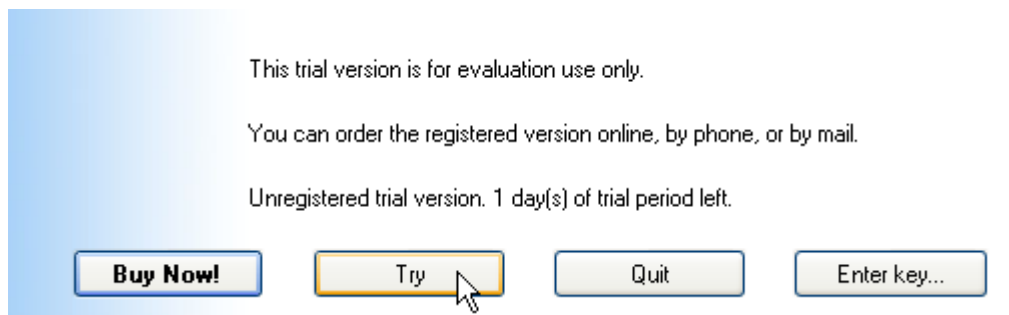
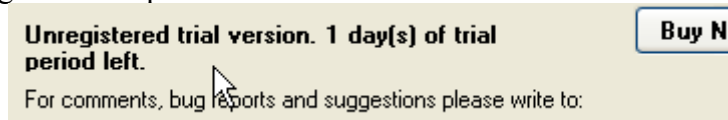


## Hazaña de un asprotect by Apuromafo



al pulsar try, pues tengo solo la opcion de usarlo.



Uso el unpacker:

Victim ImageBase - 00400000

Victim EntryPoint - 00001000

13:41:46 - unhandled break at 0242700b..

13:41:46 - asprotect detected..

13:41:46 - loading modules..

13:41:46 - unhandled break at 0242700b..

13:41:46 - asprotect detected..

13:41:46 - loading modules..

luego

\*vm(VM entry at )+scramle(ScrambledEntry at RVA:)+crc(Difference at RVA:)+Possible

EnvelopeCheck

13:42:06 - saving C:\archivos de programa\archivo.exe

luego de desempacado, busco una referencia

004ACBC4	. A1 64704B00	MOV EAX,DWORD PTR DS:[4B7064]	
004ACBC9	. 8038 00	CMF BYTE PTR DS:[EAX],0	
004ACBCC	. 0F94 DE000000	JS _facenor.004ACCB8	
004ACBD2	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
004ACBD5	. E8 E276F7FF	CALL _facenor.004242BC	
004ACBDA	. 8B40 0C	MOV EAX,DWORD PTR DS:[EAX+C]	
004ACBD0	. BA 0C000000	MOV EDI,0C	
004ACBE2	. E8 1120F7FF	CALL _facenor.0041EBF9	
004ACBE7	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
004ACBEA	. E8 CD76F7FF	CALL _facenor.004242BC	
004ACBEF	. 8B40 0C	MOV EAX,DWORD PTR DS:[EAX+C]	
004ACBF2	. 33D2	XOR EDI,EDI	
004ACBF4	. E8 171EF7FF	CALL _facenor.0041E910	
004ACBF9	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
004ACBFC	. E8 BB76F7FF	CALL _facenor.004242BC	
004ACCB1	. 8B40 0C	MOV EAX,DWORD PTR DS:[EAX+C]	
004ACCB4	. 8A15 84CD4A00	MOV DL,BYTE PTR DS:[4ACD84]	
004ACCB8	. E8 CD20F7FF	CALL _facenor.0041E9D0	
004ACCBF	. 68 90CD4A00	PUSH _facenor.004ACD90	
004ACCC4	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	0
004ACCC7	. 8B10	MOV EDI,DWORD PTR DS:[EAX]	
004ACCC9	. FF52 20	CALL DWORD PTR DS:[EDI+20]	
004ACCC1C	. 8BF0	MOV ESI,EAX	
004ACCC1E	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
004ACCC21	. E8 9676F7FF	CALL _facenor.004242BC	
004ACCC26	. BA B4CD4A00	MOV EDI,_facenor.004ACDB4	1
004ACCC2B	. E8 842CF7FF	CALL _facenor.0041F8B4	
004ACCC30	. 8D0440	LEA EAX,DWORD PTR DS:[EAX+EAX*2]	
004ACCC33	. 2BF0	SUB ESI,EAX	
004ACCC35	. 56	PUSH ESI	
004ACCC36	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
004ACCC39	. E8 7E76F7FF	CALL _facenor.004242BC	
004ACCC3E	. 33D2	XOR EDI,EDI	
004ACCC40	. 59	POP EAX	
004ACCC41	. E8 822BF7FF	CALL _facenor.0041F7C8	2
004ACCC46	. 68 C0CD4A00	PUSH _facenor.004ACDC0	
004ACCC4B	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
004ACCC4E	. 8B10	MOV EDI,DWORD PTR DS:[EAX]	
004ACCC50	. FF52 20	CALL DWORD PTR DS:[EDI+20]	
004ACCC53	. 8BF0	MOV ESI,EAX	
004ACCC55	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
004ACCC58	. E8 5F76F7FF	CALL _facenor.004242BC	
004ACCC5D	. BA B4CD4A00	MOV EDI,_facenor.004ACDB4	3
004ACCC62	. E8 4D2CF7FF	CALL _facenor.0041F8B4	
004ACCC67	. 05C0	ADD EAX,EAX	
004ACCC69	. 2BF0	SUB ESI,EAX	
004ACCC6B	. 56	PUSH ESI	
004ACCC6C	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
004ACCC6F	. E8 4876F7FF	CALL _facenor.004242BC	
004ACCC74	. 33D2	XOR EDI,EDI	
004ACCC76	. 59	POP EAX	
004ACCC77	. E8 4C2BF7FF	CALL _facenor.0041F7C8	3
004ACCC7C	. 68 DCCD4A00	PUSH _facenor.004ACDDC	
004ACCC7E	. 00000000	ASCII "unregistered version"	

encontrando unregistered version veo un salto, coloco find references y coloco bp

```
0049A38E MOV EAX,DWORD PTR DS:[4B7064]
0049A396 MOV EAX,DWORD PTR DS:[4B7064]
0049A8B6 MOV EAX,DWORD PTR DS:[4B7064]
0049A9FC MOV EAX,DWORD PTR DS:[4B7064]
0049ABE3 MOV EAX,DWORD PTR DS:[4B7064]
0049BF29 MOV EAX,DWORD PTR DS:[4B7064]
0049CB80 MOV EAX,DWORD PTR DS:[4B7064]
0049CBC4 MOV EAX,DWORD PTR DS:[4B7064]
```

al ejecutar en la segunda vez cae aquí:

0049A38E	> E8 3EFAFFFF	CALL _facenor.00499DC8	
0049A38A	84C0	TEST AL,AL	
0049A38C	75 08	JNZ SHORT _facenor.0049A396	
0049A38E	A1 64704B00	MOV EAX,DWORD PTR DS:[4B7064]	
0049A390	C500 01	MOV BYTE PTR DS:[EAX],1	
0049A392	A1 64704B00	MOV EAX,DWORD PTR DS:[4B7064]	
0049A394	8038 00	CMP BYTE PTR DS:[EAX],0	
0049A396	7F84 E5000000	JE _facenor.0049A489	
0049A3A4	330B	XOR EBX,EBX	
0049A3A6	68 00A44900	PUSH _facenor.0049A4D0	ASCII "Unregistered trial version. "
0049A3AB	8D55 F8	LEA EDI,DWORD PTR SS:[EBP-8]	
0049A3AE	A1 FC734B00	MOV EAX,DWORD PTR DS:[4B73FC]	
0049A3B0	8B00	MOV EAX,DWORD PTR DS:[EAX]	
0049A3B2	E8 32EFF6FF	CALL _facenor.004002E0	
0049A3B4	FF75 F8	PUSH DWORD PTR SS:[EBP-8]	
0049A3B6	68 F8A44900	PUSH _facenor.0049A4F8	ASCII " day(s) of trial period left."
0049A3C2	A1 BC704B00	MOV EAX,DWORD PTR DS:[4B70BC]	
0049A3C7	BA 03000000	MOV EDI,3	
0049A3CC	E8 0FAFF6FF	CALL _facenor.00400360	
0049A3D1	A1 FC734B00	MOV EAX,DWORD PTR DS:[4B73FC]	
0049A3D6	8338 00	CMP DWORD PTR DS:[EAX],0	
0049A3D9	7F 2F	JG SHORT _facenor.0049A480	
0049A3DB	A1 80704B00	MOV EAX,DWORD PTR DS:[4B7080]	
0049A3DD	8338 FF	CMP DWORD PTR DS:[EAX],-1	
0049A3E3	74 25	JE SHORT _facenor.0049A480	
0049A3E5	A1 BC704B00	MOV EAX,DWORD PTR DS:[4B70BC]	
0049A3EA	BA 20A54900	MOV EDI,_facenor.0049A520	
0049A3EF	E8 40CFF6FF	CALL _facenor.00400360	ASCII "This version has expired. Please click the "Buy Now" button to buy a full version
0049A3F4	A1 80744B00	MOV EAX,DWORD PTR DS:[4B7430]	
0049A3F9	8B00	MOV EAX,DWORD PTR DS:[EAX]	
0049A3FB	8B00 F8020000	MOV EAX,DWORD PTR DS:[EAX+2F8]	

luego lo fuerzo:

0049A382	EB 0F	JMP SHORT apuromaf.0049A393	
0049A384	56	PUSH ESI	
0049A385	E8 3EFAFFFF	CALL apuromaf.00499DC8	
0049A38A	84C0	TEST AL,AL	
0049A38C	90	NOP	
0049A38D	90	NOP	
0049A38E	A1 64704B00	MOV EAX,DWORD PTR DS:[4B7064]	
0049A393	C600 00	MOV BYTE PTR DS:[EAX],0	
0049A396	A1 64704B00	MOV EAX,DWORD PTR DS:[4B7064]	
0049A39B	8038 00	CMP BYTE PTR DS:[EAX],0	
0049A39E	E9 E6000000	JMP apuromaf.0049A489	salto a xor eax,eax
0049A3A3	90	NOP	
0049A3A4	33DB	XOR EBX,EBX	

adios nag , adios limitacion de dias y en el about, adios comentarios.

For comments, bug reports and suggestions please write to:

Los proximos chequeos son iguales, pero con el nop en el test al, escribe 1, luego no vuelve a reescribir este valor, por lo cual ejecutara registrado, hasta terminar el programa.

Programa caido, escrito del recuerdo,

Saludos APuromafo