORD NC EBP <mark>OOPDE SHC</mark> ND EAX,DV	PTR DS:I I <mark>RT 0040</mark> IORD PTR	138A48 1028 DS:[E	8090), ECX]	,EAX			ASPa	ick.0	040	102E	3			
00401024 00401027 00401029 0040102F	2872 48 7A 42 00A8 7248 05 277C01	404A A AC A	UB BYTE F <mark>PE SHORT</mark> DD BYTE F DD EAX,AC	'TR DS:[[<mark>0040106[</mark> 'TR DS:[[:017C27	EDX+48 EAX+4P	8],DH A4048	72],(ж		ASPa	ick.0	1040	106E	3			
00401034 00401037 00401038 00401038	0247 81 53 B3 A6 52	A P M	DD AL,BY1 USH EBX OV BL,ØA6 USH EDX	E PTR D	6:[ED]	I-7F]											
0040103B 0040103C 00401041 00401042	55 685CD5 F2 55 60	EA I P	ÚSH EBP MUL EBX,C USH EBP NS DWORD	WORD PTF	R SS:[CEBP+I	EDX*8	3-Е],	-16	5	c.0000	and					
00401043 00401044 00401045	6D 5A D97D 75	Î P F	NS DWORD OP EDX STCW WORD	PTR ES:	EDII;	, DX +751_				Î⁄Ŏ	COMM	and					
00401048 0040104B 0040104C 00401052	895H BC 93 8121 1F40 41	8088 A	CHG EAX,E ND DWORD NC ECX	PTR DS: BX PTR DS:	(ECX),	44J,E ,8880	87 401F										
00401053 00401058 0040105B 0040105D	15 041F49 C562 02 1009 4E	1E A L A D	DC EAX,1E DS ESP,F⊍ DC BYTE F EC ESI	:491F04 IORD PTR 'TR DS:[[DS:[E ECX],C	EDX+2 CL	נ			Modi	fica	tio	n of	segm(ent i	regis	ter
0040105E 00401060 00401062	- 73 90 3822 F9	U C S	NB SHORT MP AH, BY1 TC	00400FF(E PTR D	a:CED>	נא				ASPa	ick.0	1040	ØFFØ	9			
00401063 00401064 00401066 00401067	50 05 BE 6E 50	A O P	AD ØBE UTS DX,BY OP EBP	TE PTR ES	ES:[ED	,UX DI]				1/0	COMM	iand iand					
00401068 00401069 00401068 00401068	AD DF37 3C C7 × 77 7F	LFC	ODS DWORE BSTP TBY1 MP AL,0C7 A SHORT 0) PTR DS: E PTR DS	:[ESI] S:[ED]] I]				ASP =	ick - P	1949	10FF	-			
0040106F	11DD	A	DC EBP,EE	X							00	.540	1000	-			
00468001	=HSPack.0046	8001															
0.445.5.5.5			Loca			_			_		_		001:	PEEC4	708	16ED7	

Ahora usaremos el método que mas he visto y que a mi me ha dado resultado para llegar al OEP. Simplemente nos vamos a Options->Debugging Options o si lo prefieren Alt + O y dan en la pestaña Exceptions y dejan marcada solo la primera opción que hay:

E Debugging options
Commands Disasm CPU Registers Stack Analysis 1 Analysis 2 Analysis 3
Security Debug Events Exceptions Trace SFX Strings Addresses
☑ Ignore memory access violations in KERNEL32
Ignore (pass to program) following exceptions:
🔲 INT3 breaks
🔲 Single-step break
Memory access violation
Integer division by 0
Invalid or privileged instruction
All FPU exceptions
Ignore also following custom exceptions or ranges:
Add last exception
Add range
Delete selection
OK Undo Cancel

Le dan a OK y ahora simplemente le dan a F9 y empiezan a pasar las excepciones con Shift +F7 y F9 y teniendo mucho cuidado al contar las excepciones hasta que el programa arranque (en mi caso fueron 26 excepciones). Ahora reiniciamos Olly con Ctrl. + F2 y hacemos lo mismo pero esta vez nos pararemos en la ultima excepción y le damos a Shift + F7 solo para pasarla.

Ahora pulsamos Alt + M para sacar la ventana Memory Map y marcamos la sección .code del ejecutable y le ponemos un BP Memory on Access haciendo clic derecho sobre ella como se muestra en la imagen:

F3 51		PUSH ECX							
Memo	ry map								×
Address	Size	Owner	Section	Contains	Туре	Access	Initial	Mapped as	
				stack of ma	Privo por privo privo privo privo privo pri	IJIJZZZZZZIJIJIJIJZZZZZZZZZZZZZZZZZZZZZZZZZ		\Device\HarddiskVolume1\WIN \Device\HarddiskVolume1\WIN \Device\HarddiskVolume1\WIN \Device\HarddiskVolume1\WIN \Device\HarddiskVolume1\WIN	D(D(D(D(
00400000 00400000 00401000 00443000 00445000 00448000 400448000 400448000 400448000 400448000 400448000 400448000 400448000 500448000 500448000 500468000 500468000 50047000 60047000 60047000 60048000		ASPack ASPack ASPack ASPack ASPack ASPack ASPack ASPack ASPack ASPack ASPack ASPack ASPack	.rsrc .ass .adata	PE header code data resources imports,rel	Imag I I I I I I I I I I I I I	<u>R</u> Actualize View in Dis Dump in Cl Dump Search Set break-	assembler PU -on-access	Ctrl+B	
74 880424 77 88E5 79 5D 78 90 78 90 70 8DA424 83 8D49 00 86 90 86 90 88 90	0000000 3	MOU EAX,D MOU ESP,E POP EBP RETN NOP LEA ESP,D LEA ECX,D NOP NOP	WORD PTR BP WORD PTR WORD PTR	SS:[ESP] SS:[ESP] DS:[ECX]		Set memor Set memor Set access Conditiona	ry breakpo ry breakpo s al Branch L inboard	oint on access oint on write ogger	
<u>ee;100105e7</u> /	13-001050	70 1				Sort by			

Y ahora demos a F9 y...

🔆 - [CP	U - main th	read, n	nodule AS	SPack]												
C File	View Debug	Plugins	Options	Window	Help											
🔁 📢 X	× ►	4 +	∑ I:	→	L	EM	T	N H	C /	KB	R.	•• S		?		
	55 38EC 38C4 F4 E3 4008FC E3 0621FC E3 0624FC E3 0624FC E3 0624FC E3 0740FE E3 0827FC E3 0827FC E3 0827FC E3 0804FE E3 6394FE E3 6394FE E3 6394FE E3 6394FE E3 6394FE E3 6444FFF E3 0210FE E3 0847FE E3 0210FE E3 0210FE E3 0210FE E3 0210FE E3 0210FE E3 0210FE E3 0210FE E3 0210FC 50 C3 0000 FFFF FFFF 06 0000 00041 53 50 C3 00000 0000 0000 0000 0000 0000 0000		USH EBP OV EBP,ES DD ESP,-0 ALL 00407 ALL 00407 ALL 00407 ALL 00407 ALL 00407 ALL 00407 ALL 00421 ALL 00421 ALL 00422 ALL 00422 ALL 00422 ALL 00422 ALL 00422 ALL 00422 ALL 00422 ALL 00423 ALL 00428 ALL 00488 ALL 0048	P C 3F4 9B8 9D14 F8C 978 FC8 5C2 FC8 5C2 FC8 2BC 2BC 2BC 2BC 2BC 2BC 2BC 2BC 2BC 2BC	DS:[44 DS:[44 DS:[44 DS:[44 DS:[44 CAX],AL CAX,AL C	45630] 45630] 45630] - 1, AL 3P			ASPack. ASPack. ASPack. ASPack. ASPack. ASPack. ASPack. ASPack. ASPack. ASPack. ASPack. ASPack. ASPack. ASPack. ASPack. ASPack. ASPack. ASPack. Unknown	004033 004049 004070 0040EF 00410F 004223 004223 004223 004223 004223 004223 004223 004239 004239 004239 004236 004236 004236 004236 004236 004236	F4 B14 B178 C550 C550 C550 C550 C550 C550 C550 C55					ΕΠΑΠΑΠΑΤΑΤΑΤΑ
Address	Hex dump		ASC	11						N 00	012FFC4	7C81	6FD7 RE	TURN to	kernel:	32.7

Ya estamos en el OEP y tiene buena pinta porque parece ser que no hay Stolen Bytes así que sigamos.

Para encontrar la IAT simplemente ponte encima de la primera CALL y das Intro a ver a donde nos lleva:

🔆 - [СР	U - main thread,	module ASPack]		
C File	/iew Debug Plugin	s Options Window Help		
🔁 📢 >	< > 4	H } ↓ → H E M T W	7 H C / K B R S 🗄 🏋 ?	<u>A</u>
004033F4	E8 B3FFFFFF	CALL 004033AC	ASPack.004033AC	🔨 Regis
004033F9 004033FB	6A 00 E8 DØDEFFFF	PUSH 0 CALL 004012D0	ASPack.004012D0	EAX
00403400	8905 14504400	MOV DWORD PTR DS:[445014],EAX	05Pack 00401288	EDX 2
0040340B	8905 10504400	MOV DWORD PTR DS: [44501C], EAX	H0Fack.00401200	EBX 7
00403411 0040341B	C705 18504400 B8 4C314000	MOV DWORD PIR DS:L4450181,0H MOV EAX,40314C		EBP 6
00403420 00403421	C3 8D40 00	RETN LEA EAX.DWORD PTR DS:[EAX]		EDI
00403424	53 8330 04534400	PUSH EBX CMP_DWORD_PTR_DS+[4453D4]_0		EIP 🤅
0040342C	 7D 0A 7D 0A 	USE SHORT 00403438	ASPack.00403438	C 0 P 1
0040342E 00403433	E8 D9100000	CALL 00404511	ASPack.00404511	A 0
00403438 0040343D	68 08000000 6A 40	PUSH 8 PUSH 40		SØ
0040343F	E8 DCDEFFFF	CALL 00401320 MOU ERY EOY	ASPack.00401320	00
00403446	85DB	TEST EBX, EBX		0.0
00403448 0040344A	× 75 00 B8 E2000000	MOV EAX,0E2	нъмаск.00403456	STO 4
0040344F 00403454	E8 BD100000 V EB 0C	CALL 00404511 JMP SHORT 00403462	ASPack.00404511 ASPack.00403462	STI e
00403456	53 01 D4534409	PUSH EBX MOU FAX DWORD PTR DS+[4453D4]		S12 e ST3 e
00403450	50	PUSH EAX	000	ST4 e ST5 e
0040345D 00403462	E8 86DEFFFF 891D 90544400	MOV DWORD PTR DS:[445490],EBX	H5Mack.004012E8	ST6 e
00403468 00403469	5B C3	POP EBX RETN		517 6
0040346A	88C0 8000 34504400	MOV EAX,EAX MOU CL_BYTE PTR DS+[445034]		FST & FCW &
00403472	8805 D4534400	MOV EAX, DWORD PTR DS: [4453D4]		
00403478 0040347A	× 75 28	UNZ SHORT 004034A4	ASPack.004034A4	
0040347C 00403483	64:8B15 2C0000 8B0482	MOV EDX,DWORD PTR FS:[2C] MOV EAX.DWORD PTR DS:[EDX+EAX*4]		
00403486	C3 F8 98FFFFFF	RETN COLL 00403424	05Pack 00403424	
0040348C	8805 D4534400	MOV EAX, DWORD PTR DS:[4453D4]	HOI BOX . 00103424	
00403492	E8 48DEFFFF	CALL 004012E0	ASPack.004012E0	
00403498 00403498	85C0 v 74 01	TEST EAX,EAX JE SHORT 0040349D	ASPack.0040349D	
00403490	C3 0005 00544400	RETN MOULEON DWORD PTP DS. FAAEA981		*
004033AC:	ASPack.004033AC			
Address	Hex dump	ASCII	0012FFC4 7C816FD7 RETURN	to kernel32.7C81

No se ve nada interesante pero como siempre se llama a alguna API muy cerca del OEP, pues probare a ver que hay dentro de esas CALLs.

En la primera no hay tampoco nada interesante pero en la segunda salimos aquí:

🗶 - [СР	U - main th	nread, n	nodule A	SPack]									
C File	/iew Debug	Plugins	Options	Window	Help								
	< <u> </u>	4	2 : 1:	→	L	E M T	r w H	IC/K	B R	S 🗄	?		.
004012D0	- FF25 5C61 8BC0	14400 <mark>J</mark> M	<mark>MP DWORD</mark> DV EAX,EA	PTR DS:D	4461503							^	Regis
004012D8 004012DE	- FF25 5861 8BC0	14400 <mark>J</mark> M	M <mark>P DWORD</mark> DV EAX,EA	PTR DS:D	4461583								ECX 7
004012E0 004012E6	- FF25 5461 8BC0	14400 <mark>J</mark>	MP DWORD DV EAX,EA	PTR DS:D	4461543								EBX 7
004012E8 004012EE	- FF25 506) 8BC0 - FF25 4041	14400 <mark>0</mark> 14400 M	NP DWORD DV EAX,EA	NTR DS:L	4461503								EBP ESI 7
004012F6	- FF25 4001 8BC0 - FF25 C441	14400 0 M	DV EAX,EA	IX IX PTP Deve	4461403			01000+92 80	ic011ccStr	inglen			EDI 7
004012FE	8BC0 - FE25 C061	14400 M	DV EAX,EA	IX PTR DS: C	4461001			oleaut32.Su	usStrinal e	ngeen N			<u> </u>
00401306 00401308	8BC0 - FF25 BC61	14400 J	DV EAX,EA	IX PTR DS: D	4461BC3			oleaut32.Va	ariantClea	c			P 1 A 0
0040130E 00401310	8BC0 - FF25 B861	14400 <mark>J</mark>	OV EAX,EA MP DWORD	X PTR DS: D	4461B8]			oleaut32.Va	ariantCopy	Ind			5 0 T 0
00401316 00401318	- FF25 B461	14400 <mark>J</mark> I	DV EAX,EA <mark>MP DWORD</mark>	IX PTR DS: D	4461843			oleaut32.Va	ariantChan	geTypeEx			ĎЙ
0040131E 00401320	- FF25 4861	14400 <mark>J</mark>	DV EHX,EH MP DWORD	NA	4461483								EFL 6
00401326	- FF25 4461	14400 <mark>J</mark>	MP DWORD	PTR DS: C	4461443								STØ e ST1 e
00401320	- FF25 4061	14400 <mark>J</mark>	MP DWORD	PTR DS:D	4461403								ST2 e ST3 e
00401338 0040133E	- FF25 3C61 8BC0	14400 <mark>ji</mark> M	M <mark>P DWORD</mark> DV EAX.EA	PTR DS:D	4461303								ST4 e ST5 e
00401340 00401346	- FF25 3861 8BC0	14400 <mark>J</mark> M	<mark>MP DWOŔD</mark> DV EAX,EA	PTR DS: D	4461383								ST7 e
00401348 0040134E	- FF25 3461 8BC0	14400 <mark>J</mark> M	M <mark>P DWORD</mark> DV EAX,EA	PTR DS:D	4461343								FST 0
00401350	- FF25 3061 8BC0	14400 <mark>J</mark> M	MP DWORD DV EAX,EA	PTR DS:D	4461303								
00401358 0040135E	- FF25 2061 8BC0	14400 <mark>0</mark> M D	DV EAX,EA	IX	4461203								
00401361 00401361	56 BE 305444	400 M	USH ESI NU FSI.44	5430									
00401367 0040136A	833E 00 ~ 75 3A		MP DWORD	PTR DS: 0 00401386	ESI],Ø			ASPack.0040	313A6				
0040136C 00401371	68 440600 6A 00	200 PI	USH 644 USH 0										
00401373 00401378	E8 A8FFFF 8BC8	FFF C	ALL 00401 DV ECX,EA	<mark>.320</mark> X				ASPack.0040	31320				
0040137A	8509 75 05		EST ECX,E N7 CLODT	CX 00401000				098-04 0040	31000			*	4
03.10044	51003-009EC:												
Address	Hex dump		[esc						0012FFC4	7C816FD7	RETURN t	o kernel3	2.7081
00443000 00443008	02 00 8B C0 98 3D 40 00	0 00 8D 0 A8 20	40 00 8. ï 40 00 ÿ=0	∟.i@. .¿@.					0012FFC8 0012FFCC	7C923E6F 7C923E62	RETURN t RETURN t	o ntdll.70 o ntdll.70	0923E61

Bueno pues ya dimos con la zona caliente para dar con la IAT. Ahora nos ponemos encima de cualquiera de esos saltos incondicionales que empiezan con FF25 y nos vamos al panel que es la parte de debajo de la ventana Disassembler y hacemos clic derecho sobre el valor que se ve y elegimos Follow Address in Dump:

🔆 - [СР	U - mai	n thread,	module AS	SPack]									
C File	View Del	bug Plugin:	s Options	Window	Help								
- • • >	× ►	II 4 +	: <u>}</u> !:	→ =		E M	TWH	IC/	K	B R	S	≣ <mark>∷</mark> ?	
004012D0 004012D6	- FF25 8BC0	5C614400	<mark>JMP DWORD</mark> MOV EAX,EA	PTR DS: X	E44615C]							
004012D8	- FF25 8BC0	58614400	<mark>JMP DWORD</mark> MOV EAX,EA	PTR DS: X	[446158]							
004012E0 004012E6	- FF25 8BC0	54614400	JMP DWORD MOV EAX.EA	PTR DS: X	[446154]]							
004012E8 004012EE	- FF25 8ВС0	50614400	JMP DWORD MOV EAX.EA	PTR DS:	[446150]	1							
004012F0	- FF25 8800	4C614400	JMP DWORD MOU FAX.FA	PTR DS:	E44614C]							
004012F8	- FF25	C4614400	JMP DWORD	PTR DS:	E4461C4	1		oleaut3	32.Sy	sAllocStr	ingLen		
00401300	- FF25	C0614400	UMP DWORD	ÊTR DS:	[4461C0]	1		oleaut3	32.Sy	sStringLe	n		
00401308	- FF25	BC614400	JMP DWORD	ÊTR DS:	E4461BC	1		oleaut3	32.Va	riantClea	r		
00401310	- FF25	B8614400	JMP DWORD	ÊTR DS:	E4461B8	1		oleaut3	82.Va	riantCopy	Ind		
00401316	- FF25	B4614400	JMP DWORD	ÊTR DS:	E4461B4	1		oleaut3	82.Va	riantChan	geTypeEx	:	
0040131E	- FF25	48614400	MOV EHX,EH	A PTR DS:	[446148]	1							
00401326	- FF25	44614400	MUV EHX,EH JMP DWORD	X PTR DS:	E446144	1							
0040132E	- FF25	40614400	MOV EAX,EA <mark>JMP DWORD</mark>	X PTR DS:	[446140]	1							
00401336	- 88C0	3C614400	MOV EAX,EA <mark>JMP DWORD</mark>	X PTR DS:	E44613C	1							
0040133E	- 88C0	38614400	MOV EAX,EA JMP DWORD	X PTR DS:	E446138	3							
00401346 00401348	- 88C0	34614400	MOV EAX,EA	X PTR DS:	[446134]	1							
0040134E	- 5525	30614400	MOV EAX,EA	X PTR DS:	E446130	1							
00401356	8BC0	20614400	MOV EAX,EA	X PTR DS:	E44612C	1							
0040135E	88C0		MOV EAX,EA	X		•							
00401361	56 20	E44400	PUSH ESI	EASC									
00401367	833E	00	CMP DWORD	PTR DS:	[ESI],0			OCPack	0040	1004			
0040136C	68 44	060000	PUSH 644	004015H	•			Horack.	0040	1940			
00401371	E8 A8	FFFFF	CALL 00401	320				ASPack.	0040	1320			
00401378 0040137A	8808		TEST ECX,EH	х СХ	_			000		4000			
DS: [0044	61503=0			1	-			LINE SOK		1000			
		Copy pan Modify da	e to clipboard Es	'									
Address	Hex du	Eollow add	ta tress in Dumr				ASCII		~	0012FFC4	7C816FI		to kernel
00443000 00443010	02 00	Eollow val	ue in Dump	0	0 A8 20 0 32 13	40 00 88 C0	e.ï⊾.i@. 0″@.ñ%@.	ÿ=@.¿ @. 2∀ï⊦2‼ïч		0012FFC8	7C923E6	S2 RETURN	to ntall.
00443020 00443030	52 75 -	1 01011 70	com o amp		F 72 20	20 20 45 72	Runtime at 000	error 00000.Er		0012FFD0	80543FF	-D	
00443040 00443050	72 6F 20 20	Appearan	ce	• 22	0 20 20	20 20 20 20	ror.			0012FFD8	8648980		0511
00443060 00443070	20 20 2	0 20 20 20 0 20 20 20	20 20 20 20 20	20 20 2 20 20 2	0 20 20	20 20 20 20				0012FFE0 0012FFE4	7C839AF	-F End of 18 SE han	dler
00443080	20 20 2	0 20 00 0A 0 00 00 0A	88 C0 00 00 00 00	00 00 0 00 00 8	0 88 30	44 00 00 40	ï ^L	ē0D.		0012FFE8 0012FFEC	70816FE	20 kernel 30	32.70816FE
004430A0	00 00 0		00 00 00	00 00 0	0 01 00	00 00	н			0012FFF0 0012FFF4	000000	30	
004430C0	03 00 0	0 00 80 FF	00 00 04	00 00 0	0 88 FF	00 00	.			0012FFF8	0013000	00 ASCII	"h#"

Y ya estamos en la IAT aunque tiene muy mala pinta y esta redireccionado casi todo hacia el Asprotect pero vamos a repararla. Lo primero es ver donde empieza y donde termina y para ello subamos buscando a ver si vemos una zona de 00000000 o vemos direcciones seguidas que no tengan referencias (para saber si un dword tiene referencias lo marcamos y hacemos Ctrl. + R y si sale la lista vacía es porque no es un dato valido de nuestra IAT y sobra así que si no se ve la zona de 00000000 tendríamos que buscar el inicio de nuestra IAT mirando si los dwords tienen referencias o no. En este caso tenemos suerte y Podemos ver el comienzo de la IAT en 446128 :

		_
Address	Hex dump ASCII	~
00446050 00446070 00446070 00446090 00446090 00446090 00446080 00446080 00446080 00446080 00446080 00446080 00446080 00446100 00446120	00 00 <td< th=""><th></th></td<>	
00446130 00446140 00446150 00446160 00446170 00446170 00446180 00446190 00446180 00446180 00446180	74 44 A3 00 80 44 A3 00 98 44 A3 00 tbi.cDi.cDi.iDi.jDi. A4 44 A3 00 80 44 A3 00 FDi.cDi.iDi.jDi. A4 44 A3 00 80 44 A3 00 FDi.cDi.iDi.jDi. E4 44 A3 00 FC 44 A3 00 FDi.cDi.iDi.jDi. E4 44 A3 00 FC 44 A3 00 FDi.cDi.iDi.jDi. E4 44 A3 00 FC 44 A3 00 FDi.cDi.iDi.jDi. E4 44 A3 00 FC 44 A3 00 BE (4) ADI.iDi.iDi.iDi.iDi.iDi.iDi.iDi.iDi.iDi.i	*

Y en 4466A0 podemos ver también claramente el final:

Address	Hex dump ASCII .	 00.
004465D0 004465F0 004466F0 00446610 00446610 00446620 00446620 00446620 00446630 00446640 00446650 00446660 00446660 00446660	DC 4E A3 00 E8 4E A3 00 F4 4E A3 00 08 4F A3 00 Nù ⊧Nù Nù ⊡Où 14 4F A3 00 20 4F A3 00 2C 4F A3 00 38 4F A3 00 90 00 Où. Où, Où 80ù. 74 4F A3 00 80 4F A3 00 5C 4F A3 00 68 4F A3 00 DOù.POù.Où.Où. 74 4F A3 00 80 4F A3 00 8C 4F A3 00 98 4F A3 00 DOù.POù.Où.Où. 74 4F A3 00 80 4F A3 00 8C 4F A3 00 98 4F A3 00 toù.Coù.Où. 60 00 00 80 4F A3 00 8C 4F A3 00 00 E0 67 27 F KOÙ. 00 00 00 8C 4F A3 00 C8 4F A3 00 04 4F A3 00 V. 00 00 00 8C 4F A3 00 28 50 A3 00 34 50 A3 00 VOù.Où. 10 50 A3 00 1C 50 A3 00 28 50 A3 00 34 50 A3 00 VPÙ.LPù.(Pù.4Pù. 40 50 A3 00 1C 50 A3 00 28 50 A3 00 31 50 A3 00 VPÙ.LPù 40 50 A3 00 4C 50 A3 00 88 4F A3 00 00 00 00 1E 31 36 76 00 00 00 00 73 33 50 77 DA F6 4C 77 2C D0 4C 77 s3Pwr+Lw,šLw D0 D5 4D 77 00 00 00 00 80 48 0F 77 4C 4D 19 77. 8C 82 19 77 4E 77 19 77 A3 30 19 77 4C 4D 19 77. 4C 4D 19 77 4C 4D	
004466A0 004466B0 004466D0 004466D0 004466E0 004466F0 004466F0 00446710 00446710 00446710 00446720 00446720	00 00 <td< th=""><th>♥</th></td<>	♥

Entonces tenemos que:

El OEP es 44289C

El inicio de la IAT esta en 446128

El fin de la IAT esta en 4466A0

Y su tamaño es el resultado de restarle al fin de la IAT el inicio de la IAT así que: Tamaño de la IAT = 4466A0 - 446128= 578

A LA CAZA DEL CALL SEMI-MAGICO

Ahora reiniciemos y vayamos a 44612C que es el principio de las direcciones que debe escribir en nuestra IAT y pongamos un Memory Breakpoint on Write:





Y le damos a F9 y empezamos a pasar las excepciones otra vez igual que antes pero esta vez hay que tener mucho cuidado porque hay que contar muy bien las excepciones ya que te puedes equivocar y contar la parada en el BPM como si fuera una excepción.

La primera vez que para por nuestro BPM es en :

Esta no nos interesa así que sigamos y recordad que esta vez que paro no la debéis contar ya que no fue una excepciona si que sigamos:

× ► 🛚 🔄	+: }: ↓: →: LEMTWHC/ K	B R S ☷ # ?	<u>8</u>
3308 8450 FF 88C8 8085 FFFEFFFF 8806 8905 FFFEFFFF 8906 8803 89035 FFFEFFFF 8085 FFFEFFFF 8085 FFFEFFFF 8085 FFFEFFFF 8815 8902 8985 801 74 05 8378 01 74 05 8378 01 74 05 8378 04 75 37 8406 8345 FF 805 FFFEFFFF 805 FFFEFFFF 805 FFFEFFFF 805 FFFEFFFF 805 FFFEFFFF 805 FFFEFFFF 805 FFFEFFFF 805 FFEFFFF 805 FFEFFFF	XDR EBX,EBX MOU EL,BYTE PTR SS:LEBP-11 MOU ELX,EX LEA EAX,DWORD PTR SS:LEBP-1011 MOU EDX,SEX CALL 009E4508 MOU ECX,9F3966 MOU ECX,9F3966 MOU ECX,9F3966 MOU ECX,9F3966 MOU ECX,9F3966 MOU ECX,9F3966 CALL 009EC490 LEA ESI,DWORD PTR SS:LEBP-1011 PUSH ESI MOU EAX,DWORD PTR SS:LEBP+C1 PUSH ESI MOU EAX,DWORD PTR DS:LED11 MOU E0X,DWORD PTR DS:LED11 MOU AL,BYTE PTR DS:LES11 MOU AL,BYTE PTR SS:LEBP-11,AL INC ESI XOR ECX,ECX MOU CL,BYTE PTR SS:LEBP-1011 MOU ECX,9F39AC XOR EDX,EDX MOU DL,BYTE PTR SS:LEBP-1011 CALL 009EC490 PDSH 04 MOU ECX,9F39AC XOR EDX,EDX MOU DL,BYTE PTR SS:LEBP-1011 CALL 009EC490 PDS PTR SS:LEBP-1011 CALL 009EC490 PDS PTR SS:LEBP-1011 CALL 009EC490 PDS PTR SS:LEBP-1011 CALL 009EC490 PDS PTR SS:LEBP-1011 CALL 009EC490 PTR SS:LEBP-1011 PTR SS:LEBP-1011 PTR SS:LEBP-1011 PTR SS:LEBP-1011 PTR SS:LEBP-1011 PTR SS:LEBP PTR SS		Registers (FPU) EAX 00034460 EAX 00030460 ECX 0000000 EDX 0000000 EDX 0000016 ESP 0012FF12C EBY 0012FF12C EBY 0012FF28 EDI 0012FF28 ASCII "DeleteCriticalSection" EDI 0012FF30 EDI 0012FF57 C 0 ES 0023 32bit 0(FFFFFFFF) A 0 S 0023 32bit 0(FFFFFFFF) A 0 SS 0023 32bit 0(FFFFFFFF) A 0 SS 0023 32bit 0(FFFFFFFFF) Z 0 DS 0023 32bit 0(FFFFFFFFF) S 0 FS 0088 32bit 0(FFFFFFFFF) Z 0 DS 0023 32bit 0(FFFFFFFFF) S 0 FS 0088 32bit 0(FFFFFFFFF) Z 0 DS 0023 32bit 0(FFFFFFFFF) S 0 FS 0088 32bit 7FFDE000(FFF) T 0 6S 0000 NULL D D 0 LastErr ERROR_SUCCESS (00000000) EFL 00010202 (NO,NE,NE,A,NS,PO,GE,G) ST0 empty -UNORM BA4C 0000003 000000000 ST3 empty +UNORM BA4C 00000003 0000000000000000000000000000
Have during		0012EE1C 0044612C 05Pack 0044612C	
Res Jump 00 0	Image: Contract of the contract	0012FE20 00002001 0012FE24 0012FE30 0012FE28 44532117 0012FE30 69724365 0012FE30 69724365 0012FE30 69724365 0012FE30 69724365 0012FE30 69724365 0012FE30 669724365 0012FE30 60000000 0012FE30 00000000 0012FE40 00000000 0012FE40 00000000 0012FE40 00000000 0012FE40 00000000 0012FE40 00000000 0012FE50 00000000 0012FE60 00000000	

Esta si es importante ya que esta justo después del salto semi-mágico que nos arreglara casi toda la IAT.

El salto que tendremos que nopear será el que esta encima de donde nos detuvimos así que apuntemos la dirección donde esta ese CALL y volvamos a reiniciar con Ctrl. + F2. Le damos a F9, le damos a Ctrl. + G y metemos la dirección de donde estaba la CALL que en mi caso esta en 009EF9C1 y le damos a OK y nos llevara a donde esta la CALL. Le ponemos un BP y pulsamos Alt + O y marcamos todas opciones de la pestaña Exceptions excepto la última:

🗄 Debugging options 🛛 🛛 🔀							
Commands Disasm CPU Registers Stack Ar	nalysis 1 🛛 Analysis 2 🗍 Analysis 3 🗍						
Security Debug Events Exceptions Trace	SFX Strings Addresses						
✓ Ignore memory access violations in KERNEL32							
Ignore (pass to program) following exceptions:							
🔽 INT3 breaks							
🔽 Single-step break							
Memory access violation							
Integer division by 0							
Invalid or privileged instruction							
All FPU exceptions							
Ignore also following custom exceptions or ranges:							
	Add last exception						
	Add range						
~	Delete selection						
	OK Undo Cancel						

Damos a OK y ahora Shift + F7 y F9 y llegamos al BP.

DESEMPACAR ASPACK 2.12 COMPRIMIDO CON ASPROTECT 1.23

26-06-2008

_ <u></u>			
009EF9B7 009EF9B8	56 8845 ØC	PUSH ESI	Registers (FPU) < < <
009EF9BB 009EF9BC	50 F8 1BECEEEE	PUSH EAX	ECX 0012FE0C
	E8 7EFEFFFF	CALL 009EF844	EDX 0000000 EBX 00000016
009EF9C8	8902	MOV DWORD PTR DS: [EDX], EAX	ESP 0012FE1C EBP 0012FF2C
009EF9CH	× EB 7B 83FB 01	CMP EBX,1	ESI 0012FE2B ASCII "DeleteCriticalSection"
009EF9CF 009EF9D1	✓ 74 05 83FB 04	JE SHORT 009EF9D6 CMP EBX.4	EIP 009EF9C1
009EF9D4	~ 75 37 8006	UNZ SHORT 009EFA0D	C 0 ES 0023 32bit 0(FFFFFFF)
009EF9D8	8845 FF	MOU BYTE PTR SS:[EBP-1],AL	P 1 CS 001B 325(t 0(FFFFFFF) A 0 SS 0023 325(t 0(FFFFFFFF)
009EF9DC	3309	XOR ECX, ECX	Z 1 DS 0023 32bit 0(FFFFFFF) S 0 FS 003B 32bit 7FFDD000(FFF)
009EF9DE 009EF9E1	8D85 FFFEFFFF	LEA EAX, DWORD PTR SS: [EBP-101]	T 0 GS 0000 NULL D 0
009EF9E7 009EF9E9	8BD6 E8 1A4BFFFF	MOV EDX,ESI CALL 009E4508	0 0 LastErr ERROR_SUCCESS (00000000)
009EF9EE 009EF9E0	6А 0А В9 АСЗ99Е00	PUSH 0A MOV ECX.9E39AC	EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
009EF9F5	33D2 8955 FF	XOR EDX, EDX	ST0 empty -UNORN BEIC 00000045 0208005E ST1 empty -UNORN BA4C 00000003 00000000
009EF9FA	8D85 FFFEFFFF	LEA EAX, DWORD PTR SS:[EBP-101]	ST2 empty 0.0192141235640032540e-4933 ST3 empty +UNORM 0945 0012BA4A 00000000
009EFA05	8DB5 FFFEFFFF	LEA ESI, DWORD PTR SS: [EBP-101]	ST4 empty 0.0192094893090377850e-4933 ST5 empty +UNORM 0120 7C80F23D 7C91E051
009EFA0D	× EB 02 8B36	MOV ESI, DWORD PTR DS: [ESI]	ST6 empty 1.000000000000000000000000000000000000
009EFH0F 009EFA12	83FB 04 ∨ 75 1A	UNP EBX,4 JNZ SHORT 009EFA2E	3210 ESPUOZDI EST 4020 Cond 1000 Frr 00100000 (E0)
009EFA14 009EFA15	56 8B45 0C	PUSH ESI MOV EAX,DWORD PTR SS:[EBP+C]	FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
009EFA18 009EFA19	50 E8 BEFBFFFF	PUSH EAX CALL 009EF5DC	
009EFA1E 009EFA23	A3 5C359F00 B8 9CC59F00	MOV DWORD PTR DS:[9F355C],EAX	
009EFA28	8B17	MOV EDX, DWORD PTR DS:[EDI]	
Address	Hex dump	ASCII	0012FE1C 0044612C ASPack.0044612C
0044612C 0044613C	00 00 00 00 00 00 0 00 00 00 00 00 0	0 00 00 00 00 00 00 00 00 00 00 00	0012FE24 0012FF80
0044614C	00 00 00 00 00 0		0012FE28 44E32107 0012FE2C 74656C65
0044616C			0012FE30 69724365 0012FE34 61636974
0044617C			0012FE38 6365536C 0012FE3C 6E6E6974
0044619C 004461AC	00 00 00 00 00 00 0		0012FE40 00000000
004461BC 004461CC	00 00 00 00 00 00 0	0 00 00 00 00 00 00 00 00 00 00 00	0012FE48 00000000
004461DC 004461EC	00 00 00 00 00 00 0	0 00 00 00 00 00 00 00 00 00 00 00	0012FE50 00000000
004461FC	00 00 00 00 00 0		0012FE58 0000000
0044621C	00 00 00 00 00 0		0012FE5C 00000000 0012FE60 00000000
00446230			0012FE64 00000000 0012FE68 0000000
0044624C 0044625C	00 00 00 00 00 00 0		0012FE6C 00000000 0012FE70 00000000
0044626C	00 00 00 00 00 00 0 00 00 00 00 00 0	0 00 00 00 00 00 00 00 00 00 00 00	0012FE74 00000000

Parece que vamos bien, jeje, miren el valor que se encuentra en EAX. Es una entrada buena a la IAT. Pues quitemos el BP y nopeemos el CALL y vamos trazando con F8 hasta que vemos un POPAD (hay que tracear muy poco, en mi caso con pulsar 15 veces F8 llegue a el).

🗁 📢 🗙	► II - 4	₽ <mark>₩₩₩</mark> ₽₩₽₩ <mark>₽</mark> ₩	TWH	C / K B R S 📃 🏋 ?
009EFC67 009EFC68 009EFC70 009EFC70 009EFC73 009EFC73 009EFC73 009EFC73 009EFC80 009EFC80 009EFC80 009EFC80 009EFC90 009EFC90 009EFC90 009EFC90 009EFC90 009EFC90 009EFC80 009EFC	53 80F8 02 74 06 0FB60E 41 EB 05 B9 044000000 01CE EB CE 61 EB CE 61 EB CE 63 91FC9E00 FF0424 C3 BC 3844240C EB 01 3683 30B80000 0002 EB 1A BC EB17E8EB 14 E8 EB 11 E8 EB0E88EB 0088 EB 04 EB 04 E8 EB01E831 C0C3 EB 01E8 31C0 EB 02 CD 20 CD 20 CD 20 64:FF30 EB 01 E9 04892031 27F401=00A32D0C 30, (ASCII "0aD"	PUSH EBX CMP AL,2 JE SHORT 009EFC73 MOUZX ECX,BYTE PTR DS:[ESI] INC ECX JMP SHORT 009EFC78 MOU ECX,4 ADD ESI,ECX CALL 009EF940 POP EBX JMP SHORT 009EFC50 POPAD CALL 009EFC22 PUSH 9EFC91 INC DWORD PTR SS:[ESP] RETN MOU ESP,0C24448B JMP SHORT 009EFC99 XCHG BYTE PTR DS:[EBX+B880],AL ADD BYTE PTR DS:[EBX+B880],AL JMP SHORT 009EFC8C MOU ESP,EB817EB ADC AL,0E8 JMP SHORT 009EFCBC CALL 2087089B OR EBP,EAX JMP SHORT 009EFCBC CALL 2086FER8 ROL BL,0EB ADD EAX,EBP XOR EAX,EAX JMP SHORT 009EFCC8 INT 20 JMP SHORT 009EFCC8 INT 20 INT 20 IN		Registers (FPU) < < EAX 7C92188A ntdll.RtlDeleteCriticalSection ECX 0012FE0C EDX 0044612C ASPack.0044612C EBX 0012FF80 ASCII "0aD" ESP 0012FF80 ESI 00A32D31 EDI 0044612C ASPack.0044612C EIP 009EFC7F C 0 ES 0023 32bit 0(FFFFFFFF) A 1 SS 0023 32bit 0(FFFFFFFF) A 1 SS 0023 32bit 0(FFFFFFFF) A 1 SS 0023 32bit 0(FFFFFFFF) A 00000 NULL D 0 D 0 0000 NULL D 0 D 0 0 LastErr ERROR_SUCCESS (00000000) EFL 00000216 (NO.NB.NE.A.NS.PE.GE.G) ST0 empty -UNORM BE1C 00000045 0208005E ST1 empty -UNORM BE1C 00000045 0208005E ST3 empty +UNORM 0945 0012BA4A 00000000 ST3 empty +UNORM 0945 0012BA4A 00000000 ST4 empty 0.019204493000377850e-4933 ST5 empty +UNORM 0114 7C80F23D 7C91E051 ST6 empty 1.000000000000000000 ST7 empty 80.000000000000000000 ST7 empty 80.00000000000000000000000000000000000
Address H	ex dump		ASCII	🔀 0012FF40 00A32D0C ASCII "kernel32.dll"
0044612C 8 0044613C 0 0044615C 0 0044615C 0 0044615C 0 0044617C 0 0044618C 0 0044618C 0 0044618C 0 0044618C 0 004461CC 0 004461CC 0 004461CC 0 004461CC 0	18 92 70 00 01 2 00 00 00 00 00 00 00 2 00 00 00 00 00 00 00 00 2 00 00 00 00 00 00 00 00 00 2 00 00 00 00 00 00 00 00 2 00 00 00 00 00 00 00 00 2 00 00 00 00 00 00 00 00 2 00 00 00 00 00 00 00 00 2 00 00 00 00 00 00 00 00 2 00 00 00 00 00 00 00 00 2 00 00 00 00 00 00 00 00 3 00 00 00 00 00 00 00 00 3 00 00 00 00 00 00 00 00 3 00 00	100 100 <td>è↑Æ!</td> <td>0012FF44 00950000 0012FF48 009C0000 0012FF50 0012FF88 0012FF50 0012FF64 0012FF58 0012FF64 0012FF58 0012FF60 0012FF50 0000000 0012FF60 000302E0 0012FF64 009C0000 0012FF64 009C0000 0012FF64 009C0000 0012FF64 009C0000 0012FF64 009C0000 0012FF64 009C0000 0012FF64 009C0000 0012FF74 33A004CA 0012FF74 00A302E0</td>	è↑Æ!	0012FF44 00950000 0012FF48 009C0000 0012FF50 0012FF88 0012FF50 0012FF64 0012FF58 0012FF64 0012FF58 0012FF60 0012FF50 0000000 0012FF60 000302E0 0012FF64 009C0000 0012FF64 009C0000 0012FF64 009C0000 0012FF64 009C0000 0012FF64 009C0000 0012FF64 009C0000 0012FF64 009C0000 0012FF74 33A004CA 0012FF74 00A302E0

Bueno, en la anterior imagen podemos ver el POPAD, pero no solo eso, también podemos ver que nuestro primer valor de la IAT ya si que parece una entrada de la IAT buena. Para que nos la repare toda sin tener que tracear para reparar toda la IAT, pongamos un BP en el POPAD y demos a F9.

DESEMPACAR ASPACK 2.12 COMPRIMIDO CON ASPROTECT 1.23

26-06-2008

009EFC67 53	PUSH EBX	~	Registers (FPU) 🗸 🤇
009EFC6B ~ 74 06 009EFC6D 0FB60E	JE SHORT 009EFC73 MOVZX ECX,BYTE PTR DS:[ESI]		EAX 0000000 ECX 0012FE0C EDX 00446698 OSPack 00446698
009EFC70 41 009EFC71 V EB 05 009EFC72 P9 04000000	INC ECX JMP SHORT 009EFC78 MOU ECX 4		EBX 00A3429E ASCII "wininet.dll" ESP 0012FF44
009EFC78 01CE 009EFC78 E8 C1FCFFFF	ADD ESI,ECX CALL 009EF940		EBP 0012FF88 ESI 00A34332 EDI 00A44690 0SPaak 00446690
009EFC7F 5B 009EFC80 ^ EB CE	POP EBX JMP SHORT 009EFC50		EIP 009EFC82
009EFC83 E8 3A000000 009EFC88 68 91FC9E00	CALL 009EFCC2 PUSH 9EFC91		C 0 ES 0023 32bit 0(FFFFFFF) P 1 CS 001B 32bit 0(FFFFFFFF) c 0 001B 32bit 0(FFFFFFFF)
009EFC8D FF0424 009EFC90 C3	INC DWORD PTR SS:[ESP]		Z 1 DS 0023 32bit 0(FFFFFFF) S 0 FS 0038 32bit 7FFDD000(FFF)
009EFC96 V EB 01 009EFC98 8683 80B80000	JMP SHORT 00244486 JMP SHORT 009EFC99 XCHG BYTE PTR DS:[EBX+B880],AL		T 0 GS 0000 NULL D 0 0 0 L 2000 EPPOR SUCCESS (000000000)
009EFC9E 0002 009EFCA0 ~ EB 1A	ADD BYTE PTR DS:[EDX],AL JMP SHORT 009EFCBC MOULESE EDEC17ED		EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
009EFCA7 14 E8 009EFCA9 ~ EB 11	ADC AL,0ES JMP SHORT 009EFCBC		ST0 empty -UNORM BELC 00000045 0208005E ST1 empty -UNORM BA4C 00000003 00000000 ST2 empty 0 0192141235640032540e-4933
009EFCHB E8 EB0EE8EB 009EFCB0 0BE8 009EFCB2 × E8 08	OR EBP,EAX)	ST3 empty +UNORM 0945 0012BA4A 00000000 ST4 empty 0.0192094893090377850e-4933
009EFCB4 CD 20 009EFCB6 ~ EB 04	INT 20 JMP SHORT 009EFCBC		ST5 empty forokn 0114 (CS0F23D (C91E051 ST6 empty 1.00000000000000000000 ST7 empty 80.00000000000000000
009EFCBD C0C3 EB 009EFCC0 01E8	ROL BL, ØEB ADD EAX, EBP		3210 ESPU07DI FST 4020 Cond 1000 Err 00100000 (FCH 0275 Proc NEOP 52 Mark 11111
009EFCC2 31C0 009EFCC4 ~ EB 02 009EFCC6 CD 20	XOR EAX,EAX JMP SHORT 009EFCC8 INT 20		FOW DEFF FIEL HERR, 55 Hask IIIIII
009EFCC8 64:FF30 009EFCC8 ~ EB 01	PUSH DWORD PTR FS: (EAX)		
009EFCCD - E9 64892031	JMP 315-8636	×	
Address Hex dump 0044612C 8A 18 92 7C ED 1	ASCII 0 91 7C 05 10 91 7C F1 9E 80 7C è↑Æ;γ́▶æ;	∔ ∳æ	0012FF44 009E0000 @12FF48 009C0000 @12FF48 009C0000
0044613C E4 9A 80 7C 51 9 0044614C D4 A0 80 7C C5 9 0044615C 00 00 00 00 CE E	A 80 7C 2F 99 80 7C 8D 99 80 7C %ùǦQùǦ B 80 7C 40 97 80 7C F8 9B 80 7C ἑåǦ†¢Ç¦ 4 80 7C 31 03 92 7C 00 00 00 00	/ŏÇ @ùÇ 1∰Æ	C10C C012FF50 0012FF64 0012FF54 00A3067B ASCII "OIX"
0044616C 58 C0 80 7C 37 0 0044617C 44 20 83 7C 40 7	6 81 7C 87 0D 81 7C 8E 0B 81 7C X+C:7±ů: A 94 7C 0E 18 80 7C 09 2A 81 7C D 3:0z;;	ç.ü Atç	0012FF58 0012FFE0 0012FF5C 00000000 012FF5C 0002000
00446180 39 2F 81 70 77 6 00446190 DA CD 81 7C 24 1 004461AC 8A 05 3D 7E 00 0	H 81 7C 68 17 80 7C 51 0E 81 7C 97u;w.u; A 80 7C 47 9B 80 7C 00 00 00 00 r=ü!\$⇒Ç; 0 00 00 EA 6A 0F 77 1E 4E 0F 77 ē≰="	k≇Ç GøÇ 0.i≋	Q:UAU C:
004461BC 20 49 0F 77 7E 4 004461CC E7 EB DA 77 49 6	C 0F 77 A7 48 0F 77 00 00 00 00 1****L** F DB 77 83 78 DA 77 85 C1 DC 77 \$\u00fcruid ruid	0Ř×⊨ āx r	₩₩ 0012FF6C 00001000 ₩₩1=₩ 0012FF70 00041A00 0012FF74 33A004CA
004461EC F4 EA DA 77 68 6 004461EC F4 EA DA 77 F0 6 004461FC 87 0D 81 7C D4 F	9 DB 77 00 00 00 00 54 5D 83 7C 10 www.ww 8 DA 77 00 00 00 00 54 5D 83 7C 10 www.rw 0 80 7C 20 25 80 7C 51 9A 80 7C ç.ü!żáç!	2¢	₩1-₩ TJ3: 0012FF78 00A302E0 0012FF7C 00A34338 01000: 0012FF7C 00A34338
0044620C 03 CE 81 7C 69 E 0044621C 82 27 81 7C 0F F 0044623C 85 55 83 7C 00 6	C 80 7C B8 1C 83 7C 8E 0B 81 7C ♥fü¦i"€!! C 80 7C 0E 18 80 7C C6 97 80 7C e'üi*%Ç! a aa ae PE 98 7C C7 1D 98 7C e'üi*%Ç!	©∟â ∦†Ç ⊼≄c	3/3/01 0012FF84 0044657C H3F3CK.0044667C C/3/CL 0012FF88 0012FF98
0044623C 79 9E 80 7C 01 9 0044624C 89 4C 83 7C 19 F	E 80 7C 82 FE 80 7C 89 23 81 7C 9×C10×C1 F 80 7C 2F FC 80 7C 88 08 83 7C 11L3!↓Ç!	ē∎Ç ∕⊁Ç	Ȧ((#ů)) 0012FF8C 009EFDA4 0012FF90 009F0874 Ȧπ∂ā: 0012FF94 009F6874
0044625C 2D FD 80 7C A9 6 0044626C FF 08 86 7C 3D E 0044627C CF B4 80 7C 62 D	0 83 7C DE 2A 81 7C 00 00 00 00 00℃;03°a; F 80 7C 74 C5 9E 00 56 2B 83 7C ∎3¦=¬Ç; 2 80 7C 31 03 92 7C FC 38 81 7C 0+C;bēC;	1₩U t+× 1₩Æ	Ul
0044628C 45 1C 83 7C 77 0 0044629C 00 00 00 00 00 00 0044629C 0F 08 80 7C 00 F	A 81 7C 35 14 82 7C 28 97 80 7C ELâiw.ů: 0 00 00 FE 4F 83 7C 00 00 00 00 7 82 7C 89 BE 80 7C 81 45 83 7C ikciana:	5¶é ∎0ā ä¥c	e((ûç) 0012FFA0 0046868E HSPack.0046868E 9012FFA4 7C923E6F RETURN to ntdll.7C 0012FFA8 7C923E62 RETURN to ntdll.7C
Commanc bp 7ffdf000	•		
Proskosist at 009EEC92			

Mirad que bien quedo la IAT, jeje, ahora quitemos el BP y con el - del teclado vamos volviendo hacia atrás hasta llegar a los nops de la CALL que nopeamos y una vez allí seleccionamos todos los nops que forman parte del lugar donde estaba el CALL, hacemos clic derecho y le damos a Undo Selection para dejarlo como antes y que no nos detecte Asprotect:

DESEMPACAR ASPACK 2.12 COMPRIMIDO CON ASPROTECT 1.23

26-06-2008

	<u> </u>	
009EF985 009EF988 009EF988 009EF988 009EF988 009EF990 009EF990 009EF990 009EF990 009EF990 009EF990 009EF980 009EF980 009EF980 009EF980 009EF980 009EF922 009EF922	8845 FF 46 33DB 845D FF 8D25 FFFEFF 8BD6 E3 6B4BFFFF 6A 0A B9 B6399F00 8D35 FFFEFF E3 EBCAFFFF 8D85 FFFEFF 56 8B45 0C 56 8B45 0C 56 8B45 0C 50 90 90 90 90 90	MOV BYTE PTR SS:[EBP-1],AL A NCC ESI XOR EBX,EEX MOV BL,BYTE PTR SS:[EBP-1] CALL 009E4508 MOV ECX,EEX MOV ECX,EEX FF LEA EAX,DWORD PTR SS:[EBP-101] MOV EDX,ESI CALL 009E4508 PUSH 0A MOV ECX,9739B6 MOV ECX,FEX MOV ECX,9739B6 MOV EDX,ESI CALL 009EC490C FF LEA EAX,DWORD PTR SS:[EBP-101] PUSH ESI O09EC490C FF LEA ESI,DWORD PTR SS:[EBP+C] PUSH ESI O09EC490C PUSH EX CALL 009EFSDC NOP NOP NOP NOP NOP NOP
009EF9C4 009EF9C5 009EF9C6 009EF9C6 009EF9C6 009EF9C6 009EF9C6 009EF901 009EF901 009EF901 009EF908 009EF908 009EF908 009EF908 009EF908 009EF908 009EF908 009EF908 009EF908	90 90 8B17 8902 * EB 7B 83FB 01 * 74 05 83FB 04 * 75 37 8406 8845 FF 46 33C9 8845 FF 46 33C9 8840 FF 8D85 FFFEF 8D85 FFFEF 8BD6 E8 1A4BFFF	Backup > Copy > Binary > Undo selection Alt+BkSp Assemble Space Label : Comment ; Breakpoint > New origin here Ctrl+Gray* Go to Ctrl+Gray*
		Follow in Dump •
Address 0044612C 0044613C 0044614C 0044615C 0044615C 0044618C 0044618C 0044618C 004461AC 004461AC	Hex dump - 8A 18 92 7C E4 9A 80 7C 04 00 00 00 58 CØ 80 7C 44 20 83 7C 44 20 83 7C DA CD 81 7C DA CD 81 7C 20 49 05 3D 7E	Search for Search
004461CC 004461DC	E7 E8 DA 77 18 76 DA 77 -	Dump debugged process rwic wax rwit w 0012FF70 00041A00
004461EC 0044620C 0044620C 00446221C 00446221C 0044623C 0044623C 0044624C 0044625C 0044622C 0044622C 0044622C 0044622C 0044622C 0044622C	F4 EA DA 77 87 ØD 81 77 03 CE 81 77 82 27 81 70 87 52 83 70 8 79 9E 80 70 8 89 40 83 70 8 79 9E 80 70 8 89 40 80 80 70 8 60 80 70 8 8 70 8 645 10 83 70 7 9 9 90<	Appearance 0012FF78 0012FF78 004302E0 0044669C F AC 80 7C 0E 18 80 7C C6 97 80 7C 6'''''''''''''''''''''''''''''''''''

Ahora volvemos a pulsar Ctrl. + O y volvemos a dejar desmarcadas todas las opciones menos la primera:

🗄 Debugging options 🛛 🔀							
Commands Disasm CPU Registers Stack Analysis 1 Analysis 2 Analysis 3							
Security Debug Events Exceptions Trace SFX Strings Addresses							
Ignore memory access violations in KERNEL32							
Ignore (pass to program) following exceptions:							
🔲 INT3 breaks							
🔲 Single-step break							
Memory access violation							
Integer division by 0							
Invalid or privileged instruction							
All FPU exceptions							
Ignore also following custom exceptions or ranges:							
Add last exception							
Add range							
Delete selection							
Cancel							

Aceptamos y le damos a F9 y empezamos a contar las excepciones incluida la primera que te da a al darle a F9. En mi caso, a la 10 ya arranca el programa así que vuelvo a reiniciar el Olly y vuelvo a hacer todo igual para reparar la IAT hasta volver a llegar a este punto donde ya se que tengo que parar en la excepción 9[°] en mi caso. Una vez parado en la ultima excepción antes de que arranque el programa, voy al Memory Map con Alt + M y pongo un Breakpoint on Memory Access en la sección .code del ejecutable y le doy a F7 y F9 y nos parara en el OEP y esta vez con la IAT prácticamente reparada.

26-06-2008

🖻 ┥ 🗙			LEM	тwнс	/ K	B R	S	?	
Image: Constraint of the system 0044289D 0044289D 0044289D 004428P2 004428B1 004428B1 004428B2 004428B1 004428C0 004428C1 004428C2 004428C3 004428C4 004428C5 004428C6 004428C7 00442901 00442901 00442915 00442915 00442920 00442920 00442920 00442920 00442920 00442920 00442920 00442920 00442920 00442920 00442920 </th <th>55 8BEC 83C4 F4 E8 4008FCFF E8 0021FCFF E8 054FCFF E8 06C6FCFF E8 08E7FCFF E8 08E7FCFF E8 08E7FCFF E8 08E7FCFF E8 08E7FCFF E8 639AFEFF E8 639AFEFF E8 639AFEFF E8 639AFEFF E8 639AFEFF E8 659AFEFF E8 0517EFF E8 0517EFF E</th> <th>► ► ► ► PUSH EBP MOV EBP,ESP ADD ESP,-0C CALL 004035F4 CALL 004093F4 CALL 004097D14 CALL 00407D14 CALL 0040F8C CALL 0040F8C CALL 0040F8C CALL 0040F8C CALL 0040F8C CALL 0042F8C CALL 0042F8C CALL 0042CBC CALL 0042CEAC CALL 0042CEAC CALL 0042E3C CALL 0042E3C CALL 0042E3C CALL 0042E3C CALL 0042E3C CALL 0042E3C CALL 0042E3C CALL 0042E3C CALL 0042E3C CALL 0042CFAC CALL 0042CFAC CALL 0042CFAC CALL 0042FAC CALL 0042CFAC CALL 0042SAFA CALL 0042SAFA CALL 0042AFC CALL 0042AFC MOV EAX, DWORD PTR DS:1 MOV EAX, DWORD PTR DS:1 MOV EAX, DWORD PTR DS: EEP POP EBP RETN ADD BYTE PTR</th> <th>L E M DS: [445630] DS: [445630] 44490[] DS: [445630] AX], AL AX], AL</th> <th>TWHC ~</th> <th>Register Register ECX 7C92 EDX 7C92 EDX 7C92 EDX 7C92 EDX 7C92 EDX 7C92 EDX 7C92 ESP 0012 ESP 0012 ESP 0012 ESP 0012 ESP 0012 EST 002 ST0 EST 0027 ST1 empt ST1 empt ST1 empt ST2 empt ST3 empt ST3 empt ST4 empt ST4 empt ST5 empt ST6 empt ST7 empt ST6 empt ST7 empt</th> <th>B R s (FPU) 4289C ASPs 26315 ntdl 26008 ntdl 26608 ntdl 27FC4 27FC4 28E6F ntdl 28E6F ntdl 28E6F ntdl 289C ASPs 0023 32bi 0023 32bi 0020 NULL stErr ERRO 1000 NULL stErr ERRO 1000 NULL stErr ERRO 1000 NULL 1000 NULL 10</th> <th>S CK.0044289 L.7C926315 L.7C928605 L.7C923E6F CK.0044289 t 0(FFFFFF t 00000 BA4C 00000 BA4C 00000 BA4C 00000 BA4C 00000 BA4C 00000 CSSS NB,NE,A,NS BE1C 00000 BA4C 00000 CSSS NB,NE,A,NS BE1C 00000 CSSS NB,NE,A,NS BE1C 00000 CSSS NB,NE,A,NS BE1C 00000 CSSS NB,NE,A,NS BA4C 00000 CSSS NB,NE,A,NS BA4C 00000 CSSS NB,NE,A,NS BA5C 00125 0000000000 CSSS CSSS CSSS NB,NE,A,NS BA5C 00125 CSSS NB,NE,A,NS BA5C 00125 CSSS NB,NE,A,NS BA5C 00125 CSSS NB,NE,A,NS SSS NB,NE,A,NS SSS CSSS CSSS CSSS NB,NE,A,NS SSS CSSS CSSS CSSS NB,NE,A,NS SSS C</th> <th>2 2 2 2 2 2 2 2 2 2 2 2 2 2</th> <th>5E 1900 1900 1900 1900 1900 1900 1900 190</th>	55 8BEC 83C4 F4 E8 4008FCFF E8 0021FCFF E8 054FCFF E8 06C6FCFF E8 08E7FCFF E8 08E7FCFF E8 08E7FCFF E8 08E7FCFF E8 08E7FCFF E8 639AFEFF E8 639AFEFF E8 639AFEFF E8 639AFEFF E8 639AFEFF E8 659AFEFF E8 0517EFF E8 0517EFF E	► ► ► ► PUSH EBP MOV EBP,ESP ADD ESP,-0C CALL 004035F4 CALL 004093F4 CALL 004097D14 CALL 00407D14 CALL 0040F8C CALL 0040F8C CALL 0040F8C CALL 0040F8C CALL 0040F8C CALL 0042F8C CALL 0042F8C CALL 0042CBC CALL 0042CEAC CALL 0042CEAC CALL 0042E3C CALL 0042E3C CALL 0042E3C CALL 0042E3C CALL 0042E3C CALL 0042E3C CALL 0042E3C CALL 0042E3C CALL 0042E3C CALL 0042CFAC CALL 0042CFAC CALL 0042CFAC CALL 0042FAC CALL 0042CFAC CALL 0042SAFA CALL 0042SAFA CALL 0042AFC CALL 0042AFC MOV EAX, DWORD PTR DS:1 MOV EAX, DWORD PTR DS:1 MOV EAX, DWORD PTR DS: EEP POP EBP RETN ADD BYTE PTR	L E M DS: [445630] DS: [445630] 44490[] DS: [445630] AX], AL AX], AL	TWHC ~	Register Register ECX 7C92 EDX 7C92 EDX 7C92 EDX 7C92 EDX 7C92 EDX 7C92 EDX 7C92 ESP 0012 ESP 0012 ESP 0012 ESP 0012 ESP 0012 EST 002 ST0 EST 0027 ST1 empt ST1 empt ST1 empt ST2 empt ST3 empt ST3 empt ST4 empt ST4 empt ST5 empt ST6 empt ST7 empt ST6 empt ST7 empt	B R s (FPU) 4289C ASPs 26315 ntdl 26008 ntdl 26608 ntdl 27FC4 27FC4 28E6F ntdl 28E6F ntdl 28E6F ntdl 289C ASPs 0023 32bi 0023 32bi 0020 NULL stErr ERRO 1000 NULL stErr ERRO 1000 NULL stErr ERRO 1000 NULL 1000 NULL 10	S CK.0044289 L.7C926315 L.7C928605 L.7C923E6F CK.0044289 t 0(FFFFFF t 00000 BA4C 00000 BA4C 00000 BA4C 00000 BA4C 00000 BA4C 00000 CSSS NB,NE,A,NS BE1C 00000 BA4C 00000 CSSS NB,NE,A,NS BE1C 00000 CSSS NB,NE,A,NS BE1C 00000 CSSS NB,NE,A,NS BE1C 00000 CSSS NB,NE,A,NS BA4C 00000 CSSS NB,NE,A,NS BA4C 00000 CSSS NB,NE,A,NS BA5C 00125 0000000000 CSSS CSSS CSSS NB,NE,A,NS BA5C 00125 CSSS NB,NE,A,NS BA5C 00125 CSSS NB,NE,A,NS BA5C 00125 CSSS NB,NE,A,NS SSS NB,NE,A,NS SSS CSSS CSSS CSSS NB,NE,A,NS SSS CSSS CSSS CSSS NB,NE,A,NS SSS C	2 2 2 2 2 2 2 2 2 2 2 2 2 2	5E 1900 1900 1900 1900 1900 1900 1900 190
Address 0044612C 0044613C 0044613C 0044615C 0044613C 0044613C 0044613C 0044619C 0044619C 004461BC 004461BC 004461BC 004461EC 004461EC 004462C 004462C 004462C 0044622C 0044623C 0044625C 0044623C 0044623C	Hex dump 8A 18 92 7C ED 1 E4 9A 80 7C 51 9 B8 C9 9E 00 CF B B8 C9 9E 00 CF B S8 C9 9E 00 CF B S8 C0 80 7C 37 0 S8 C9 9E 00 CF B S8 C0 80 7C 37 0 S8 C9 9E 00 CF B S8 C0 80 7C 27 7 B4 20 81 7C 24 1 B7< EB DA 7C 14 6 82 27 83 7C 28 6 837 52 83 7C 19 6 84 80	0 91 7C 05 10 91 7C A 80 7C 2F 99 80 7C B 80 7C 2F 99 80 7C A 80 7C 31 03 92 7C A 81 7C 0E 18 80 7C A 91 7C 0E 18 80 7C A 91 7C 0E 18 80 7C A 80 7C 4F 9B 80 7C A 80 7C 4F 9B 80 7C C 0F 77 A7 4B 0F 77 F DB 77 83 78 DA 77 F 08 7C 80 25 80 7C C 80 7C 88 1C 83 7C C 80 7C 82 FE 80 7C C 80 7C 2F 22 80 7C F 80 7C 2F 28 7C F 80 7C 74 C5 9E 00 F 80 7C 35 14 82 7C F 80 7C 35 14 82 7C A 9E 00 FE 4F 83 7C	F1 9E 80 7C 8 8D 99 80 7C 8 78 98 80 7C 8 18 CA 9E 00 0 8E 08 81 7C 2 09 2A 81 7C 9 00 00 00 00 0 1 60 00 00 00 00 1 1 23 C1 DC 77 1 1 1 54 5D 83 7C 1 <th>SCII *fE: >>=: :: >>: :: : </th> <th></th> <th>0012FFC4 0012FFC0 0012FFC0 0012FFD0 0012FFD0 0012FFE0 0012FFE0 0012FFE0 0012FFE8 0012FFE8 0012FFE8 0012FFF8 0012FFF8 0012FFF8</th> <th>7C816FD7 7C923E62 7FFDC000 80543FFD 0012FFC8 8374F020 FFFFFFFF 7C839AA 7C816FE0 00000000 00000000 00000000 00000000 0000</th> <th>RETURN to RETURN to RETURN to kernel32. ASCII "h#</th> <th>kerne ntdll. ntdll. 7C839Af 7C816FE</th>	SCII *fE: >>=: :: >>: :: :		0012FFC4 0012FFC0 0012FFC0 0012FFD0 0012FFD0 0012FFE0 0012FFE0 0012FFE0 0012FFE8 0012FFE8 0012FFE8 0012FFF8 0012FFF8 0012FFF8	7C816FD7 7C923E62 7FFDC000 80543FFD 0012FFC8 8374F020 FFFFFFFF 7C839AA 7C816FE0 00000000 00000000 00000000 00000000 0000	RETURN to RETURN to RETURN to kernel32. ASCII "h#	kerne ntdll. ntdll. 7C839Af 7C816FE

Este es el momento de dumpear y yo lo haré con el plugin para Olly OllyDump así que adelante:

🔆 - [СРІ	J - main th	read, module A	SPack]			
C File V	iew Debug	Plugins Options	Window H	Help		
<mark>⊫</mark> ∢ ×	· • II	1 +BP-OLLY	VD	ł	EMTWHC/KBR	S
0044289C 0044289D 0044289F 00442892	55 8BEC 83C4 F4 F8 4DØBEC	2 Asprotect_1.	2X_XP		Registers (FPU) EAX 0044289C ASPack ECX 7C926315 ntdll.	<.00
004428A7 004428AC 004428B1	E8 0C21FC E8 6354FC E8 D6C6FC	4 Conditional Br 5 DllBreakEx	anch Logger		EDX 7C98C008 ntdll. EBX 7FFDC000 ESP 0012FFC4 EBP 0012FFF0	.709
00442886 00442888 004428C0 004428C5	E8 BDC/FC E8 08E7FC E8 974DFD E8 B61AFE	6 Hide Debugge 7 ODbgScript	r		ESI 70923E62 ntdll. EDI 70923E6F ntdll.	.7C9 .7C9 k.00
004428CA 004428CF	E8 F986FE E8 E899FE	8 OllyDump			Dump debugged process	0(F
004428D4 004428D9 004428DE 004428E3	E8 639AFE E8 CEA5FE E8 95ABFE E8 30BAFE	9 Punto E(vento 0 WindowJuggle	os) er	+	Find OEP by Section Hop (Trace into) Find OEP by Section Hop (Trace over)	0(F 0(F 7FF
004428E8 004428ED 004428F2 004428F7	E8 6FBAFE E8 FABAFE E8 69E1FE E8 A4AFFF	FF CALL 00428 FF CALL 00428 FF CALL 00430 FF CALL 00430	1350 13EC 1860 1880	-	Options R.	_SUC B.NE
004428FC 00442901 00442906 00442908	A1 305644 E8 D210FE BA 382944 A1 305644	00 MOV EAX,DU FF CALL 00423 00 MOV EDX,44 00 MOV EAX,DU	JORD PTR D: 908 42938 JORD PTR D:	S:[4 S:[44	About BE 456301 ST2 empty +UNORM 45 ST3 empty +UNORM 45	E1C A4C 128

OllyDump - ASPack.exe							
Start <u>A</u> ddress:	400000	<u>S</u> ize	; 78000		Dump		
Entry Point:	1000	-> <u>M</u> odify:	4289C	<u>G</u> et EIP as OB	P Ca <u>n</u> cel		
Base of <u>C</u> ode:	1000	Base of	<u>D</u> ata: 43000				
💌 <u>F</u> ix Raw Size 8	& Offset of D	ump Image					
Section Virtual	Size Virl	ual Offset	Raw Size	Raw Offset	Charactaristic 🔨		
00042	000 000	001000	00042000	00001000	C0000040		
00002	000 000	043000	00002000	00043000	C0000040 📃		
00001	000 000	045000	00001000	00045000	C0000040		
00002	000 00	046000	00002000	00046000	C0000040		
00002	000 00	048000	00002000	00048000	C0000040		
00001	000 00	04A000	00001000	0004A000	C0000040		
00001	000 00	D4B000	00001000	0004B000	C0000040 🗸		
<					>		
 Rebuild Import Method<u>1</u> : Search JMP[API] CALL[API] in memory image Method<u>2</u> : Search DLL & API name string in dumped file 							

Nos aparece una ventana como la de arriba a la cual le desmarcamos la opción Rebuild Import y le damos a Dump y en la siguiente ventana elegimos un nombre y una ubicación y le damos a Guardar y ya tenemos nuestro dumpeado.

Save Dump to F	File					? 🔀
Save Dump to F Guardar en: Documentos recientes Escritorio Mis documentos	Tile ASPack SETUP ASPack, e	< exe exe		• * E	☆ ⊞ •	? 🗙
Mi PC	<u>N</u> ombre: Tip <u>o</u> :	dumpeado.exe Executable file(*.e	xe)		•	<u>G</u> uardar Cancelar

Ahora le vamos a reparar la IAT y para ello usaremos Import Rec.

Lo ejecutamos y como se muestra en la siguiente imagen, buscamos en la lista nuestro proceso para atachearlo y hacemos clic encima.

💰 Import REConstructor v1.6 FINAL (C) 2001-2003 MackT/uCF	
Attach to an Active Process	
c:\archivos de programa\import reconstructor 1.6\import reconstructor v1.6 final\importrec. c:\archivos de programa\aspack\aspack.exe (00001150) c:\windows\system32\notepad.exe (000017A8) c:\archivos de programa\microsoft office\office11\winword.exe (00000BB4) c:\archivos de programa\ollydbg 110\ollydbg.exe (00001054)	Pick DLL Show Invalid
c:\archivos de programa\windows live\mail\wilmail.exe (000007D0) c:\windows\system32\wscntfy.exe (00001500) c:\windows\system32\ntvdm.exe (00001718) c:\archivos de programa\bitcomet\bitcomet.exe (000014B4) c:\tvr\tvr.exe (00000DA8)	Show Suspect Auto Trace
	Clear Imports
Log	
	Clear Log
IAT Infos needed New Import Infos (IID+ASCII+LOADER)	Options
RVA D0000000 Size D0000000 RVA 00000000 Size 00001000 Load Tree Save Tree Get Imports	About Exit

Ahora llega el momento de meter el OEP, RVA y Size y para eso lo apuntamos todo antes.

El Oep es el que tenemos apuntado menos la Image Base que es 400000.

44289C - 400000 = 4289C Axial que ya tenemos el dato para meter en el OEP.

El RVA es el inicio de nuestra IAT menos la Image Base así que:

446128 - 400000 = 46128

Y el Size es el tamaño de nuestra IAT.

Metamos solo el OEP y demos al botón IAT AutoSearch a ver que pasa.

💰 Import REConstructor v1.6 FINAL (C) 2001-2003 MackT/uCF	
Attach to an Active Process	
c:\archivos de programa\aspack\aspack.exe (00001150)	Pick DLL
Imported Functions Found	
2.FThunk:0004612C.NbFunc:1F (decimal:31) valid:ND	Show Invalid
User32.dll FThunk:000461AC NbFunc:1 (decimal:1) valid:YES oleaut32.dll FThunk:000461B4 NbFunc:5 (decimal:5) valid:YES advapi32.dll FThunk:000461CC NbFunc:A (decimal:10) valid:YES 2 FThunk:000461F9 NbFunc:2C (decimal:50) valid:ND	Show Suspect
version.dll FThunk:000462EC NbFunc:3 (decimal:3) valid:YES gdi32.dll FThunk:000462EC NbFunc:3A (decimal:58) valid:YES	Auto Trace
user32.dll FThunk:000463E8 NbFunc:8C (decimal:140) valid:YES shell32.dll FThunk:0004661C NbFunc:1 (decimal:1) valid:YES	Clear Imports
Log	
Current imports: C (decimal:12) valid module(s) (added: +C (decimal:+12)) 14F (decimal:335) imported function(s). (added: +14F (decimal:+335)) (8 (decimal:8) unresolved pointer(s)) (added: +8 (decimal:+8)) Driginal IAT RVA found at: 0004615C in Section RVA: 00046000 Size:00002000	Clear Log
IAT Infos needed New Import Infos (IID+ASCII+LOADER)	Options
OEP 0004289C IAT AutoSearch RVA 00000000 Size 0000120E RVA 00046128 Size 00000578 Iv Add new section	About
Load Tree Save Tree Get Imports Fix Dump	Exit

Como vemos, todos los datos coinciden así que vamos bien. Ahora demos al botón Get Imports y nos deben de aparecer todas las llamadas a las apis que realiza nuestra IAT.

Pero hay un problema, como pueden ver arriba, hay entradas malas que tendremos que resolver nosotros pero antes me queda un ultimo cartucho, usaremos el plugin para Asprotect 1.22 que se le puede meter al ImportRec y que en mi caso ya lo trae así que hago clic en el botón Show Invalid y acto seguido clic derecho encima de la lista que aparece y ejecuto el plugin.

Import REConstructo	or v1.6 FINAL (C) 2001	-2003 MackT/uCF	
12	Attach to an	Active Process	
c:\archivos de programa	NaspackNaspack.exe (00001	150)	Pick DLL
	Imported Functions Fo	und	
 	NbFunc:1F (decimal:31) valid:1)461AC NbFunc:1 (decimal:1)	NO valid:YES	Show Invalid
deaut32.dll FThunk deaut32.dll FThunk deaut32.dll FThunk deaut32.dll FThunk deaut32.dll FThunk	Invalidate function(s) Disassemble / HexView	™valid:YES)) valid:YES 	Show Suspect
version.dll FThunk:0 gdi32.dll FThunk:00 user32.dll FThunk:0 shell32.dll FThunk:0	Trace Level1 (Disasm) Trace Level2 (Hook) Trace Level3 (Trap Flag)	alid:YES 'alid:YES I) valid:YES ilid:YES	Auto Trace Clear Imports
	Plugin Tracers 0	Null	
	Advanced Commands	ASProtect 1.22	_
rva:00046284 forwarded Current imports: C (decimal:12) valid mod –	Cut thunk(s) Delete thunk(s)	RtlGetLastWin32Error	Clear Log
14F (decimal:335) import [8 (decimal:8) unresolver	Expand all nodes Collapse all nodes	mal:+335))	.
IAT Infos nee	eded New	Import Infos (IID+ASCII+LOADER)	Options
OEP 0004289C I/4 RVA 00046128 Siz	AT AutoSearch RVA	00000000 Size 0000120E	About
Load Tree Save Tree	Get Imports	Fix Dump	Exit

Y el resultado es...

💰 Import REConstructor v1.6 FINAL (C) 2001-2003 MackT/uCF	
Attach to an Active Process	
c:\archivos de programa\aspack\aspack.exe (00001150)	Pick DLL
Imported Functions Found	
rva:0004615C mod:kernel32.dll ord:0176 name:GetModuleHandleA	Show Invalid
rva:00046160 mod:kernel32.dll ord:0174 name:GetLastError	Chour Support
rva:00046168 mod:kernel32.dll ord:010A name:GetCommandLineA	Show Suspect
 rva:0004616C mod:kernel32.dll ord:00B8 name:ExitThread rva:00046170 mod:kernel32.dll ord:006D name:CreateThread 	Auto Trace
rva:00046174 mod:kernel32.dll ord:038C name:WriteFile	
 rva:00046178 mod:kernel32.dll ord:0307 name:SetFilePointer rva:00046176 mod:kernel32.dll ord:03E5 name:SetFilePointer 	Clear Imports
Log	
Current imports:	Charles
E [decimal:14] valid module(s) [added: +2 [decimal:+2]] 14F [decimal:335] imported function(s).	
(0 (decimal:0) unresolved pointer(s)) (added: -8 (decimal:-8))	
	Options
IAT Infos needed New Import Infos (IID+ASCII+LOADER)	
0EP 0004289C IAT Autosearch RVA 00000000 Size 0000184E	About
RVA 00046128 Size 00000578 Image: Add new section	
Load Tree Save Tree Get Imports Fix Dump	

Como se puede apreciar, en el Log nos dice que ya no quedan mas entradas malas por resolver y nos felicita.

i Ya la tenemos reparada!

Ahora demos al botón Fix Dump y elijamos el dumpeado que hicimos antes:

Choose your du	imp file to	fix			?	<
Buscar en: Documentos recientes Escritorio	ASPac	k exe do.exe exe		+ E		
Mis documentos Mi PC Mis sitios de red	<u>N</u> ombre: Tip <u>o</u> :	dumpeado.exe PE files (*.exe, *.dll) Abrir como archivo de	e <u>s</u> ólo lectura		 ▲brir Cancelar 	

Le damos a Abrir y...

En el Log nos dice que el archivo se guardo sin problemas así que intentemos ejecutar nuestro dumpeado a ver que pasa. Ojo, el dumpeado con la IAT correcta se guardara como dumpeado_.exe.



Bueno, este Asprotect tiene algunos ases en la manga pero intentaremos derrotarlo. Carguémoslo en otro Olly .

Bueno, aparecemos en el OEP bueno y el método que voy a usar para sacar el error es el siguiente.

En el Olly con el dumpeado, dejo pulsada F8 hasta que me da la siguiente excepción:

Access violation when writing to [0000001]

Si miramos la pila vemos justo arriba del todo:

0012FFB0 0044291B RETURN to dumpeado.0044291B from 009EC9A0

O sea, que donde estamos hemos llegado desde un CALL y si todo hubiera ido bien nos habría retornado a 0044291B así que vayamos allí a ver que vemos. Para ello hacemos clic derecho sobre esa entrada de la pila y elegimos Follow in Disassembler o pulsamos Intro y apareceremos en el retorno de esa CALL.

Es curioso pero estamos unas líneas mas abajo del OEP y el CALL que nos mando allí es el que esta justo encima y es el único de todos los que vemos ahí que usa una dirección indirecta.

Pues bien, vayamos al Olly que tiene el programa original parado en el OEP y vayamos con F8 hasta llegar a ese CALL sin ejecutarlo y cuando estemos encima de el pulsamos F7y vemos:

<u> </u>		· · · · · · · · · · · · · · · · · · ·			<u>66</u>
009EC981 009EC986 009EC992 009EC994 009EC994 009EC999 009EC998 009EC998 009EC998 009EC996 009EC997	A1 58369F00 E8 11F8FFFF 833D 84359F00 1 75 05 E8 5FFFFFF 5E 5B 5D C2 0800 90	MOV EAX, DWORD PTR DS: [9F3658] CALL 009EC49C CHP DWORD PTR DS: [9F3584],0 UNZ SHORT 009EC999 CALL 009EC8F8 POP EST POP EBX POP EBX POP EBN NOP		~	Registers (FPU) EAX 0000001 ECX 0000001 ECX 0000001 EDX 0012FF2C EBX 7FFDC000 ESP 0012FF80 EBP 0012FF00 ESI 7C923E62 nt; EDI 7C923E6F nt;
009EC9A0	833D A8359F00	CMP DWORD PTR DS:[9F35A8],0			EIP 009EC9A0
009EC9A7 009EC9A9 009EC9AF	74 06 FF15 A8359F00 C3 A1 54369F00	CALL DWORD PTR DS:[9F35A8] RETN MOV_EAX,DWORD PTR DS:[9F3654]	ASPack.004427C0		C 0 ES 0023 321 P 0 CS 001B 321 A 0 SS 0023 321 Z 0 DS 0023 321
009EC9B5 009EC9B6 009EC9B8 009EC9B9	C3 8BCØ 55 8BEC	REIN MOV EAX,EAX PUSH EBP MOV EBP.ESP			S 0 FS 003B 32 T 0 GS 0000 NU D 0
009EC9BB 009EC9BE 009EC9C0 ~	8845 08 85C0 75 07	MOV EAX,DWORD PTR SS:[EBP+8] TEST EAX,EAX UNZ SHORT 009EC9C9			EFL 00000202 (N
009EC9C2 009EC9C7 009EC9C9	AI 60359F00 EB 06 50	MOV EAX,DWORD PTR DS:[9F3560] JMP SHORT 009EC9CF PUSH EAX			ST0 empty 0.000 ST1 empty -5.50 ST2 empty -UNOR ST3 empty -UNOR
009EC9CA 009EC9CF 009EC9D0 009EC9D3 009EC9D3	E8 A97AFFFF 5D C2 0400 90 40 00	CALL 009E4478 POP EBP RETN 4 NOP	JMP to kernel32.GetModuleHandleA		ST4 empty -NAN ST5 empty 1.000 ST6 empty 1.000 ST7 empty 1.000
009EC9D6 009EC9D8 009EC9E1 009EC9E2 009EC9E3	E8 9D7AFFFF FF35 40369F00 58 C3 C3	CALL 009E4478 PUSH DWORD PTR DS:[9F3640] POP EAX RETN RETN	JMP to kernel32.GetModuleHandleA		FST 4020 Cond FCW 027F Prec

Pues vale, guardemos esta dirección por si nos volviera a hacer falta y ahora con F7 vamos traceando a ver que pasa y veremos que no se cumple la condición y el salto no se realiza y nos quedamos parados un momento en el CALL que esta justo después del salto para ver a donde va ya que justo después tenemos un RETN y ese CALL es lo ultimo que se ejecutara en ese trozo de código y veremos esto:

009EC9A9 FF15 A8359F00 CALL DWORD PTR DS:[9F35A8] ASPack.004427A8

O sea, que eso es lo mismo que un CALL 004427A8, pues apuntemos eso también que va ha ser vital.

Ahora vamos a comprobar algo; estando parado en el CALL, pon un BP en el salto que tienes justo encima y que no se realizo antes porque la condición no se cumplía. Ahora quitemos el BPM y demos a F9 a ver si vuelve a parar ahí.

Bueno pues ya os digo que no para y como 004427CO esta dentro del código del ejecutable pues vamos a hacer algo.

Sabemos que:

00442915 FF15 0C494400 CALL DWORD PTR DS:[44490C]

Nos manda de cabeza a ...

009EC9A9 FF15 A8359F00 CALL DWORD PTR DS:[9F35A8] ASPack.004427A8

Y que este ultimo CALL es igual que hacer CALL 004427CO

Pues me la juego, voy a hacer algo interesante porque no tendré ni que crear ningún tipo de injerto especial ni nada, simplemente cambiare al primer CALL para que vaya al lugar que va el otro CALL ya que el error que me da en el dumpeado es porque el salto indirecto del primer CALL no esta bien y con esto podríamos solucionarlo. Quedaría así:

DESEMPACAR ASPACK 2	.12 COMPRIMIDO CON ASPRO	TECT 1.23	26-06-2008
00442809 ES 027HFEFF 0044280E ES CEASFEFF 0044280E ES 308AFEFF 004428E3 ES 308AFEFF 004428E3 ES 308AFEFF 004428E3 ES 6FBAFEFF 004428E1 ES 6FBAFEFF 004428F2 ES 6981FEFF 004428F7 ES A4AFFFFF 004428F7 ES A4AFFFFF 004428F7 ES A4AFFFFF 00442901 ES D210FEFF 00442906 BA 38294400 00442908 A1 30564400 00442910 ES DF0DFEFF 00442915 ES S211FEFF 00442915 ES D21BFCFF 00442918 A1 30564400 00442919 90 S311FEFF 00442920 ES D21BFCFF 00442920 C3 00442920 00442920 C3 00442920 00442920	CALL 0042CEAC CALL 0042CEAC CALL 0042E318 CALL 0042E35C CALL 0042E35C CALL 0043D8A0 CALL 0043D8A0 CALL 0043D8A0 MOV EAX, DWORD PTR DS: [445630] CALL 00423908 MOV EAX, DWORD PTR DS: [445630] CALL 004236F4 CALL 004427A8 NOP MOV EAX, DWORD PTR DS: [445630] CALL 00423AF4 CALL 004427A8 NOP MOV EAX, DWORD PTR DS: [445630] CALL 0047 CALL 0047 CAL 004	Unknown command	A 0 Z 1 S 0 D 0 0 EFL ST1 ST2 ST3 ST4 ST5 ST4 ST5 ST7 FST FCW
0044293F 0000	HUD BYTE PIR US:LEHX],AL		

Ahora guardemos los cambios seleccionando las líneas que hemos modificado y haciendo clic derecho y dándole a Copy to Executable->Selecction y acto seguido reiniciemos el Olly que tiene el dumpeado y ejecutémoslo a ver que pasa ahora.

Y nos vuelve a dar otro error igual que el de antes. Axial que lo mismo, miremos en el Stack a ver si hay suerte y...

0012FE00 0043F1BE RETURN to dumpeado.0043F1BE from 009EC8F4

Pues vallamos a 0043F1BE colocándonos encima de esa entrada del Stack y dándole a Intro a ver que se cuece por allí.

SEMPAC	AR ASPACE	(2.12 COMPRIMIDO CON A	ASPROTECT 1.23	26-06-2008
0043F18B 0043F18D 0043F190 0043F196 0043F19B 0043F19B 0043F1A4 0043F1A4 0043F1A8	33D2 8B45 FC 8B80 58020000 E8 FD3EFDFF 8B45 FC 8B80 E4020000 C640 20 00 33D2 8B45 FC	XOR EDX,EDX MOU EAX,DWORD PTR SS:[EBP-4] MOU EAX,DWORD PTR DS:[EAX+258] CALL 00413098 MOU EAX,DWORD PTR SS:[EBP-4] MOU EAX,DWORD PTR DS:[EAX+2E4] MOU BYTE PTR DS:[EAX+20],0 XOR EDX,EDX MOU EOX,DWORD PTR SS:[EBP-4]	dumpeado.00413098	STØ empty ST1 empty ST2 empty ST3 empty ST4 empty ST5 empty ST6 empty ST7 empty
0043F1AD 0043F1B3 0043F1B3 0043F1B5	8880 7C020000 E8 1C3FFDFF FF15 04494400	MOU EAX, DWORD PTR DS: [EAX+27C] CALL 00413004 CALL DWORD PTR DS: [444904]	dumpeado.004130D4 dumpeado.00435246	FST 4020 FCW 027F
0043F1C3 0043F1C5 0043F1C6 0043F1C7 0043F1C8	26:F4 CC 46 F2: B8 A1340EBD	HLT INT3 INC ESI PREFIX REPNE: MOV EAX, BD0E34A1	Privileged command Superfluous prefix	
0043F1CD 0043F1CE 0043F1D1 0043F1D2 0043F1D3 0043F1D3	59 680F 05 F8 58 DBD8 40	POP ECX IMUL ECX,DWORD PTR DS:[EDI],5 CLC POP EAX FCMOUNU ST,ST DEC ESP		
0043F1D6 ^		UMP SHORT 0043F188	dumpeado.0043F188	~
0043F246=d	umpeado.0043F24	6		
Address H	lex dump	ASCII		043F1BE RETURN to dumpead

Pues miremos en el original a ver que hace el CALL que tenemos justo arriba que es el culpable del error. Simplemente vamos a la dirección donde esta la CALL y damos a Intro y, sorpresa sorpresa, jeje, lo único que hace es ir a esa zona que se crea en ejecución y donde solo se encuentra un RETN con lo cual ese CALL es simplemente una trampa para que no lo podamos dumpear limpiamente así que nopeemos ese CALL en el dumpeado y quedara así:

0043F18D 0043F190 0043F198 0043F198 0043F198 0043F198 0043F1A4 0043F1A8 0043F1AB 0043F1AD 0043F1AB	8845 FC 8880 58020000 E8 FD3EFDFF 8845 FC 8880 E4020000 C640 20 00 33D2 8845 FC 88845 FC 8880 7C020000 E8 1C3FFDFF	MOV EAX,DWORD PTR SS:[EBP-4] MOV EAX,DWORD PTR DS:[EAX+258] CALL 00413098 MOV EAX,DWORD PTR SS:[EBP-4] MOV EAX,DWORD PTR DS:[EAX+2E4] MOV EAX,DWORD PTR DS:[EAX+20],0 XOR EDX,EDX MOV EAX,DWORD PTR SS:[EBP-4] MOV EAX,DWORD PTR DS:[EAX+27C] CALL 004130D4	dumpeado.00413098 dumpeado.004130D4	51 51 51 51 51 51 51 51 51 51 51 51 51 5
0043F1B8 0043F1B9 0043F1BA 0043F1BB 0043F1BB 0043F1BC 0043F1BD	90 90 90 90 90 90	NOP NOP NOP NOP NOP		FU
0043F1BE 0043F1C3 0043F1C5	 E9 83000000 26:F4 CC 	UMP 0043F246 HLT INT3	dumpeado.0043F246 Privileged command	
0043F1C6 0043F1C7 0043F1C8 0043F1CD	46 F2: B8 A1340EBD 59	INC ESI PREFIX REPNE: MOU EAX,BDØE34A1 POP ECX	Superfluous prefix	
0043F1CE	680F 05	IMUL ECX, DWORD PTR DS: [EDI],5	×	

Volvamos a guardar los cambios realizados y volvamos a reiniciar el Olly que tiene el dumpeado y volvamos a ejecutarlo a ver que pasa ahora y...

Otra vez igual, y esto empieza a desesperar. Ahora en el Stack tengo esto:

0012FE00 0043F24C RETURN to dumpeado.0043F24C from 009EC8F4

Axial que, como en las otras ocasiones, me planto encima de esa entrada y le doy a Intro y llego a:

0043F240 0043F241 0043F242 0043F243 0043F243 0043F244 0043F245 0043F246	D4 98 89 90 29 80 > FF15_0849440	DB D4 DB 98 DB 98 DB 90 DB 29 DB 80 CALL_DWORD PTR DS: [444908]	CHAR ')'	EBF EBF ED: ED: EIF
0043F24C	. B2 01	MOV DL,1		P ·
0043524E 00435253 00435258 00435258 00435258 00435258 00435256 00435266 00435266 00435266 00435270 00435270 00435278 00435278 00435288 00435288 00435288 00435288 00435288 00435294 00435297 00435295	 B2 01 B3 54804200 E8 04BFFEFF 8945 E0 33C0 55 68 B2F24300 64:FF30 64:8920 B1 01 BA 44F54300 8845 E0 E8 BCC0FEFF 8D4D D4 BA 64F54300 8845 E0 E8 28C4FEFF 8B45 FC 8B80 E401000 83C0 20 E8 E842FCFF 33C0 	MOV ELX, 428054 CALL 0042815C MOV DWORD PTR SS:[EBP-20],EAX XOR EAX,EAX PUSH EBP PUSH 43F282 PUSH DWORD PTR FS:[EAX] MOV DWORD PTR FS:[EAX],ESP MOV CL,1 MOV EDX,43F544 MOV EAX,DWORD PTR SS:[EBP-20] CALL 00428334 LEA ECX,DWORD PTR SS:[EBP-2C] MOV EAX,DWORD PTR SS:[EBP-2C] MOV EAX,DWORD PTR SS:[EBP-2C] MOV EAX,DWORD PTR SS:[EBP-2C] MOV EAX,DWORD PTR SS:[EBP-4] MOV EAX,DWORD PTR SS:[EAX+1E4] ADD EAX,20 CALL 00403584 XOR EAX,EAX	dumpeado.0042B15C ASCII "Software\ASPack\Options" dumpeado.0042B334 ASCII "Lang_LanguageFile" dumpeado.0042B6B0 dumpeado.00403584	PAZST CCC EFL STTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
0043F29F 0043F2A0 0043F2A0	59 59 64:8910	POP ECX POP ECX MOU DWORD PTR ES:FEAX1.EDX		

Vuelvo a ir al Olly que tiene el original y voy a la dirección donde esta esa CALL que vemos encima de donde retornamos y vemos que otra vez es lo mismo, un CALL que nos manda a un lugar de la memoria creado en ejecución y que lo único que ejecuta allí es un RETN. Pero claro, en el dumpeado tampoco existe ese lugar y, por tanto, no existe ese RETN pero como ya dije, un CALL con un RETN detrás no sirve absolutamente para nada así que nopeamos esa CALL en el dumpeado y volvemos a guardar de nuevo los cambios.

Volvemos a reiniciar el Olly con el dumpeado y volvemos a ejecutarlo y...

😂 ASPack 2.12		
ASP Versión	ack 2.12	Compresor de Win32 EXE, DLL, OCX Registrado a: UNREGISTERED O days
Abrir archivo Compri	mir 🗍 Opciones 🗍 Ad	cerca de Ayuda
Abrir	In Nombre Archivo Tamaño (Antes o	formación del archivo de comprimir)
	,	

Por fin, jeje. Pero eso de los O días es porque modifique la fecha haciendo pruebas pero te saldrá la cantidad de días que te quedan. Eso si, para que mi método funcione y no caduque, tienes que descomprimirlo antes de que caduque ya que la comprobación se encuentra en la primera CALL que modificamos y, no se como, pero, cuando caduca, en el original esa CALL coge otro valor que esta justo debajo del destino que tiene ahora y si vais veréis algo muy curioso allí jeje.

Bueno, yo suponía que se había acabado el trabajo pero me dio por probar a comprimir algún exe y cuando acepto la ventanita que me dice que va a comprimir el archivo y le digo que si, vuelve a saltar otro error como los anteriores así que veamos a ver donde esta el fallo.

Esta vez en el Stack tenemos esto:

0012F8DC 004410FE RETURN to dumpeado.004410FE from 009EC8F4

Usando el mismo método que en todas las otras fallas, llego a:

004410EC 004410EF 004410F5 004410F5	 8845 FC 8880 1003000 8843 53 FF15 0449440 	MOV EAX,DWORD PTR SS:[EBP-4] MOV AL,BYTE PTR DS:[EAX+310] MOV BYTE PTR DS:[EBX+53],AL CALL DWORD PTR DS:[E44904]		A Reg EA) EC)
004410FE 00441103 00441104 00441105 00441105 00441106 00441107 00441109	.~ E9 44000000 D6 0F D8 19 22 0D 9D	JHP 00441147 DB D6 DB 0F DB D8 DB 19 DB 22 DB 22 DB 0D DB 9D	dumpeado.00441147 CHAR ''''	EB ES ES ES ED EI
0044110A 0044110B 0044110C 0044110C 0044110E 0044110E 0044110F 00441110 00441111 00441111	14 A3 6E 3D 41 93 36 86 45	DB 14 DB A3 DB 6E DB 3D DB 41 DB 93 DB 36 DB 36 DB 86 DB 45	CHAR 'n' CHAR '=' CHAR 'A' CHAR '6' CHAR '6'	
00441113 00441114 00441115 00441116 00441117 00441117 00441118 00441118 00441118 00441118	4C 8E FF D3 8C 73 19 1C CØ CA	DB 4C DB 8E DB FF DB D3 DB 8C DB 19 DB 12 DB 12 DB 12 DB 12 DB 12 DB 12 DB 12	CHAR 'L' CHAR 's'	STI STI STI STI STI STI STI STI
0044111DI	ØF	IDB ØF		1.9.

Me vuelvo a ir a la dirección de este CALL en el original y una vez encima pulso Intro y otra vez la misma historia, otro RETN así que a nopear ese CALL en el dumpeado y a guardar los cambios.

Otra vez vuelvo a intentarlo y esta vez al volver a aceptar la ventanita que sale para comprimir me vuelve a dar otro error y esta vez en el Stack tenemos:

0012F8DC 0044114D RETURN to dumpeado.0044114D from 009EC8F4

Y en la dirección de retorno:

00441140 00441142 00441142 00441143 00441143 00441145 00441145 00441146	85 FE 06 6E CE 1A > FF15	0849440	UB 86 DB 96 DB 96 DB 96 DB 66 DB 66 DB 66 DB 1A CALL DWORD PTR DS: [444908]	CHAR 'n'	10101010101010
0044114D	. 8B45	FC	MOV EAX.DWORD PTR SS:[EBP-4]		
00441150	. 8B80	0803000	MOV EAX.DWORD PTR DS:[EAX+308]		F
00441156	. 05 98	000000	ADD EAX.98		r
0044115B	. 8B55	FC	MOV EDX.DWORD PTR SS:[EBP-4]		
0044115E	. 8B92	0403000	MOV EDX.DWORD PTR DS:[EDX+304]		
00441164	. E8 1E	24FCFF	CALL 00403584	dumpeado.00403584	
00441169	. BA 70	ED4300	MOV EDX.43ED7C		
0044116E	. 8B45	FC	MOV EAX,DWORD PTR SS:[EBP-4]		
00441171	. 8B80	0803000	MOV EAX, DWORD PTR DS: [EAX+308]		
00441177	. 8990	7002000	MOV DWORD PTR DS:[EAX+27C],EDX		
0044117D	. 8B10		MOV EDX,DWORD PTR DS:[EAX]		
0044117F	. FF92	C400000(CALL DWORD PTR DS:[EDX+C4]		
00441185	. 3300		XOR EAX,EAX		
00441107			DOD EDV		

Pues hago ooootra vez lo mismo y ooootra vez igual, otro RETN así que a nopear la CALL y a volver a guardar los cambios.

Vuelvo a reiniciar Olly un poco cansado ya de esto y vuelvo a intentarlo y esta vez casi termina pero al final de la compresión salta otro error y siguiendo otra vez el método pues tengo en el Stack:

0012F92C 00441E29 RETURN to dumpeado.00441E29 from 009EC8F4

Y en el retorno:

00441E01 00441E07 00441E0D	8B93 2C020000 8B83 F0010000 E8 E6E3FEFF	MOV EDX,DWORD PTR DS:[EBX+22C] MOV EAX,DWORD PTR DS:[EBX+1F0] CALL 004301F8	dumpeado.004301F8	EBI
00441E12 00441E14 00441E19	8BC3 E8 87F0FFFF FF45 FC	MOV EAX,EBX CALL 00440EA0 INC DWORD PTR SS:[EBP-4]	dumpeado.00440EA0	EI
00441E1C 00441E1D 00441E23	4E ^ 0F85 B9FEFFFF FF15 04494400	DEC ESI JNZ 00441CDC CALL DWORD PTR DS: [444904]	dumpeado.00441CDC	P
00441E29	~~E9 3E000000	JMP 00441E6C	dumpeado.00441E6C	5
00441E2E	17	POP SS	Modification of segment register	T T
00441E2F	11E3	ADC EBX,ESP		Lò à
00441E31	C6	???	Unknown command	n i
00441E32	BE 56D5EECA	MOV ESI,CAEED556		
00441E37	BE 2CH6DDF1	MOV ESI,F1DDR62C		EFI
00441E3C	40	DEC ESP		ST
00441E30	2366 НН	HND ESP, DWURD PTR DS:LESI-56J	dumon do . 00444547	ŜŤ
00441E40	× 75 05	JBE SHUKT 00441E47	dumpeado.00441E47	ST:
00441E42				ST
00441E44	24 57	HNU HL,57 MOU FOI 06176164		ST
00441E46	BE 646117H6	100 ESI, H6176164	LOCK eventive is not allowed	ST
00441E46	17	LUCK HID EHA, 0244H407	Modification of common mediator	ST
00441551	46	NEC ECD	nodification of segment register	ST
00441652	1950	ANC ERR ERV		
00441555	000C41 000CDD7	AND ECY NUMBER PTP DEVIECY+770000001		FS
00441E5C	D7	Y OT BYTE PTR DS. [EBY+0] 1		FC
00441F5D	36* FD	STD	Superfluous prefix	
00441E5E	199021 92560FB	SBB DWORD PTR DS: FECX+BE0E56921.EBP	ouper ruous pret in	
00441F66	2F	DAS		
00441F67	SE	POP EST		

Bueno, pues miremos esa CALL en el original a ver que es.

Y otra vez la misma historia así que a nopear también esa CALL en el dumpeado y a guardar los cambios.

Lo volvemos a intentar y otra vez mas el mismo error así que miremos otra vez a ver si esto se acaba ya.

En el Stack tenemos:

0012F92C 00441E72 RETURN to dumpeado.00441E72 from 009EC8F4

Y en el retorno:

00441E65 00441E66 00441E67 00441E68	BE 2F 5E 95	DB BE DB 2F DB 5E DB 95	CHAR :	Ŭ EF
00441E69 00441E6A 00441E6B 00441E6C	0D 66 11 > FF15 0849440	DB 0D DB 66 DB 11 COLL DWORD FTR DS+F4449081	CHAR 'f'	S1 S1 S1
00441E72	> 93300	XOR EAX.EAX		S]
00441E74 00441E75 00441E75	· 5A · 59	POP EDX POP ECX POP ECX		S1 S1 S1
00441E77 00441E7A	. 64:8910 . 68 941E4400	MÖV DWORD PTR FS:[EAX],EDX PUSH 441594		FS F(
00441E82 00441E82 00441E87	. BA 02000000 . E8 C816FCFF	MOV EDX, 20 CALL 00403554	dumpeado.00403554	
00441E8C 00441E8D 00441E92	^ E9 8212FCFF .^ EB EB	UMP 00403114 UMP SHORT 00441E7F	dumpeado.00403114 dumpeado.00441E7F	
00441E94 00441E95 00441E96	. 5F . 5E . 5B	POP EDI POP ESI POP EBX		
00441E97 00441E99 00441E99	. 8BE5 . 5D . C3	MOV ESP,EBP POP EBP RETN		
00441E9B 00441E9C 00441E9C	00 FFFFFFF 0P000000	DB 00 DD FFFFFFF DD 00000000	~	
Jump from	n 00441CB5			

Y al mirar esa CALL en el original veo que es más de lo mismo así que a nopearla y a guardar el dumpeado.

Y vuelvo a intentarlo y...

😂 ASPack 2.12	
ASPACK Versión 2.12 Abrir archivo Comprimir Opciones Au Progreso de compr	Compresor de Win32 EXE, DLL, OCX Registrado a: UNREGISTERED O days cerca de Ayuda
Comprimir!	100 %
Tamaño de compre	esion
Probar!	41 %
E2å eve	

Y a continuación veréis que si lo comprimió y funciona perfectamente.

ropiedades de E2A	A.exe ? 🔀	Propiedades de E2	2A.exe 🛛 🤶 🔀
General Compatibilida	ad Resumen	General Compatibili	dad Resumen
62A	E2A.exe	62A	E2A.exe
Tipo de archivo:	Aplicación	Tipo de archivo:	Aplicación
Descripción:	E24	Descripción:	E24
Ubicación:	C:\Documents and Settings\AGUSTIN\Escritorio	Ubicación:	C:\Documents and Settings\AGUSTIN\Escritorio
Tamaño:	770 KB (788.992 bytes)	Tamaño:	321 KB (328.704 bytes)
Tamaño en disco:	772 KB (790.528 bytes)	Tamaño en disco:	324 KB (331.776 bytes)
Creado:	sábado, 26 de julio de 2008, 16:50:52	Creado:	sábado, 26 de julio de 2008, 16:50:52
Modificado:	martes, 15 de julio de 2008, 23:54:31	Modificado:	martes, 15 de julio de 2008, 23:54:31
Último acceso:	sábado, 26 de julio de 2008, 16:53:35	Último acceso:	sábado, 26 de julio de 2008, 16:52:09
Atributos: So	lo lectura Dculto Opciones avanzadas)	Atributos: 🔲	olo lectura Dculto Opciones avanzadas
	Aceptar Cancelar Apligar		Aceptar Cancelar Apligar

Bueno, el objetivo de este tuto esta cumplido pero queda muy feo eso de UNREGISTERED así que lo cambiaremos usando un editor hexadecimal buscando las palabras esas ya que no aparecen en el Olly y con el editor hexa funciona.

Lo abrimos con cualquier editor hexa y buscamos y a mí con el Pspad me aparece así:

72	0709	6276	4C6F	7765	72.65	6408	uterbvLowered.
4F	7264	6572	0200	0006	5450	616E	TabOrderTPan
50	616E	656C	3204	4C65	6674	0201	el.Panel2.Left
70	0201	0557	6964	7468	039C	0106	.TopWidth.œ
67	6874	0328	0105	416C	6967	6E07	Height.(Align.
54	6F70	0854	6162	4F72	6465	7202	.alTop.TabOrder.
54	4265	7665	6C06	4265	7665	6C31	TBevel.Bevel1
66	7402	0803	546F	7002	0805	5769	.LeftTopWi
03	8001	0648	6569	6768	7402	5905	dth.EHeight.Y.
70	6507	0762	7346	7261	6D65	0553	ShapebsFrame.S
65	0708	6273	5261	6973	6564	0000	tylebsRaised
61	62.65	6COA	4061	6265	6054	7269	.TLabel.LabelTri
4C	6566	7403	E000	0354	6F70	023E	al.Left.àTop.≻
64	7468	03 A C	0006	4865	6967	6874	.Width.¬Height
41	6069	676E	6D65	6E74	0708	7461	Alignmentta
74	6572	0841	7574	6F53	697A	6508	Center.AutoSize.
70	7469	6F6E	060C	554E	5245	4749	.Caption <mark>UNREGI</mark>
52	4544	0A46	6F6E	742E	436F	6C6F	STERED.Font.Colo
63	6C52	6564	0B46	6F6E	742E	4865	rclRed.Font.He
74	02F5	0946	6F6E	742E	4E61	6D65	ight.ö.Font.Name
53	2053	616E	7320	5365	72.69	660A	MS Sans Serif.
74	2E53	7479	6065	0B06	6673	426F	Font.StylefsBo
OA	5061	7265	6E74	466F	6E74	0808	ldParentFont

Y lo cambio por:

72	0709	6276	4C6F	7765	7265	6408	uterbvLowered.
4F	7264	6572	0200	0006	5450	616E	TabOrderTPan
50	616E	656C	3204	4C65	6674	0201	el.Panel2.Left
70	0201	0557	6964	7468	039C	0106	.TopWidth.œ
67	6874	0328	0105	416C	6967	6E07	Height.(Align.
54	6F70	0854	6162	4F72	6465	7202	.alTop.TabOrder.
54	42.65	7665	6C06	4265	7665	6C31	TBevel.Bevel1
66	7402	0803	546F	7002	0805	5769	.LeftTopWi
03	8C01	0648	6569	6768	7402	5905	dth.CHeight.Y.
70	6507	0762	7346	7261	6D65	0553	ShapebsFrame.S
65	0708	6273	5261	6973	6564	0000	tylebsRaised
61	62.65	6COA	4061	6265	6C54	7269	.TLabel.LabelTri
4C	6566	7403	E000	0354	6F70	023E	al.Left.àTop.>
64	7468	O3AC	0006	4865	6967	6874	.Width.¬Height
41	6069	676E	6D65	6E74	0708	7461	Alignmentta
74	6572	0841	7574	6F53	697A	6508	Center.AutoSize.
70	7469	6F6E	060C	2020	2020	4147	.Caption AG
20	2020	0 A46	6F 6E	742E	436F	6C6F	UML .Font.Colo
63	6C52	6564	0B46	6F6E	742E	4865	rclRed.Font.He
74	02 F 5	0946	6F6E	742E	4E61	6D65	ight.õ.Font.Name
53	2053	616E	7320	5365	72.69	660A	MS Sans Serif.
74	2E53	7479	6065	0B06	6673	426F	Font.StvlefsBo

Y guardo los cambios y voy a ver:

Fue bien pero hay mas cosillas que quitar de en medio como el rotulo que sale abajo cuando vas a la pestaña opciones.

😂 ASPack 2.12			
Versión 2.12	Compresor de Win32 EXE, DLL, OCX ————————————————————————————————————		
Abrir archivo Comprimir Opciones Acerca de Ayuda	I		
Comprimir recursos 🔽 usar cargador	DLL de Windows		
🔽 Crear copiar de seguridad (fichero 🔲 Conservar dal	tos extras		
🔽 Autocomprimir despues de cargar 🔲 Añadir a menu	u de contexto		
Salir al finalizar	nbre de la sección		
Compresion Máx Unregistered version, Options are not saved	▼ Lenguaje		

Volvemos a abrirlo en el editor hexa y buscamos y llenamos esa frase con espacios y el resultado es:

442	6576	656C	0642	6576	656C	3404	TBevel.Bevel4.
674	0200	0354	6F70	0200	0557	6964	LeftTopWid
386	0106	4865	6967	6874	038D	0005	th.tHeight.D
967	6E07	0861	6C43	6C69	656E	7400	AlignalClient.
44C	6162	656C	104C	6162	656C	5365	TLabel.LabelSe
96F	6E4E	616D	6504	4C65	6674	0307	ctionName.Left
46F	7002	5205	5769	6474	6802	4806	Top.R.Width.H.
967	6874	020D	0743	6170	7469	6F6E	HeightCaption
365	6374	696F	6E27	7320	6E61	6D65	Section's name
654	4061	6265	6C09	4C61	62.65	6C4C	TLabel.LabelL
704	4065	6674	032E	0103	546F	7002	ang.LeftTop.
769	6474	6802	3006	4865	6967	6874	p.Width.O.Height
743	6170	7469	6F6E	0608	4061	6E67	CaptionLang
765	0000	0654	4061	6265	6C11	4C61	uageTLabel.La
C55	6E72	6567	6973	7465	7265	6404	belUnregistered.
674	0204	0354	6F70	027F	0557	6964	LeftTop.□.Wid
3D8	0006	4865	6967	6874	020D	0743	th.ØHeightC
469	6F6E	062E	556E	7265	6769	7374	aption <mark>Unregist</mark>
564	2076	6572	7369	6F6E	2E20	4F70	ered version. Op
F6E	7320	6172	6520	6E6F	7420	7361	tions are not sa
42E	2020	0A46	6F6E	742E	436F	6C6F	vedFont.Colo
563	6052	6564	0846	6F6E	742E	4865	rclRed.Font.He
0.0.4	OORE	0044		B 4 6 B	470.04	CD CD	· · · · · · · · · · ·
874	0215	0946	6F6E	742E	4E61	6065	ight.o.font.Name
874	0215	0946	6F6E	742E	4661	6065	lght.o.Font.Name
874	0215	0946	6F6E	742E	4661	6065	lght.o.Font.Name
874 44C	6162	0946 656C	6F6E	6162	4£61 656C	БД65 5365	ight.o.Font.Name
874 44C 96F	6162 6E4E	656C 616D	104C 6504	6162 4C65	4£61 656C 6674	5365 0307	ight.o.Font.Name TLabel.LabelSe ctionName.Left
874 44C 96F 46F	6162 6E4E 7002	656C 616D 5205	104C 6504 5769	6162 4C65 6474	4£61 656C 6674 6802	5365 0307 4806	ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H.
874 44C 96F 46F 967	6162 6E4E 7002 6874	656C 616D 5205 020D	6F6E 104C 6504 5769 0743	6162 4C65 6474 6170	4£61 656C 6674 6802 7469	5365 0307 4806 6F6E	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption
874 96F 46F 967 365	6162 6E4E 7002 6874 6374	656C 616D 5205 020D 696F	6F6E 104C 6504 5769 0743 6E27	6162 4C65 6474 6170 7320	4£61 656C 6674 6802 7469 6E61	5365 0307 4806 6F6E 6D65	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption Section's name
874 96F 46F 967 365 654	6162 6E4E 7002 6874 6374 4C61	656C 616D 5205 020D 696F 6265	6F6E 104C 6504 5769 0743 6E27 6C09	6162 4C65 6474 6170 7320 4C61	4£61 656C 6674 6802 7469 6E61 6265	5365 0307 4806 6F6E 6D65 6C4C	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption Section's name TLabel.LabelL
874 44C 96F 46F 967 365 654 704	6162 6E4E 7002 6874 6374 4C61 4C65	656C 616D 5205 020D 696F 6265 6674	104C 6504 5769 0743 6E27 6C09 032E	6162 4C65 6474 6170 7320 4C61 0103	4E61 656C 6674 6802 7469 6E61 6265 546F	5365 0307 4806 6F6E 6D65 6C4C 7002	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption Section's name TLabel.LabelL ang.LeftTop.
874 96F 46F 967 365 654 704 769	6162 6E4E 7002 6874 6374 4C61 4C65 6474	656C 616D 5205 020D 696F 6265 6674 6802	104C 6504 5769 0743 6E27 6C09 032E 3006	6162 4C65 6474 6170 7320 4C61 0103 4865	4E61 656C 6674 6802 7469 6E61 6265 546F 6967	5365 0307 4806 6F6E 6D65 6C4C 7002 6874	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption Section's name TLabel.LabelL ang.LeftTop. p.Width.O.Height
874 96F 46F 967 365 654 704 769 743	6162 6E4E 7002 6874 6374 4C61 4C65 6474 6170	656C 616D 5205 020D 696F 6265 6674 6802 7469	104C 6504 5769 0743 6E27 6C09 032E 3006 6F6E	6162 4C65 6474 6170 7320 4C61 0103 4865 0608	4E61 656C 6674 6802 7469 6E61 6265 546F 6967 4C61	5365 0307 4806 6F6E 6D65 6C4C 7002 6874 6E67	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption Section's name TLabel.LabelL ang.LeftTop. p.Width.O.Height CaptionLang
874 44C 96F 46F 967 365 654 704 769 743 765	6162 6E4E 7002 6874 6374 4C61 4C65 6474 6170 0000	656C 616D 5205 020D 696F 6265 6674 6802 7469 0654	104C 6504 5769 0743 6E27 6C09 032E 3006 6F6E 4C61	6162 4C65 6474 6170 7320 4C61 0103 4865 0608 6265	4E61 656C 6674 6802 7469 6E61 6265 546F 6967 4C61 6C11	5365 0307 4806 6F6E 6D65 6C4C 7002 6874 6E67 4C61	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption Section's name TLabel.LabelL ang.LeftTop. p.Width.O.Height CaptionLang uageTLabel.La
874 96F 46F 967 365 654 704 769 743 765 C55	6162 6E4E 7002 6874 6374 4C61 4C65 6474 6170 0000 6E72	656C 616D 5205 020D 696F 6265 6674 6802 7469 0654 6567	104C 6504 5769 0743 6E27 6C09 032E 3006 6F6E 4C61 6973	6162 4C65 6474 6170 7320 4C61 0103 4865 0608 6265 7465	4E61 656C 6674 6802 7469 6E61 6265 546F 6967 4C61 6C11 7265	5365 0307 4806 6F6E 6D65 6C4C 7002 6874 6E67 4C61 6404	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption Section's name TLabel.LabelL ang.LeftTop. p.Width.O.Height CaptionLang uageTLabel.La
874 96F 96F 365 654 704 769 743 765 674	6162 6E4E 7002 6874 6374 4C61 4C65 6474 6170 0000 6E72 0204	656C 616D 5205 020D 696F 6265 6674 6802 7469 0654 6567 0354	104C 6504 5769 0743 6E27 6C09 032E 3006 6F6E 4C61 6973 6F70	742E 6162 4C65 6474 6170 7320 4C61 0103 4865 0608 6265 7465 027F	4E61 656C 6674 6802 7469 6E61 6265 546F 6967 4C61 6C11 7265 0557	5365 0307 4806 6F6E 6D65 6C4C 7002 6874 6E67 4C61 6404 6964	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption Section's name TLabel.LabelL ang.LeftTop. p.Width.O.Height Caption.Lang uageTLabel.La belUnregistered. LeftTop.O.Wid
874 96F 96F 967 365 654 704 769 743 765 C55 674 3D8	6162 6E4E 7002 6874 6374 4C61 4C65 6474 6170 0000 6E72 0204 0006	656C 616D 5205 020D 696F 6265 6674 6802 7469 0654 6567 0354 4865	6F6E 104C 6504 5769 0743 6E27 6C09 032E 3006 6F6E 4C61 6973 6F70 6967	6162 4C65 6474 6170 7320 4C61 0103 4865 0608 6265 7465 027F 6874	4E61 656C 6674 6802 7469 6E61 6265 546F 6967 4C61 6C11 7265 0557 020D	5365 0307 4806 6F6E 6D65 6C4C 7002 6874 6E67 4C61 6404 6964 0743	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption Section's name TLabel.LabelL ang.LeftTop. p.Width.O.Height Caption.Lang uageTLabel.La belUnregistered. LeftTop.D.Wid th.ØHeightC
874 44C 96F 46F 967 365 654 704 769 743 765 C55 674 3D8 469	6162 6E4E 7002 6874 6374 4C61 4C65 6474 6170 0000 6E72 0204 0006 6F6E	656C 616D 5205 020D 696F 6265 6674 6802 7469 0654 6567 0354 4865 062E	6F6E 104C 6504 5769 0743 6E27 6C09 032E 3006 6F6E 4C61 6973 6F70 6967 2020	742E 6162 4C65 6474 6170 7320 4C61 0103 4865 0408 6265 7465 027F 6874 2020	4E61 656C 6674 6802 7469 6E61 6265 546F 6967 4C61 6C11 7265 0557 020D 2020	5365 0307 4806 6F6E 6D65 6C4C 7002 6874 6E67 4C61 6404 6964 0743 2020	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption Section's name TLabel.LabelL ang.LeftTop. p.Width.O.Height Caption.Lang uageTLabel.La belUnregistered. LeftTop.O.Wid th.ØHeightC aption
874 44C 96F 46F 967 365 654 704 769 743 765 674 3D8 469 020	6162 6E4E 7002 6874 6374 4C61 4C65 6474 6170 0000 6E72 0204 0006 6F6E 2020	656C 616D 5205 020D 696F 6265 6674 6802 7469 0654 6567 0354 4865 062E 2020	104C 6504 5769 0743 6E27 6C09 032E 3006 6F6E 4C61 6973 6F70 6967 2020 2020	742E 6162 4C65 6474 6170 7320 4C61 0103 4865 0408 6265 7465 027F 6874 2020 2020	4E61 656C 6674 6802 7469 6E61 6265 546F 6967 4C61 6C11 7265 0557 020D 2020 2020	5365 0307 4806 6F6E 6D65 6C4C 7002 6874 6E67 4C61 6404 6964 0743 2020 2020	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption Section's name TLabel.LabelL ang.LeftTop. p.Width.O.Height Caption.Lang uageTLabel.La belUnregistered. LeftTop.O.Wid th.ØHeightC aption
874 44C 96F 46F 967 365 654 704 769 743 765 674 3D8 469 020 020	6162 6E4E 7002 6874 6374 4C61 4C65 6474 6170 0000 6E72 0204 0204 0006 6F6E 2020	656C 616D 5205 020D 696F 6265 6674 6802 7469 0654 6567 0354 4865 062E 2020 2020	6F6E 104C 6504 5769 0743 6E27 6C09 032E 3006 6F6E 4C61 6973 6F70 6967 2020 2020 2020	 6162 4C65 6474 6170 7320 4C61 0103 4865 0208 6265 7465 027F 6874 2020 2020 2020 	4E61 656C 6674 6802 7469 6E61 6265 546F 6967 4C61 6C11 7265 0557 020D 2020 2020 2020	5365 0307 4806 6F6E 6D65 6C4C 7002 6874 6E67 4C61 6404 6964 0743 2020 2020 2020	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption Section's name TLabel.LabelL ang.LeftTop. p.Width.O.Height Caption.Lang uageTLabel.La belUnregistered. LeftTop.O.Wid th.ØHeightC aption
874 44C 96F 46F 967 365 654 704 769 743 765 C55 674 3D8 469 020 020 020	6162 6E4E 7002 6874 6374 4C61 4C65 6474 6170 0000 6E72 0204 0204 0204 0204 0202 2020 2020	656C 616D 5205 020D 696F 6265 6674 6802 7469 0654 6567 0354 4865 062E 2020 2020 0A46	104C 6504 5769 0743 6E27 6C09 032E 3006 6F6E 4C61 6973 6F70 6967 2020 2020 2020 6F6E	742E 6162 4C65 6474 6170 7320 4C61 0103 4865 0608 6265 7465 027F 6874 2020 2020 2020 742E	4E61 656C 6674 6802 7469 6E61 6265 546F 6967 4C61 6C11 7265 0557 020D 2020 2020 2020 436F	5365 0307 4806 6F6E 6D65 6C4C 7002 6874 6E67 4C61 6404 6964 0743 2020 2020 2020 6C6F	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption Section's name TLabel.LabelL ang.LeftTop. p.Width.O.Height Caption.Lang uageTLabel.La belUnregistered. LeftTop.O.Wid th.Ø.HeightC aption
874 44C 96F 46F 967 365 654 704 769 743 765 674 3D8 469 020 020 020 563	6162 6E4E 7002 6874 6374 4C61 4C65 6474 6170 0000 6E72 0204 0006 6F6E 2020 2020 2020 6C52	656C 616D 5205 020D 696F 6265 6674 6802 7469 0654 6567 0354 4865 062E 2020 2020 0A46 6564	6F6E 104C 6504 5769 0743 6E27 6C09 032E 3006 6F6E 4C61 6973 6F70 6967 2020 2020 2020 6F6E 0B46	742E 6162 4C65 6474 6170 7320 4C61 0103 4865 0208 6265 7465 027F 6874 2020 2020 2020 742E 6F6E	4E61 656C 6674 6802 7469 6E61 6265 546F 6967 4C61 6211 7265 0557 020D 2020 2020 2020 436F 742E	5365 0307 4806 6F6E 6D65 6C4C 7002 6874 6E67 4C61 6404 6964 0743 2020 2020 2020 2020 6C6F 4865	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption Section's name TLabel.LabelL ang.LeftTop. p.Width.O.Height Caption.Lang uageTLabel.La belUnregistered. LeftTop.O.Wid th.Ø.HeightC aption Font.Colo rclRed.Font.He
874 44C 96F 46F 967 365 654 704 769 743 765 674 3D8 469 020 020 020 563 874	6162 6E4E 7002 6874 6374 4C61 4C65 6474 6170 0000 6E72 0204 0204 0006 6F6E 2020 2020 2020 2020 6C52 02F5	656C 616D 5205 020D 696F 6265 6674 6802 7469 0654 6567 0354 4865 062E 2020 2020 0A46 6564 0946	6F6E 104C 6504 5769 0743 6E27 6C09 032E 3006 6F6E 4C61 6973 6F70 2020 2020 2020 6F6E 0B46 6F6E	742E 6162 4C65 6474 6170 7320 4C61 0103 4865 0208 6265 7465 027F 6874 2020 2020 2020 2020 742E 6F6E 742E	4E61 656C 6674 6802 7469 6E61 6265 546F 6967 4C61 6211 7265 0557 020D 2020 2020 2020 2020 2020 436F 742E 4E61	5365 0307 4806 6F6E 6D65 6C4C 7002 6874 6E67 4C61 6404 6964 0743 2020 2020 2020 2020 2020 6C6F 4865	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption Section's name TLabel.LabelL ang.LeftTop. p.Width.O.Height Caption.Lang uageTLabel.La belUnregistered. LeftTop.O.Wid th.Ø.HeightC aption
874 44C 96F 46F 967 365 654 704 769 743 765 C55 674 3D8 469 020 020 020 563 874 D53	6162 6E4E 7002 6874 6374 4C61 4C65 6474 6170 0000 6E72 0204 0204 0006 6F6E 2020 2020 6C52 02F5 2053	656C 616D 5205 020D 696F 6265 6674 6802 7469 0654 6567 0354 4865 062E 2020 2020 2020 0A46 6564 0946 616E	6F6E 104C 6504 5769 0743 6E27 6C09 032E 3006 6F6E 4C61 6973 6F70 6967 2020 2020 2020 2020 6F6E 0B46 6F6E 7320	742E 6162 4C65 6474 6170 7320 4C61 0103 4865 0208 6265 7465 027F 6874 2020 2020 2020 2020 742E 6F6E 742E 5365	44661 656C 6674 6802 7469 6E61 6265 546F 6967 4C61 6211 7265 0557 020D 2020 2020 2020 2020 2020 2020 202	5365 0307 4806 6F6E 6D65 6C4C 7002 6874 6E67 4C61 6404 6964 0743 2020 2020 2020 2020 6C6F 4865 6D65	Ight.o.Font.Name TLabel.LabelSe ctionName.Left Top.R.Width.H. HeightCaption Section's name TLabel.LabelL ang.LeftTop. p.Width.O.Height Caption.Lang uageTLabel.La belUnregistered. LeftTop.O.Wid th.Ø.HeightC aption Font.Colo rclRed.Font.He ight.Õ.Font.Name MS Sans Serif.

Otra cosilla que le voy a hacer es poner por defecto el lenguaje español ya que este exe no guarda la configuración, pues por lo menos que salga de entrada en español y lo voy a hacer con el editor hexa también. Simplemente busco "english.ini" que es el que esta por defecto y solo aparece una entrada así que nos lo pone fácil.

			2000		00.10	1020	youw in individue
EFF	8845	FC8B	80E4	0100	008B	4820	°°þÿ <eü<€ä<h< td=""></eü<€ä<h<>
444	008B	45F0	E8E7	B3FE	FF33	COSA	°D. <eðèç³þÿ3àz< td=""></eðèç³þÿ3àz<>
489	1068	BAO2	4400	8B45	FOE8	5629	YYd‰.h°.D. <eðèv)< td=""></eðèv)<>
3E9	SC2E	FCFF	EBFO	33CO	5859	5964	üÿÃé\.üÿëð3ÀZYYd
8D7	0244	008B	45F4	E839	29FC	FFC3	‰.h×.D. <eôè9)üÿã< td=""></eôè9)üÿã<>
EFC	FFEB	F080	7DFB	0075	246A	1068	é?.üÿëð€}û.u\$j.h
400	6828	0444	008B	45FC	E807	65FD	.D.h(.D. <eüè.eý< td=""></eüè.eý<>
85D	4EFC	FFA1	3056	4400	E8E7	37FE	ÿPè]Nüÿ;OVD.èç7þ
5FC	8B80	E401	0000	E84D	6BFF	FF8B	ÿ <eü<€äèmkÿÿ<< td=""></eü<€äèmkÿÿ<<>
B80	9002	0000	E8E7	74FE	FF8B	55FC	Eü<€□èçtþÿ< Uü
401	0000	8942	0C33	COSA	5959	6489	<′ä‰B.3ÀZYYd‰
603	4400	8D45	E4E8	F631	FCFF	8D45	.hV.D.□Eäèö1üÿ□E
E31	FCFF	8D45	ECE8	E631	FCFF	C3E9	èèî1üÿ□Eìèæ1üÿÃé
CFF	EBEO	5F5E	5B8B	E55D	C300	0000	À-üÿëà_^[<å]Ã
FFF	0400	0000	2E69	6E69	0000	0000	ÿÿÿÿini
FFF	0800	0000	656E	676C	6973	682E	ÿÿÿÿenglish.
900	FFFF	FFFF	1400	0000	4061	6E67	ini.ÿÿÿÿLang
765	2066	696C	6573	7C2A	2E69	6E69	uage files *.ini
000	FFFF	FFFF	3700	0000	506C	6561	ÿÿÿÿ7Plea
C20	63.68	6F6F	7365	2074	6865	2065	se, choose the e
C69	7368	2E69	6E69	206F	7220	616E	nglish.ini or an

	2022	0 x 2 x 4	2000		00.00	1020	
EFF	8845	FC8B	80E4	0100	008B	4820	°°þÿ <eü<€ä<h< td=""></eü<€ä<h<>
444	008B	45F0	E8E7	B3FE	FF33	COSA	°D. <eðèç³þÿ3àz< td=""></eðèç³þÿ3àz<>
489	1068	BAO2	4400	8845	FOE8	5629	YYd‰.h°.D. <eðèv)< td=""></eðèv)<>
3E9	SC2E	FCFF	EBFO	33CO	5859	5964	üÿÃé∖.üÿëð3ÀZYYd
8D7	0244	008B	45F4	E839	29FC	FFC3	‰.h×.D. <eôè9)üÿã< td=""></eôè9)üÿã<>
EFC	FFEB	F080	7DFB	0075	246A	1068	é?.üÿëð€}û.u\$j.h
400	6828	0444	008B	45FC	E807	65FD	.D.h(.D. <eüè.eý< td=""></eüè.eý<>
85D	4 EFC	FFA1	3056	4400	E8E7	37FE	ÿPè]Nüÿ;OVD.èç7þ
5FC	8B80	E401	0000	E84D	6BFF	FF8B	ÿ <eü<€äèmkÿÿ<< td=""></eü<€äèmkÿÿ<<>
B80	9002	0000	E8E7	74FE	FF8B	55FC	Eü<€□èçtþÿ< Uü
401	0000	8942	0C33	COSA	5959	6489	<′ä%B.3ÀZYYd%
603	4400	8D45	E4E8	F631	FCFF	8D45	.hV.D.□Eäèö1üÿ□E
E31	FCFF	8D45	ECE8	E631	FCFF	C3E9	èèî1üÿ□Eìèæ1üÿÃé
CFF	EBEO	5F5E	5B8B	E55D	C300	0000	À-üÿëà_^[<å]Ã
FFF	0400	0000	2E69	6E69	0000	0000	ÿÿÿÿini
FFF	0800	0000	7370	616E	6973	682E	ÿÿÿÿ <mark>span</mark> ish.
900	FFFF	FFFF	1400	0000	4061	6E67	ini.ÿÿÿÿLang
765	2066	696C	6573	7C2A	2E69	6E69	uage files *.ini
000	FFFF	FFFF	3700	0000	506C	6561	ÿÿÿÿ7Plea
C20	63.68	6F6F	7365	2074	6865	2065	se, choose the e
C69	7368	2E69	6E69	206F	7220	616E	nglish.ini or an

Y como tenemos la suerte de que las dos palabras tienen el mismo largo pues mejor aun.

Ya hay una cosa menos. Ahora a por lo de days, pero eso lo haré en el Olly para que me sirva de ayuda para encontrar la cifra que aparece también ya que days si aparece en las strings.

Hacemos una búsqueda de las strings en el exe:



Y buscamos la string "days" y le ponemos un BP con F2:

	00077 04 UT 300
00438741 MOV EHX,43809C	HSCII 04, "ILZB"
00438786 MUV EHX,43CD88	HSCII "12"
0043B8CF MOV EHX,43CDC4	HSCII "04"
0043B961 MOV EAX,43CDB8	ASCII "12"
0043B99D MOV_EAX,43CDD0	ASCII "05"
0043BA62 MOV_EDX,43CDDC	ASCII ".reloc"
0043BA80 CMP_DWORD_PTR_DS:[EAX+34],400000	ASCII "MZP"
0043C1FE MOV EAX,43CDEC	ASCII "06"
0043CB69 MOV_EDX,43CE00	ASCII ".bak"
0043CFF0 MOV EAX,44390C	UNICODE "REGYSTRYTYPELIB"
0043D23F MOV_EDX,43D61C	ASCII "kernel32.dll"
0043D291 MOV EDX,43D634	ASCII "\$"
0043DE2D MOV EAX,43DE80	ASCII "HTTP://"
0043DEC8 PUSH 43E090	ASCII "InternetReader"
0043DF01 PUSH 43E0A0	ASCII "HTTP/1.0"
0043DF0F PUSH 43E0AC	ASCII "GET"
0043E233 PUSH_43E250	ASCII "NVarFileInfoNTranslation"
0043E33B MOV_EDX,43E3F4	ASCII "\StringFileInfo\"
0043E41F MOV EDX,43E458	ASCII "ProductVersion"
0043E4AE MOV EAX,43E4C8	ASCII "%d.%d.%d.%d"
0043EE03 MOV EDX,43EED4	ASCII "ASPack - "
0043EFBA MOV EDX,43F4E8	ASCII "/@"
0043EFE1 MOV EDX,43F4F4	ASCII " days"
0043F015 MOV_ECX,43F504	ASCII "Aspack.hlp"
0043F064 MOV EAX,43E0E4	ASCII 0C,"TVersionInfo"
0043F0DE MOV EDX,43F518	ASCII "SOFTWARE\ASPack"
0043F0EE MOV_EDX,43F530	ASCII "VersionNum"
0043F12F MOV_EDX,43F530	ASCII "VersionNum"
0043F26B MOV_EDX,43F544	ASCII "Software\ASPack\Options"
0043F27B MOV_EDX,43F564	ASCII "Lang_LanguageFile"
0043F2FB MOV_EDX,43F580	ASCII "*.ini"
0043F38E MOV_EAX,43F590	ASCII ".ini"
0043F534 IMUL_EBP, DWORD_PTR_DS:[EDI+6E],6D754E	UNICODE "va"
0043F60A MOV EDX,43F6A0	ASCII "08"
0043F61E MOV_ECX,43F6A4	ASCII "Error"
0043F6F0 MOV ECX,43F7C8	ASCII ″aspack.ini″
0043F722 MOV EDX,43F7DC	ASCII "Item"
0043F747 MOV EDX,43F7EC	ASCII "PopMenuHistory"
0043F818 MOV_ECX,43F8F0	ASCII "aspack.ini"
0043F866 MOV EDX,43F904	ASCII "Item"
0043F888 MOV EDX, 43F914	HSCII "PopMenuHistory"
0043F967 MUV EDX, 43FR60	HSCII "10"
0043F981 MUV ECX, 43FR64	HSCII "Error"
0043F998 MOV ECX,43FH74	HSCII ".bak"
0043FB49 MOV EDX, 43FERC	HSCII "exefile\shell\"
0043FB80 MOV EDX, 43FEC4	HSUII "NCOMMANd"
0043FBD4 MOV EDX, 43FED8	HSUIT " "%1""
0043FC16 MOV_EDX.43FEF4	ASCII "dllfile\shell\"

Damos a F9 y vemos que para aquí:

1				
I	0043EFB0	8BC3	MOV EAX.EBX	
I	004055500	EO OFAIENEE	COLL 0041212C	dumpeedo 00412120
I	00405552		LEO EON DWODD DID CO. LEDD CO.	dumpeado.00413130
I	0043EFB7	8045 08	LEH EHX, DWORD FIR SS:LEBP-281	
I	0043EFBA	BA E8F44300	MOV EDX,43F4E8	ASCII "/@"
I	0043EFBF	E8 EC46FCFF	CALL 00403680	dumpeado.00403680
I	0043FFC4	9D45 D9	LEG EGY DWORD PTR SS.FERR-291	
I	00400000		DUCU FOY	
I	0043EFU7	50	FUSH EHA	
I	0043EFC8	8D55 D4	LEH EDX,DWORD PIR SS:LEBP-2CJ	
I	0043EFCB	A1 00494400	MOV EAX.DWORD PTR DS:[444900]	
I	0043FFD0	E8 4E6DECEE	COLL 00405024	dumpeado, 00405024
I	0049FED5	OPEE DA	MOLLERY DWORD PTP 99, FERP-201	ampeddol oo loobe l
I	00400000	0000 D4	DOD FOY	
I	0043EFU8	58	PUP EHA	
I	0043EFD9[E8 D246FCFF	CHLL 00403680	dumpeado.00403680
I	0043EFDE	8D45 D8	LEA EAX.DWORD PTR SS:[EBP-28]	
	0043EEE1	BA F4F44300	MOU EDX.43F4F4	ASCII " days"
Г	0043EEE6	E8 C546ECEE	COLL 00403680	dumpeado 00403680
I	0040EEED		MOULERY DWORD DID CO. LEDD-201	dumpeado.oo+000bo
I	0043EFEB	0000000	HOV EDA, DWORD FIR SSILEDF-201	
I	0043EFEE	8BU3	MUV EHX,EBX	
I	0043EFF0	E8 7741FDFF	CALL 0041316C	dumpeado.0041316C
I	0043EFF5	8D55 DØ	LEA EDX.DWORD PTR SS:[EBP-30]	
I	0043FFF8	3300	XOR FAX FAX	
I	00405550	EO NROOFCEE	COLL 00402000	dumpopdo, 88482800
I	0043EFFH	ODAE DO	MOULEOV DWODD DID CONFERD 201	uumpeauo.004020HC
I	0043EFFF	8845 D0	NUV EHX, DWURD PIR SSILEBP-301	
I	0043F002[8055 04	LEA EDX,DWORD PIR SS:LEBP-2CJ	
I	0043F005	E8 6E71FCFF	CALL 00406178	dumpeado.00406178
I	0043F00A	8855 D4	MOV EDX.DWORD PTR SS:[EBP-2C]	
I	0043F00D	01 30564400	MOULEON DWORD PTR DS. [445630]	
I	00405010	000001100		
I	00405012	0000 00	HOU ENA, SU	COOLT NOTIFIED IN LONG
I	0043F015	B9 04F54300	MUV ECX, 43F504	HSUII "HSpack.nip"
I	0043F01A	E8 D546FCFF	CHLL 004036F4	dumpeado.004036F4
I	0043F01F	A1 30564400	MOV EAX.DWORD PTR DS:[445630]	
I	0043F024	C740 5C 881300	MOU DWORD PTR DS:[EAX+5C].1388	
I	0043F02B	9845 FC	MOLL FOX DWORD PTR SS. FERP-41	
I	00400020		MOU DUTE DTD DC. FOV.9001 0	
I	0043F02E	1000 0000000	HOV BYTE FIR DS:LEHAT500,0	
I	0043F035	8845 FC	MUV EHX,DWURD PIR SS:LEBP-4J	
I	0043F038	8B80 E4020000	MOV EAX,DWORD PTR DS:[EAX+2E4]	
1	0043F03E	C640 20 00	MOV BYTE PTR DS:[EAX+20].0	
I	0043E042	3302	XOR EDX.EDX	
I	00435044	OBAE EC	MOLL FOY DWORD PTP SS [FERD-41	
I	00405047	0040 7000000	MOU EOV DWODD DTD DC.FEOV+3703	
I	00405047	0000 (0020000	HOV EHA, DWORD FIR DS:LEHA+2703	1 1 00440004
1	0043F04D	E8_8240FDFF	CHEL 00413004	dumpeado.00413004
I	0043F052	8D55 D4	LEA EDX,DWORD PTR SS:[EBP-2C]	
I	0043F055	A1 30564400	MOV EAX.DWORD PTR DS:[445630]	
I	0043E050	F8 D14CEEEE	COLL 00423D30	dumpeado, 00423D30

Vamos traceando a ver si aparecen los días que muestra y:



Bueno pues estuve haciendo pruebas y la forma que me funciono fue nopear los dos CALLs que están justo debajo del BP y con eso ya no salen los días.

UU40EFDF	EO EUMORURE	CHLL 00403000	uumpeauo.00405660	A Be
0043EFC4	8D45 D8	LEA EAX,DWORD PTR SS:[EBP-28]		EP
0043EFC7	50	PUSH ERX		ĒC
0043EFC8	8055 04	LEH EDX, DWORD PTR SS:LEBP-20J		ED
0043EFCB	H1 00494400	MOV EAX,DWORD PTR DS:[444900]		EE
0043EFD0	E8_4F6DFCFF	CALL 00405D24	dumpeado.00405D24	ES
0043EFD5	8B55 D4	MOV EDX,DWORD PTR SS:[EBP-2C]		FE
0043EFD8	58	POP EAX		ES
0043EFD9	E8 D246FCFF	CALL 004036B0	dumpeado.00403680	ĒĒ
0043EFDE	8D45 D8	LEA EAX, DWORD PTR SS:[EBP-28]		
0043EFE1	BA F4F44300	MOV EDX,43F4F4	ASCII " days"	EI
0043EFE6	90	NOP		C
0043EFE7	90	NOP		Ĕ
0043EFE8	90	NOP		
0043EFE9	90	NOP		2
0043EFEA	90	NOP		Š.
0043EFEB	8B55 D8	MOV EDX,DWORD PTR SS:[EBP-28]		Ť
0043EFEE	8BC3	MOV EAX,EBX		, in the second s
0043EFF0	90	NOP		l l l l l l l l l l l l l l l l l l l
0043EFF1	90	NOP		
0043EFF2	90	NOP		EF
0043EFF3	90	NOP		ST
0043EFF4	90	NOP		št
0043EFF5	8D55 DØ	LEA EDX,DWORD PTR SS:[EBP-30]		št
0043EFF8	3300	XOR EAX,EAX		ŠŤ
0043EFFA	E8 AD38FCFF	CALL 004028AC	dumpeado.004028AC	ŠŤ
0043EFFF	8B45 DØ	MOV EAX, DWORD PTR SS:[EBP-30]		št
0043F002	8D55_D4	LEA EDX, DWORD PTR SS:[EBP-2C]		št
0043F005	E8_6E71FCFF	CALL 00406178	dumpeado.00406178	št
0043F00A	8855 D4	MOV EDX, DWORD PTR SS: [EBP-2C]		01
0043F00D	A1_30564400	MOV EAX, DWORD PTR DS:[445630]		ES
0043F012	8300 30	ADD EAX,30		ĒČ
0043F015	B9 04F54300	MOV ECX,43F504	ASCII "Aspack.hlp"	
0043F01A	E8 D546FCFF	CALL 004036F4	dumpeado.004036F4	
0043F01F	A1 30564400	MOV EAX, DWORD PTR DS: [445630]		
0043F024	C740 5C 881300	(MOV DWORD PTR DS:[EAX+5C],1388		
0043F02B	8B45 FC	MOV EAX, DWORD PTR SS:[EBP-4]		
0043F02E	Ceso 0C030000	MOV BYTE PTR DS:[EAX+30C],0		
0043F035	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]		
0043F038	8880 E4020000	MOV EAX, DWORD PTR DS: [EAX+2E4]		
0043F03E	C640 20 00	MOV BYTE PTR DS:[EAX+20],0		
0043F042	3302	XOR EDX,EDX		
0043F044	8B45 FC	MOV EAX, DWORD PTR SS:[EBP-4]		
0043F047	8B80 7C020000	MOV EAX,DWORD PTR DS:[EAX+27C]		
0043F04D	E8 8240FDFF	CALL 004130D4	dumpeado.004130D4	

Bueno, yo le hice algún que otro cambio más jejeje

😂 ASPack 2.12					
ASPack Versión 2.12	Compresor de Win32 EXE, DLL, OCX ————————————————————————————————————				
Abrir archivo Comprimir Opciones Acerca de Ayuda					
E-Mail: <u>support</u>					
×××× Crackeado	por Aquml ****				
Alexey	Solodovnikov © 1998-2002				

Si se pulsa en donde pone **** Crackeado por Aguml **** te lleva a google

Bueno, lo hice para que lo entienda gente tan torpe como yo que empiecen desde O ya que la gran mayoría de la comunidad sabe manejarse en esto y no necesitan tantas imágenes.

Pos eso, espero que disfrutéis los Newbies tanto como yo cuando lo destripe.