

Firegraphic 10

By Apuromafo

27/04/2011
Crackslatinos
Apuromafo

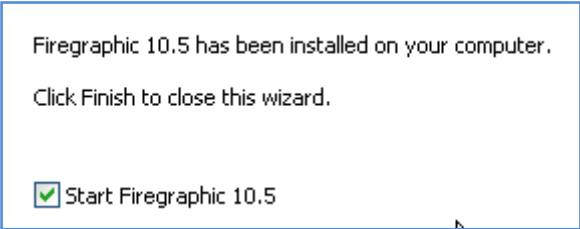
Programa:	Firegraphic 10.5 (c) Copyright Firegraphic.com 2001-2010	
Descripción:	Programa Multifacético para Imágenes	
Herramientas:	OllyDbg v.1.10, tiempo.	
Objetivos:	Anular la nag o registrar en el intento, y revisar que tal esta programado.	
Cracker: [Apuromafo]	Fecha: 26-04-2010	

INTRODUCCION:
Vine a dar una vuelta a la lista como iba todo, y converso un momento con un gran amigo, me comentaba que intento varias formas pero no logro quitar una nag, y este escrito es para ayudar a que pueda tener una referencia en caso que aun no lo resuelva.

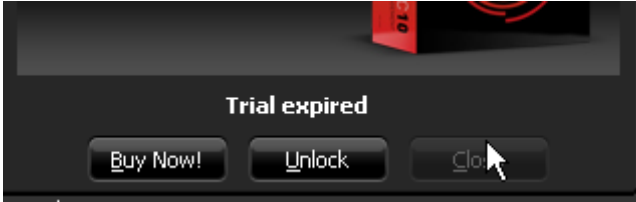
PREAMBULO:
Buen día, espero que los ánimos no cambien con el transcurso del tiempo, en este escrito, pues solo veremos un programa sin fin de lucro, y si fuera por claves, se buscan en la web, pero el objetivo de este no es la liberación de un nuevo cracked, sino mas bien conocer un programa mas por si alguien le interesa ver y de paso ver como se puede resolver o donde encontrar el dilema de nag o de estar registrado.

Lo que leía era esto:
Tengo una nag que no hay manera de encontrar. Es la nag inicial, e pensado en crear una pequeña aplicación que la cierre o la esconda puesto que no es una nag fuerte del tipo parent, sin embargo si pudieses echarle un vistazo a la nag la manera de eliminarla porque no soy capaz de detectarla.

Comienzo instalando la Aplicación:



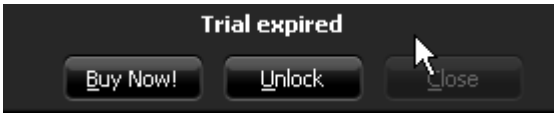
Elimino las ramas de REGEDIT puesto que quiero trabajar como expired:



Posicionado con un plugin llamado Windows

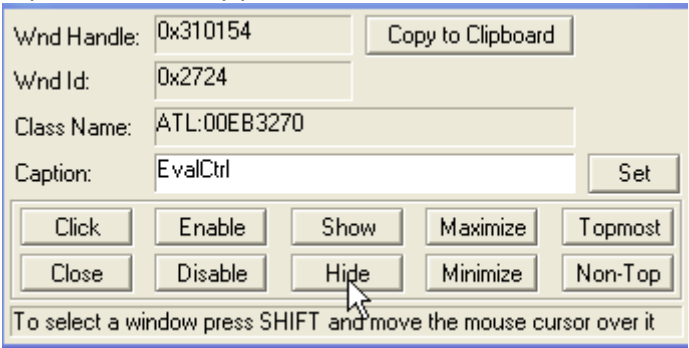
WindowJuggler plugin v0.06 BETA

Juggler Wnd Handle: [text box] Copy to



Pulso en el lugar que se muestra, me dice el

Caption "EvalCtrl" y pulso HIDE



Y la nag desaparece.

Por lo que la teoría de crear una aplicación que encuentre el handle del EVALCTRL y esconderlo y/o cerrarlo puede ser valido, con esto estaría listo la idea.
Por lo tanto, con la limitación de días -solo muestra la nag- y si la cierro "puedo seguir usando la aplicación inclusive mas del tiempo", es una nag que si no estuviera, seria full.

Comienzo a analizar un poco y utilizo Olly y busco el texto del Caption: y encuentro todo lo que debo analizar ID_REG /unreg y todo lo necesario .

0051C447	PUSH 0096B7C	UNICODE "ID_FILTERPROGRESSDLG_MSG1"
0051C8D9	PUSH 0096BD0	UNICODE "ID_FILTERPROGRESSDLG_MSG2"
0051CCC6	PUSH 0096C04	UNICODE "%s\\%s %s"
0051CD16	PUSH 0096C18	UNICODE "%s\\%s (%d) %s"
0051D5E5	PUSH 0096C34	UNICODE "ID_ABOUT"
0051D823	PUSH 008F244	UNICODE "Firegraphic"
0051D828	PUSH 0096C48	UNICODE "%s %d.%d.%d"
0051D838	PUSH 0096C60	UNICODE "ID_REGISTERED"
0051D95A	PUSH 0096C80	UNICODE "ID_UNREGISTERED"
0051DF5E	PUSH 0096CA0	UNICODE "ID_OUTPUTSETTINGDLG"
0051DFC2	PUSH 0091510	UNICODE "ID_OPTIONS_BTN"
0051E02B	PUSH 00914D8	UNICODE "ID_BROWSE_BTN"
0051E094	PUSH 0092E50	UNICODE "ID_USECURRENT_BTN"
0051E109	PUSH 0096CC8	UNICODE "ID_OUTPUTSETTINGDLG_1"
0051E184	PUSH 0096CF4	UNICODE "ID_OUTPUTSETTINGDLG_2"
0051E1FF	PUSH 0096D20	UNICODE "ID_OUTPUTSETTINGDLG_3"
0051E268	PUSH 0093310	UNICODE "ID_PREFIX_TITLE"
0051E2D7	PUSH 0096D4C	UNICODE "ID_OUTPUTSETTINGDLG_5"
0051E343	PUSH 0096D78	UNICODE "ID_OUTPUTSETTINGDLG_6"
0051E3AF	PUSH 0096DA4	UNICODE "ID_OUTPUTSETTINGDLG_7"
0051E41B	PUSH 0090B00	UNICODE "ID_OK"
0051E484	PUSH 008F114	UNICODE "ID_CANCEL"
0051E74A	PUSH 0091558	UNICODE "ID_PATHNOTEEXISTS"
0051E78B	PUSH 0090A58	UNICODE "APP"
0051EDD2	MOV DWORD PTR [EB2720],00906DC	UNICODE "At lAxWin90"
0051F880	PUSH 0096DF8	UNICODE "ID_EVAL_DLG_BUY"
0051F935	PUSH 0096E18	UNICODE "ID_EVAL_DLG_UNLOCK"
0051F9EB	PUSH 0096E40	UNICODE "ID_EVAL_DLG_CLOSE"
0051FB22	PUSH 0096E64	UNICODE "about:blank"
0051FB7B	PUSH 0096E7C	UNICODE "eval\\index.html"
0051FB87	PUSH 0096E9C	UNICODE "%s\\%s"
005201A7	PUSH 0092CEC	UNICODE "ID_REGISTERDLG_MSG2"
00520215	PUSH 0092C9C	UNICODE "ID_REGISTERDLG_MSG3"
00520233	PUSH 0092CC4	UNICODE "ID_REGISTERDLG_MSG4"
005202EF	PUSH 0096EA8	UNICODE "ID_EVAL_DLG_TRIAL_PERIOD_LEFT"
0052035A	PUSH 0096EE4	UNICODE "ID_EVAL_DLG_EXPIRED"
00527A98	MOV DWORD PTR [EBP-78],0096F10	UNICODE "EvalCtrl"
00527EF5	MOV DWORD PTR [EAX+3C],00A610C	ASCII "PyR"

Al entrar Veo claramente que estas 2 comparaciones son las que hacen que decida el valor de esto, posiblemente una tenga relación a registrado, y otra a alguna handle.

005279E8	833D ACCEC0	CMP DWORD PTR [ECAEAC],1	
005279EF	75 0D	JNZ SHORT 005279FE	Firegrap.005279FE
005279F1	833D FCAEEC0	CMP DWORD PTR [ECFEFC],0	
005279F8	0F85 66010000	JNZ 00527B64	Firegrap.00527B64
005279FE	C745 E0 0000	MOV [LOCAL.8],0	
00527A05	C745 E4 0000	MOV [LOCAL.7],0	
00527A0C	C745 E8 4001	MOV [LOCAL.6],140	
00527A13	C745 EC 4001	MOV [LOCAL.5],140	
00527A1A	68 0C030000	PUSH 38C	
00527A1F	E8 73536200	CALL 00B4CD97	Firegrap.00B4CD97
00527A24	83C4 04	ADD ESP,4	
00527A27	8945 D8	MOV [LOCAL.10],EAX	msvcrt.77C28DCC
00527A2A	C745 FC 0000	MOV [LOCAL.1],0	
00527A31	837D D8 00	CMP [LOCAL.10],0	
00527A35	74 10	JE SHORT 00527A47	Firegrap.00527A47
00527A37	8B4D D8	MOV ECX,[LOCAL.10]	Firegrap.00CC57E8
00527A3A	E8 917AFFFF	CALL 0051F4D0	Firegrap.0051F4D0
00527A3F	8985 DCFEFF	MOV [LOCAL.73],EAX	msvcrt.77C28DCC
00527A45	EB 0A	JMP SHORT 00527A51	Firegrap.00527A51
00527A47	C785 DCFEFF	MOV [LOCAL.73],0	
00527A51	8B95 DCFEFF	MOV EDX,[LOCAL.73]	Firegrap.00410045
00527A57	8955 DC	MOV [LOCAL.9],EDX	webcheck.74AED000
00527A5A	C745 FC FFFF	MOV [LOCAL.1],-1	
00527A61	8B85 E8FEFF	MOV EAX,[LOCAL.70]	Firegrap.004D005C
00527A67	8B4D DC	MOV ECX,[LOCAL.9]	
00527A6A	8948 3C	MOV DWORD PTR [EAX+3C],ECX	msvcrt._except_handler3
00527A6D	8D55 98	LEA EDI,[LOCAL.26]	
00527A70	8955 A8	MOV [LOCAL.22],EDI	webcheck.74AED000
00527A73	8B45 A8	MOV EAX,[LOCAL.22]	
00527A76	C700 24270000	MOV DWORD PTR [EAX],2724	
00527A7C	8D4D 94	LEA ECX,[LOCAL.27]	
00527A7F	894D A4	MOV [LOCAL.23],ECX	msvcrt._except_handler3
00527A82	8B55 A4	MOV EDX,[LOCAL.23]	
00527A85	8D45 E0	LEA EAX,[LOCAL.8]	
00527A88	8902	MOV DWORD PTR [EDX],EAX	msvcrt.77C28DCC
00527A8A	C745 80 0000	MOV [LOCAL.32],0	
00527A91	C745 84 0000	MOV [LOCAL.31],56000000	
00527A98	C745 88 106F	MOV [LOCAL.30],0096F10	UNICODE "EvalCtrl"
00527A9F	8B8D E8FEFF	MOV ECX,[LOCAL.70]	Firegrap.004D005C

Si cambio a 5279e8 a cero, desaparece la nag. Programa registrado diría yo.
Este Eval CTRL sera nuestra referencia.

Busco el origen del recurso:

0042B179	CALL NEAR DWORD PTR [C7C3B8]	kernel32.FindResourceW
0042B1CE	CALL NEAR DWORD PTR [C7C3BC]	kernel32.FindResourceExW
0042B269	CALL NEAR DWORD PTR [C7C3BC]	kernel32.FindResourceExW
0042B3C0	CALL NEAR DWORD PTR [C7C40C]	kernel32.GetProcAddress

Y encuentro como crea app.dat ,y algunas referencias importantes como recurso en si.
Pero si se borra, quizás no cargaria bien las skin o algun recurso.

Volviendo a la nag Pienso en cerrarla , una forma simple de cerrarla es forzar su destruccion con destroy window

0054C391	52	PUSH EDX	hWnd = 01AC79F0
0054C392	FF15 58C7C701	CALL NEAR DWORD PTR [C7C758]	DestroyWindow
0054C398	8B85 C0FEFFFF	MOV EAX,[LOCAL.80]	
0054C39E	8B48 3C	MOV ECX,DWORD PTR [EAX+3C]	
0054C3A1	894D C8	MOV [LOCAL.14],ECX	
0054C3A4	8B55 C8	MOV EDX,[LOCAL.14]	
0054C3A7	8955 CC	MOV [LOCAL.13],EDX	
0054C3AA	837D CC 00	CMP [LOCAL.13],0	
0054C3AE	74 17	JE SHORT 0054C3C7	Firegrap.0054C3C7
0054C3B0	6A 01	PUSH 1	

Si reviso el lugar indicado es cuando ya tiene como parametro edx, establecido en 54c2b8 , el salto hace forzar a la eliminacion de la nag.

0054C275	C785 78FFFFFF	MOV [LOCAL.34],0D96F10	UNICODE "EvalCtrl"
0054C27F	8B85 C0FEFFFF	MOV EAX,[LOCAL.80]	
0054C285	8B48 C8	MOV ECX,DWORD PTR [EAX+38]	
0054C288	898D 7CFFFFFF	MOV [LOCAL.33],ECX	
0054C28E	8B95 C0FEFFFF	MOV EDX,[LOCAL.80]	
0054C294	8B42 3C	MOV EAX,DWORD PTR [EDX+3C]	Firegrap.00DA6054
0054C297	8945 80	MOV [LOCAL.32],EAX	
0054C29A	833D A032EB01	CMP DWORD PTR [EB32A0],0	
0054C2A1	75 0A	JNZ SHORT 0054C2AD	Firegrap.0054C2AD
0054C2A3	C705 A032EB01	MOV DWORD PTR [EB32A0],0	
0054C2AD	0FB64D 8F	MOVZX ECX,BYTE PTR [EBP-71]	
0054C2B1	51	PUSH ECX	Arg5 = 000001F0
0054C2B2	8B55 80	MOV EDX,[LOCAL.32]	
0054C2B5	83C2 20	ADD EDX,20	
0054C2B8	52	PUSH EDX	Arg4 = 01AC79F0
0054C2B9	68 7032EB00	PUSH 0EB3270	Arg3 = 00EB3270
0054C2BE	68 F480EC00	PUSH 0EC80F4	Arg2 = 00EC80F4
0054C2C3	68 BC80EC00	PUSH 0EC80BC	Arg1 = 00EC80BC
0054C2C8	E8 83BE0C00	CALL 00618150	Firegrap.00618150
0054C2CD	83C4 14	ADD ESP,14	
0054C2D0	66:8945 90	MOV WORD PTR [EBP-70],AX	
0054C2D4	83BD 74FFFFFF	CMP [LOCAL.35],0	
0054C2D8	E9 B1000000	JMP 0054C391	destruye la ventana eval CTRL

Ya existe la nag y se puede destruir, pero quiero ver si encuentro los dias,

Pruebo con GetSystemTimeAsFileTime

00B522BE	8BFF	MOV EDI,EDI	
00B522C0	55	PUSH EBP	
00B522C1	8BEC	MOV EBP,ESP	
00B522C3	51	PUSH ECX	
00B522C4	51	PUSH ECX	
00B522C5	8D45 F8	LEA EAX,[LOCAL.2]	
00B522C8	50	PUSH EAX	pFileTime = 4BC04B9F
00B522C9	FF15 CCC3C701	CALL NEAR DWORD PTR [C7C3CC]	GetSystemTimeAsFileTime
00B522CF	8B45 F8	MOV EAX,[LOCAL.2]	Firegrap.00C69444
00B522D2	8B4D FC	MOV ECX,[LOCAL.1]	
00B522D5	6A 00	PUSH 0	
00B522D7	05 0080C12A	ADD EAX,2AC18000	

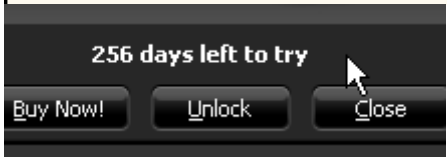
Y claramente esta api de tiempo es verificado solo cuando ECAEAC no es cero, por ende, si cambio el salto NO HAY NAG.

0054C163	83E9 3C	SUB ECX,3C	
0054C166	E8 E5880200	CALL 00574A50	Firegrap.00574A50
0054C168	833D ACAEEC01	CMP DWORD PTR [ECAEAC],0	
0054C172	0F84 F5010001	JE 0054C36D	Firegrap.0054C36D
0054C178	6A 00	PUSH 0	
0054C17A	E8 3F616000	CALL 00B522BE	api de tiempo!!
0054C17F	83C4 04	ADD ESP,4	

Buscando un poco donde escribe el valor y llego a mirar este lugar, los calls estan ordenados, y demuestra todo lo que hace como trial o registrado:

00583B44	FF15 68B5C701	CALL NEAR DWORD PTR [C7C3CC]	shell32.ShGetDesktopFolder
00583B4A	B9 18AEEC00	MOV ECX,0ECAE18	tiempo transcurrido por startA (valor en regedit)
00583B4F	E8 4CEA0400	CALL 005D2600	almacena los dias?
00583B54	A3 C0AEEC00	MOV DWORD PTR [ECAEC0],EAX	
00583B59	B9 18AEEC00	MOV ECX,0ECAE18	toma en cuanta las variables nombre, serial actualizaciones
00583B5E	E8 CDEA0400	CALL 005D2890	
00583B63	6A 01	PUSH 1	
00583B65	B9 18AEEC00	MOV ECX,0ECAE18	
00583B6A	E8 A1DE0400	CALL 005D1A70	posible zona de comparacion serial
00583B6F	833D ACAEEC01	CMP DWORD PTR [ECAEAC],0	Firegrap.00583BE2
00583B76	75 0A	JNZ SHORT 00583BE2	?? lugar innecesario... si es o no es igual cae de la misma forma
00583B78	B9 18AEEC00	MOV ECX,0ECAE18	Firegrap.005D1A20
00583B7D	E8 3EDE0400	CALL 005D1A20	
00583B82	B9 18AEEC00	MOV ECX,0ECAE18	
00583B87	E8 3479C8FF	CALL 0040B520	Firegrap.0040B520
00583B8C	B9 18AEEC00	MOV ECX,0ECAE18	
00583B91	E8 DA410500	CALL 005D7D00	
00583B96	68 05800000	PUSH 8005	
00583B9B	8D85 04FAFFF	LEA EAX,DWORD PTR [EBP-5FC]	
00583BA0	50	PUSH EAX	
00583BA2	B9 18AEEC00	MOV ECX,0ECAE18	
00583BA7	E8 E4410000	CALL 00587DF0	
00583BAC	6A 00	PUSH 0	
00583BAE	6A 00	PUSH 0	
00583BB0	68 04010000	PUSH 104	
00583BB3	8D8D E4E9FFF	LEA ECX,DWORD PTR [EBP-161C]	
00583BB8	51	PUSH ECX	
00583BBE	68 580AD900	PUSH 0D90A58	
00583BC3	B9 18AEEC00	MOV ECX,0ECAE18	
00583BC8	E8 15C20800	CALL 0063FE40	
00583BCD	68 9880D900	PUSH 0D98898	
00583BD2	8D95 E4E9FFF	LEA EDX,DWORD PTR [EBP-161C]	

Modify dword at 00ECA...
Hexadecimal 00000100
Signed 256
Unsigned 256
OK Cancel



Confirmado ecae0 maneja las variables según el lugar llamado .

Ahora se como quitar la nag, como extender los días (hacerlo registrado), me falta revisar el call si es el serial o no Leo el readme.txt

=====

Serial Numbers

=====

1. You can find the 16-character serial number (e.g. xxxxxxxxxxxxxxxx) on the receipt page from the online store, and in the e-mail confirmation you received. You will be asked for this number after installing


2. If your new 16-character serial number does not work, please contact at <http://www.firegraphic.com/contact/> for assistance.

1) el serial esta construido de 16 valores, pulso el unlock si no es valido, muestra la nag, pasa por las variables de registro y si es invalido, pues se perdio la licencia!!!

0054C166	E8 E580200	CALL Firegrap.00574A50
0054C16B	833D AC8EEC00	CMP DWORD PTR DS:[EC8EAC],0
0054C172	0F84 F5010000	JE Firegrap.0054C360
0054C178	C705 AC8EEC00	MOV DWORD PTR DS:[EC8EAC],0
0054C182	E9 E6010000	JMP Firegrap.0054C360
0054C187	90	NOP
0054C188	8B15 C88EEC00	MOV EDX,DWORD PTR DS:[EC8EAC]



Y PULSO unlock

 Thank you for purchasing Firegraphic!

Please enter the unlock code below:

Name:

Company:

Key:

Website: www.firegraphic.com

Pulso pausa, alt+k, y retrocedo al mensaje de invalido

Llego al primer dialogo

004CAF13	E9 DF000000	JMP 004CAFF7	Sin_limi.004CAFF7
004CAF18	68 542CD900	PUSH 0D92C54	Unicode "ID_REGISTRATION"
004CAF1D	8D55 BC	LEA EDX,DWORD PTR [EBP-44]	
004CAF20	52	PUSH EDX	
004CAF21	B9 18AEEC00	MOV ECX,0EC8E18	
004CAF26	E8 55D71500	CALL 00620680	Sin_limi.00620680
004CAF2B	9995 B8FEFFFF	MOV DWORD PTR [EBP-148],EAX	
004CAF31	8B85 B8FEFFFF	MOV EAX,DWORD PTR [EBP-148]	
004CAF37	8985 F4FEFFFF	MOV DWORD PTR [EBP-10C],EAX	
004CAF3D	C745 FC 0C000000	MOV DWORD PTR [EBP-4],0C	
004CAF44	68 EC2CD900	PUSH 0D92CEC	Unicode "ID_REGISTERDLG_MSG2"
004CAF49	8D4D B4	LEA ECX,DWORD PTR [EBP-4C]	
004CAF4C	51	PUSH ECX	
004CAF4D	B9 18AEEC00	MOV ECX,0EC8E18	
004CAF52	E8 29D71500	CALL 00620680	Sin_limi.00620680
004CAF57	9995 B4FEFFFF	MOV DWORD PTR [EBP-14C],EAX	
004CAF5D	8B95 B4FEFFFF	MOV EDX,DWORD PTR [EBP-14C]	
004CAF63	8995 E8FEFFFF	MOV DWORD PTR [EBP-118],EDX	
004CAF69	C645 FC 0D	MOV BYTE PTR [EBP-4],0D	
004CAF6D	8B85 F4FEFFFF	MOV EAX,DWORD PTR [EBP-10C]	
004CAF73	8B08	MOV ECX,DWORD PTR [EAX]	
004CAF75	898D F0FEFFFF	MOV DWORD PTR [EBP-110],ECX	
004CAF7B	6A 40	PUSH 40	
004CAF7D	51	PUSH ECX	
004CAF7E	9B04	MOV EDI,ESP	
004CAF80	8965 C0	MOV DWORD PTR [EBP-40],ESP	
004CAF83	8995 ECFEFFFF	MOV DWORD PTR [EBP-114],EDX	
004CAF89	8B85 ECFEFFFF	MOV EAX,DWORD PTR [EBP-114]	
004CAF8F	8B8D F0FEFFFF	MOV ECX,DWORD PTR [EBP-110]	
004CAF95	8908	MOV DWORD PTR [EAX],ECX	
004CAF97	8B95 E8FEFFFF	MOV EDX,DWORD PTR [EBP-118]	
004CAF9D	8B02	MOV EAX,DWORD PTR [EDX]	
004CAF9F	8985 E4FEFFFF	MOV DWORD PTR [EBP-11C],EAX	
004CAFA5	51	PUSH ECX	
004CAFA6	8BCC	MOV ECX,ESP	
004CAFA8	8965 B8	MOV DWORD PTR [EBP-48],ESP	
004CAFAB	898D E0FEFFFF	MOV DWORD PTR [EBP-120],ECX	
004CAFAD	8B95 E0FEFFFF	MOV EDX,DWORD PTR [EBP-120]	
004CAFAD	8B85 E4FEFFFF	MOV EAX,DWORD PTR [EBP-11C]	
004CAFBD	8902	MOV DWORD PTR [EDX],EAX	
004CAFBD	8B8D D4FEFFFF	MOV ECX,DWORD PTR [EBP-12C]	
004CAFBD	8B51 04	MOV EDX,DWORD PTR [ECX+4]	
004CAFCD	52	PUSH EDX	
004CAFCE	E9 62DDF9FF	CALL 00468D30	Sin_limi.00468D30
004CAFCE	83C4 10	ADD ESP,10	
004CAF01	C645 FC 0E	MOV BYTE PTR [EBP-4],0E	
004CAF05	C645 FC 0C	MOV BYTE PTR [EBP-4],0C	
004CAF09	8D4D B4	LEA ECX,DWORD PTR [EBP-4C]	

Y lo que condiciona aquellos mensajes son una comparación con un valor

004CAE27	833D AC8EEC00	CMP DWORD PTR [EC8EAC],4
004CAE2F	0F85 F4000000	JNZ 004C0F18

Viendo el valor, puede ser comparado en bastantes lugares, pero en solo 2 se escribe el valor

004CABDD	MOV	DWORD	PTR	[ECX:EAX], EAX	
004CABE2	CMP	DWORD	PTR	[ECX:EAX], 0	DS:[00ECX:EAX]=00000000
004CAC45	CMP	DWORD	PTR	[ECX:EAX], 0	DS:[00ECX:EAX]=00000000
004CAD36	CMP	DWORD	PTR	[ECX:EAX], 2	DS:[00ECX:EAX]=00000000
004CAE27	CMP	DWORD	PTR	[ECX:EAX], 4	DS:[00ECX:EAX]=00000000
0051D873	CMP	DWORD	PTR	[ECX:EAX], 0	DS:[00ECX:EAX]=00000000
0051FF87	CMP	DWORD	PTR	[ECX:EAX], 0	DS:[00ECX:EAX]=00000000
0052019E	CMP	DWORD	PTR	[ECX:EAX], 3	DS:[00ECX:EAX]=00000000
0052020C	CMP	DWORD	PTR	[ECX:EAX], 2	DS:[00ECX:EAX]=00000000
0052027A	CMP	DWORD	PTR	[ECX:EAX], 4	DS:[00ECX:EAX]=00000000
005202D9	CMP	DWORD	PTR	[ECX:EAX], 1	DS:[00ECX:EAX]=00000000
0052797E	CMP	DWORD	PTR	[ECX:EAX], 0	DS:[00ECX:EAX]=00000000
005279E8	CMP	DWORD	PTR	[ECX:EAX], 1	DS:[00ECX:EAX]=00000000
0054C16B	CMP	DWORD	PTR	[ECX:EAX], 0	DS:[00ECX:EAX]=00000000
00583BCF	CMP	DWORD	PTR	[ECX:EAX], 0	DS:[00ECX:EAX]=00000000
005D82F0	MOV	DWORD	PTR	[ECX:EAX], 4	DS:[00ECX:EAX]=00000000

004CABD3	B9 18AEEC00	MOV ECX,0ECAE18	
004CABD8	E8 936E1000	CALL 005D1A70	ojo 1
004CABDD	A3 ACAEEC00	MOV DWORD PTR [ECX],EAX	
004CABE2	83D0 ACAEEC00	CMP DWORD PTR [ECX],0	
004CABE9	75 5A	JNZ SHORT 004CAC45	Si limit.004CAC45
004CABF0	B9 18AEEC00	MOV ECX,0ECAE18	

Tengo el nombre , la compañía y el serial que deben estar en upercase ->mayúsculas

Primera verificación que no falten valores

005D1A7E	8B45 D8	MOV ECX, DWORD PTR [EBP-28]	
005D1A81	05 A0000000	ADD EAX, 0A0	
005D1A86	50	PUSH EAX	
005D1A87	E8 A434E7FF	CALL 00444F30	Sin_limi.00444F30
005D1A8C	83C4 08	ADD ESP, 8	
005D1A8F	0FB6C8	MOVZX ECX, AL	
005D1A92	85C9	TEST ECX, ECX	Sin_limi.00ECAE18
005D1A94	74 09	JE SHORT 005D1A9F	Sin_limi.005D1A9F
005D1A96	B8 01000000	MOV EAX, 1	
005D1A9B	EB 63	JMP SHORT 005D1B00	Sin_limi.005D1B00
005D1A9D	EB 25	JMP SHORT 005D1AC4	Sin_limi.005D1AC4
005D1A9F	68 5C9DD800	PUSH 0089D5C	
005D1AA4	8B55 D8	MOV EDI, DWORD PTR [EBP-28]	
005D1AA7	81C2 98000000	ADD EDI, 98	
005D1AAD	52	PUSH EDI	Sin_limi.00ECAE18
005D1AAE	E8 7D34E7FF	CALL 00444F30	Sin_limi.00444F30
005D1AB3	83C4 08	ADD ESP, 8	
005D1AB6	0FB6C0	MOVZX EAX, AL	
005D1AB9	85C0	TEST EAX, EAX	
005D1ABB	74 07	JE SHORT 005D1AC4	Sin_limi.005D1AC4
005D1ABD	B8 03000000	MOV EAX, 3	
005D1AC2	EB 3C	JMP SHORT 005D1B00	Sin_limi.005D1B00
005D1AC4	8B4D D8	MOV ECX, DWORD PTR [EBP-28]	
005D1AC7	8B91 A0000000	MOV EDI, DWORD PTR [ECX+A0]	
005D1ACD	9555 E4	MOV DWORD PTR [EBP-1C], EDI	Sin_limi.00ECAE18
005D1AD0	8B45 D8	MOV EAX, DWORD PTR [EBP-28]	
005D1AD3	8B88 9C000000	MOV ECX, DWORD PTR [EAX+9C]	
005D1AD9	934D E0	MOV DWORD PTR [EBP-20], ECX	Sin_limi.00ECAE18
005D1ADC	8B55 D8	MOV EDI, DWORD PTR [EBP-28]	
005D1ADF	8B82 98000000	MOV EAX, DWORD PTR [EDI+98]	
005D1AE5	9345 DC	MOV DWORD PTR [EBP-24], EAX	
005D1AE8	8B4D 08	MOV ECX, DWORD PTR [EBP+8]	
005D1AEB	51	PUSH ECX	Sin_limi.00ECAE18
005D1AEC	8B55 E4	MOV EDI, DWORD PTR [EBP-1C]	
005D1AEF	52	PUSH EDI	Sin_limi.00ECAE18
005D1AF0	8B45 E0	MOV EAX, DWORD PTR [EBP-20]	Sin_limi.004C0000
005D1AF3	50	PUSH EAX	
005D1AF4	8B4D DC	MOV ECX, DWORD PTR [EBP-24]	Sin_limi.004B004F
005D1AF7	51	PUSH ECX	Sin_limi.00ECAE18
005D1AF8	8B4D D8	MOV ECX, DWORD PTR [EBP-28]	
005D1AFB	E8 10000000	CALL 005D1B10	Sin_limi.005D1B10
005D1B00	8BE5	MOV ESP, EBP	
005D1B02	5D	POP EBP	
005D1B03	C2 0400	RETN 4	

005D1AB7	85C0	TEST EAX,EAX	
005D1AB8	74 07	JE SHORT 005D1AC4	Sin_limi.005D1AC4
005D1ABD	B8 03000000	MOV EAX,3	
005D1AC2	EB 3C	JMP SHORT 005D1B00	Sin_limi.005D1B00
005D1AC4	8B4D D8	MOV ECX,DWORD PTR [EBP-28]	Sin_limi.00ECAE18
005D1AC7	8B91 A0000000	MOV EDX,DWORD PTR [ECX+A0]	
005D1ACD	8955 E4	MOV DWORD PTR [EBP-1C],EDX	
005D1AD0	8B45 D8	MOV EAX,DWORD PTR [EBP-28]	Sin_limi.00ECAE18
005D1AD3	8B88 9C000000	MOV ECX,DWORD PTR [EAX+9C]	Sin_limi.0067006E
005D1AD9	894D E0	MOV DWORD PTR [EBP-20],ECX	Sin_limi.00ECAE18
005D1ADC	8B55 D8	MOV EDX,DWORD PTR [EBP-28]	Sin_limi.00ECAE18
005D1ADF	8B82 98000000	MOV EAX,DWORD PTR [EDX+98]	Sin_limi.00410045
005D1AE5	8945 DC	MOV DWORD PTR [EBP-24],EAX	
005D1AE8	8B4D 08	MOV ECX,DWORD PTR [EBP+8]	
005D1AEB	51	PUSH ECX	Sin_limi.00ECAE18
005D1AEC	8B55 E4	MOV EDX,DWORD PTR [EBP-1C]	
005D1AEF	52	PUSH EDX	
005D1AF0	8B45 E0	MOV EAX,DWORD PTR [EBP-20]	
005D1AF3	50	PUSH EAX	
005D1AF4	8B4D DC	MOV ECX,DWORD PTR [EBP-24]	
005D1AF7	51	PUSH ECX	Sin_limi.00ECAE18
005D1AF8	8B4D D8	MOV ECX,DWORD PTR [EBP-28]	Sin_limi.00ECAE18
005D1AFB	E8 10000000	CALL 005D1B10	ojo 2
005D1B00	8BE5	MOV ESP,EBP	
005D1B02	5D	POP EBP	0016D990
005D1B03	C2 0400	RETN 4	
005D1B06	CC	INT3	

El call llega a otra mas

005D1B0F	CC	INT3	
005D1B10	55	PUSH EBP	
005D1B11	8BEC	MOV EBP,ESP	
005D1B13	51	PUSH ECX	Sin_limi.00ECAE18
005D1B14	894D FC	MOV DWORD PTR [EBP-4],ECX	Sin_limi.00ECAE18
005D1B17	8B45 14	MOV EAX,DWORD PTR [EBP+14]	
005D1B1A	50	PUSH EAX	
005D1B18	8B4D 10	MOV ECX,DWORD PTR [EBP+10]	
005D1B1E	51	PUSH ECX	Sin_limi.00ECAE18
005D1B1F	8B55 0C	MOV EDX,DWORD PTR [EBP+C]	
005D1B22	52	PUSH EDX	
005D1B23	8B45 08	MOV EAX,DWORD PTR [EBP+8]	
005D1B26	50	PUSH EAX	
005D1B27	8B4D FC	MOV ECX,DWORD PTR [EBP-4]	
005D1B2A	E8 41000000	CALL 005D1B70	Sin_limi.005D1B70
005D1B2F	8B4D FC	MOV ECX,DWORD PTR [EBP-4]	
005D1B32	8981 94000000	MOV DWORD PTR [ECX+94],EAX	
005D1B38	8B55 FC	MOV EDX,DWORD PTR [EBP-4]	
005D1B3B	83BA 94000000	CMP DWORD PTR [EDX+94],0	
005D1B42	74 11	JE SHORT 005D1B55	Sin_limi.005D1B55
005D1B44	8B4D FC	MOV ECX,DWORD PTR [EBP-4]	
005D1B47	E8 B40A0000	CALL 005D2600	Sin_limi.005D2600
005D1B4C	8B4D FC	MOV ECX,DWORD PTR [EBP-4]	
005D1B4F	8981 A8000000	MOV DWORD PTR [ECX+A8],EAX	
005D1B55	8B55 FC	MOV EDX,DWORD PTR [EBP-4]	
005D1B58	8B82 94000000	MOV EAX,DWORD PTR [EDX+94]	
005D1B5E	8BE5	MOV ESP,EBP	
005D1B60	5D	POP EBP	0016D990
005D1B61	C2 1000	RETN 10	
005D1B64	CC	INT3	
005D1B65	CC	INT3	

Y comienza la verificación del serial , vemos la comparación del largo con 10h/16d ó 0Ch/12d.

005D1B6C	CC	INT3	
005D1B6D	CC	INT3	
005D1B6E	CC	INT3	
005D1B6F	CC	INT3	
005D1B70	55	PUSH EBP	
005D1B71	8BEC	MOV EBP,ESP	
005D1B73	6A FF	PUSH -1	
005D1B75	68 6630C400	PUSH 0C43066	
005D1B7A	64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	
005D1B80	50	PUSH EAX	
005D1B81	81EC AC050000	SUB ESP,5AC	
005D1B87	A1 544AE600	MOV EAX,DWORD PTR [E64AE4]	
005D1B8C	33C5	XOR EAX,EBP	
005D1B8E	8945 F0	MOV DWORD PTR [EBP-10],EAX	
005D1B91	50	PUSH EAX	
005D1B92	8D45 F4	LEA EAX,DWORD PTR [EBP-C]	
005D1B95	64:A3 00000000	MOV DWORD PTR FS:[0],EAX	
005D1B98	898D 50FAFFFF	MOV DWORD PTR [EBP-50],ECX	Sin_limi.00ECAE18
005D1BA1	8B45 10	MOV EAX,DWORD PTR [EBP+10]	
005D1BA4	50	PUSH EAX	
005D1BA5	E8 2BAF5700	CALL 00B4CAD5	Sin_limi.00B4CAD5
005D1BA9	83C4 04	ADD ESP,4	
005D1BAD	8985 58FFFFFF	MOV DWORD PTR [EBP-A8],EAX	
005D1BB3	83BD 58FFFFFF	CMP DWORD PTR [EBP-A8],10	
005D1BB8	74 13	JE SHORT 005D1BCF	Sin_limi.005D1BCF
005D1BBC	83BD 58FFFFFF	CMP DWORD PTR [EBP-A8],0C	
005D1BC3	74 0A	JE SHORT 005D1BCF	Sin_limi.005D1BCF
005D1BC5	B8 03000000	MOV EAX,3	
005D1BCA	E9 12040000	JMP 005D1FE1	Sin_limi.005D1FE1
005D1BCF	6A 04	PUSH 4	
005D1BD1	8B4D 10	MOV ECX,DWORD PTR [EBP+10]	

En el primer traceo

Primer check

005D1BAA	.	83C4 04	ADD ESP,4	
005D1BAD	.	8985 58FFFFFF	MOV [LOCAL.42],EAX	
005D1BB3	.	83BD 58FFFFFF	>CMP [LOCAL.42],10	
005D1BBA	.	74 13	JE SHORT 005D1BCF	/Si ES 16, pasa por Zona check
005D1BBC	.	83BD 58FFFFFF	>CMP [LOCAL.42],0C	/si es 12, no pasa por este
005D1BC3	.	74 0A	JE SHORT 005D1BCF	
005D1BC5	.	B8 03000000	MOV EAX,3	
005D1BCA	.	E9 12040000	JMP 005D1FE1	

Zona check

005D1D27	.	05 6C070000	ADD EAX,76C	
005D1D2C	.	3B85 A8FAFFF	CMP EAX,[LOCAL.342]	; 2009 vs /2010
005D1D32	.	75 14	JNZ SHORT 005D1D48	; Sin_limi.005D1D48
005D1D34	.	8B8D B8FAFFF	MOV ECX,[LOCAL.338]	
005D1D3A	.	8B51 10	MOV EDX,DWORD PTR [ECX+10]	
005D1D3D	.	83C2 01	ADD EDX,1	
005D1D40	.	3B95 A4FAFFF	CMP EDX,[LOCAL.343]	
005D1D46	.	7F 3C	JG SHORT 005D1D84	; Sin_limi.005D1D84
005D1D48	>	8B85 B8FAFFF	MOV EAX,[LOCAL.338]	
005D1D4E	.	8B48 14	MOV ECX,DWORD PTR [EAX+14]	
005D1D51	.	81C1 6C070000	ADD ECX,76C	
005D1D57	.	3B8D A8FAFFF	CMP ECX,[LOCAL.342]	; 2009 vs /2010

```
005D1D5D |. 75 2F      JNZ SHORT 005D1D8E          ; Sin_limi.005D1D8E
005D1D5F |. 8B95 B8FAFFFF MOV EDX,[LOCAL.338]
005D1D65 |. 8B42 10      MOV EAX,DWORD PTR [EDX+10]
005D1D68 |. 83C0 01      ADD EAX,1
005D1D6B |. 3B85 A4FAFFFF CMP EAX,[LOCAL.343]
005D1D71 |. 75 1B      JNZ SHORT 005D1D8E          ; Sin_limi.005D1D8E
005D1D73 |. 8B8D B8FAFFFF MOV ECX,[LOCAL.338]
005D1D79 |. 8B51 0C      MOV EDX,DWORD PTR [ECX+C]
005D1D7C |. 3B95 A0FAFFFF CMP EDX,[LOCAL.344]
005D1D82 |. 7E 0A      JLE SHORT 005D1D8E          ; Sin_limi.005D1D8E
005D1D84 |> B8 02000000  MOV EAX,2 /chico malo
005D1D89 |. E9 53020000  JMP 005D1FE1          ; Sin_limi.005D1FE1
```

recorta los trozos del serial

```
005D1BCF |> \6A 04      PUSH 4          ; /Arg3 = 00000004
005D1BD1 |. 8B4D 10      MOV ECX,[ARG.3]          ; |
005D1BD4 |. 51          PUSH ECX          ; |Arg2 = 0017B0B0
005D1BD5 |. 8D95 0CFFFFFF LEA EDX,[LOCAL.61]      ; |
005D1BDB |. 52          PUSH EDX          ; |Arg1 = 02A6FA14
005D1BDC |. E8 44D15700  CALL 00B4ED25          ; \Firegrap.00B4ED25
005D1BE1 |. 83C4 0C      ADD ESP,0C
005D1BE4 |. 33C0        XOR EAX,EAX
005D1BE6 |. 66:8985 14FFF>MOV WORD PTR [EBP-EC],AX
005D1BED |. 6A 04      PUSH 4          ; /Arg3 = 00000004
005D1BEF |. 8B4D 10      MOV ECX,[ARG.3]          ; |
005D1BF2 |. 83C1 08      ADD ECX,8          ; |
005D1BF5 |. 51          PUSH ECX          ; |Arg2 = 0017B0B0
005D1BF6 |. 8D95 5CFFFFFF LEA EDX,[LOCAL.41]      ; |
005D1BFC |. 52          PUSH EDX          ; |Arg1 = 02A6FA14
005D1BFD |. E8 23D15700  CALL 00B4ED25          ; \Firegrap.00B4ED25
005D1C02 |. 83C4 0C      ADD ESP,0C
005D1C05 |. 33C0        XOR EAX,EAX
005D1C07 |. 66:8985 64FFF>MOV WORD PTR [EBP-9C],AX
005D1C0E |. 6A 04      PUSH 4          ; /Arg3 = 00000004
005D1C10 |. 8B4D 10      MOV ECX,[ARG.3]          ; |
005D1C13 |. 83C1 10      ADD ECX,10         ; |
005D1C16 |. 51          PUSH ECX          ; |Arg2 = 0017B0B0
005D1C17 |. 8D95 34FFFFFF LEA EDX,[LOCAL.51]      ; |
005D1C1D |. 52          PUSH EDX          ; |Arg1 = 02A6FA14
005D1C1E |. E8 02D15700  CALL 00B4ED25          ; \Firegrap.00B4ED25
005D1C23 |. 83C4 0C      ADD ESP,0C
005D1C26 |. 33C0        XOR EAX,EAX
005D1C28 |. 66:8985 3CFFF>MOV WORD PTR [EBP-C4],AX
005D1C2F |. 8B4D 10      MOV ECX,[ARG.3]
005D1C32 |. 51          PUSH ECX
005D1C33 |. E8 9DAE5700  CALL 00B4CAD5          ; Firegrap.00B4CAD5
005D1C38 |. 83C4 04      ADD ESP,4
005D1C3B |. 83F8 10      CMP EAX,10
005D1C3E |. 0F85 4C010000 JNZ 005D1D90          ; Firegrap.005D1D90
```

une las primera 2 partes del serial

```
005D1D90 |> \68 5C9DD800  PUSH 0D89D5C          ; /Arg2 = 00D89D5C
005D1D95 |. 8D85 C4FAFFFF LEA EAX,[LOCAL.335]      ; |
005D1D9B |. 50          PUSH EAX          ; |Arg1 = 00194580
005D1D9C |. E8 C8D35700  CALL 00B4F169          ; \Firegrap.00B4F169
005D1DA1 |. 83C4 08      ADD ESP,8
005D1DA4 |> 8D8D 5CFFFFFF LEA ECX,[LOCAL.41] ->
005D1DAA |. 51          PUSH ECX
005D1DAB |. 8D95 0CFFFFFF LEA EDX,[LOCAL.61]
005D1DB1 |. 52          PUSH EDX
005D1DB2 |. 68 5CF2D800  PUSH 0D8F25C          ; UNICODE "%s%s"
```

ahora los convierte en el formato que es el valido

```
005D1DD1 |. 50          PUSH EAX          ; /Arg2 = 00194580
005D1DD2 |. 8D55 80      LEA EDX,[LOCAL.32]          ; |
005D1DD5 |. 52          PUSH EDX          ; |Arg1 = 02A6FA14
005D1DD6 |. E8 F58EE5FF  CALL 0042ACD0          ; \Firegrap.0042ACD0
005D1DD8 |. 83C4 08      ADD ESP,8
005D1DDE |. 50          PUSH EAX
005D1DDF |. 68 B885D900  PUSH 0D985B8          ; UNICODE "%08X"
```

y crea la llave

```
005D1DE8 |. E8 9BD35700  CALL 00B4F188          ; Firegrap.00B4F188 sera similar a wsprint?
```


Ahora comienzo a comparar y a crear lo necesario:

005010C3	83C4 04	CALL 00B520EA	Sin_limi.00B520EA
005010C6	8985 BCFAFFFF	ADD ESP,4	
005010C8	8995 C0FAFFFF	MOV DWORD PTR [EBP-544],EAX	
005010C9	8095 BCFAFFFF	MOV DWORD PTR [EBP-540],EDX	
005010D0	52	LEA EDX,DWORD PTR [EBP-544]	
005010D1	E8 EC035800	PUSH EDX	
005010D2	83C4 04	CALL 00B520EA	
005010D3	8985 BCFAFFFF	ADD ESP,4	
005010D4	8885 BCFAFFFF	MOV DWORD PTR [EBP-548],EAX	
005010D5	8848 14	MOV EAX,DWORD PTR [EBP-548]	
005010D6	81C1 6C070000	MOV ECX,DWORD PTR [EAX+14]	
005010D7	3B8D A8FAFFFF	ADD ECX,76C	
005010D8	90	CMP ECX,DWORD PTR [EBP-558]	2009 vs /2010
005010D9	90	NOE	
005010DA	8895 BCFAFFFF	NOE	
005010DB	8842 14	MOV EDX,DWORD PTR [EBP-548]	
005010DC	05 6C070000	MOV EAX,DWORD PTR [EDX+14]	
005010DD	3B85 A8FAFFFF	ADD EAX,76C	
005010DE	75 14	CMP EAX,DWORD PTR [EBP-558]	2009 vs /2010
005010DF	888D BCFAFFFF	JNZ SHORT 00501048	Sin_limi.00501048
005010E0	8851 10	MOV ECX,DWORD PTR [EBP-548]	
005010E1	83C2 01	MOV EDX,DWORD PTR [ECX+10]	
005010E2	3B95 A4FAFFFF	ADD EDX,1	
005010E3	7F 3C	CMP EDX,DWORD PTR [EBP-55C]	
005010E4	8885 BCFAFFFF	JG SHORT 00501084	Sin_limi.00501084
005010E5	8848 14	MOV EAX,DWORD PTR [EBP-548]	
005010E6	81C1 6C070000	MOV ECX,DWORD PTR [EAX+14]	
005010E7	3B8D A8FAFFFF	ADD ECX,76C	
005010E8	75 2F	CMP ECX,DWORD PTR [EBP-558]	2009 vs /2010
005010E9	8895 BCFAFFFF	JNZ SHORT 0050108E	Sin_limi.0050108E
005010EA	8842 10	MOV EDX,DWORD PTR [EBP-548]	
005010EB	83C0 01	MOV EAX,DWORD PTR [EDX+10]	
005010EC	3B85 A4FAFFFF	ADD EAX,1	
005010ED	75 1B	CMP EAX,DWORD PTR [EBP-55C]	
005010EE	888D BCFAFFFF	JNZ SHORT 0050108E	Sin_limi.0050108E
005010EF	8851 0C	MOV ECX,DWORD PTR [EBP-548]	
005010F0	3B95 A0FAFFFF	MOV EDX,DWORD PTR [ECX+C]	
005010F1	7E 0A	CMP EDX,DWORD PTR [EBP-560]	
005010F2	B8 02000000	JLE SHORT 0050108E	Sin_limi.0050108E
005010F3	E9 53020000	MOV EAX,2	
005010F4	EB 14	JMP 00501FE1	Sin_limi.00501FE1
005010F5	68 5C9DD800	JMP SHORT 00501DA4	Sin_limi.00501DA4
005010F6	8085 C4FAFFFF	PUSH 0D89D5C	
005010F7	50	LEA EAX,DWORD PTR [EBP-53C]	
005010F8	E8 C8D35700	PUSH EAX	
005010F9	83C4 08	CALL 00B4F169	Sin_limi.00B4F169
005010FA	808D 5CFFFFFF	ADD ESP,8	
005010FB	51	LEA ECX,DWORD PTR [EBP-A4]	
005010FC	8D95 0CFFFFFF	PUSH ECX	
005010FD	52	LEA EDX,DWORD PTR [EBP-F4]	
005010FE	68 5CF2D800	PUSH EDX	
005010FF	8D45 80	PUSH 0D8F25C	UNICODE "%s%s"
00501100	50	LEA EAX,DWORD PTR [EBP-80]	
00501101	E8 C8D35700	PUSH EAX	
00501102	83C4 10	CALL 00B4F188	Sin_limi.00B4F188
00501103	ADD ESP,10		
Stack address=0012A060, (UNICODE "0000")			
CX=000007DA			

Veo que toma partes del serial para determinar la fecha de duración de este
Encuentro que tiene relacion a cantidad de licencias y duración., son los ultimos 4 digitos
Si coloco en el ultimo 1234 , llega a mover 2, por ende estoy con una clave vencida
Pruebo algunas combinaciones simples 6475 /6010 u otras y paso bien (2015)
El formato va asi: NombreCompañiaSerial deberia ya terminar en 6010 para pasar la primera
condicion, bien mostraba en el primer traceo, que toma las partes y las guarda en posiciones.
Pasada la primera, (colocando 6010)

00000000:xxx6010

Y llego a la siguiente condicion de las xxxx marcadas

005010F6	8D55 A8	MOV WORD PTR [EBP-50],CX	6475 vs/0000
005010F9	52	LEA EDX,DWORD PTR [EBP-58]	
005010FA	8D85 34FFFFFF	PUSH EDX	
005010FB	50	LEA EAX,DWORD PTR [EBP-CC]	
005010FC	E8 82CB5700	PUSH EAX	
005010FD	83C4 08	CALL 00B4E988	Sin_limi.00B4E988
005010FE	85C0	ADD ESP,8	
005010FF	74 0A	TEST EAX,EAX	
00501100	B8 03000000	JE SHORT 00501E17	Sin_limi.00501E17
00501101	E9 CA010000	MOV EAX,3	
00501102	6A 00	JMP 00501FE1	Sin_limi.00501FE1
00501103	6A 00	PUSH 0	
00501104	68 0054DA00	PUSH 0	
00501105	B9 18AEEC00	PUSH 0DA5480	UNICODE "REGISTRATION_KEY"
00501106	E8 56DA0600	MOV ECX,0ECAE18	
00501107	8985 30FFFFFF	CALL 0063F880	Sin_limi.0063F880
00501108	837D 0C 00	MOV DWORD PTR [EBP-00],EAX	
00501109	74 0B	CMP DWORD PTR [EBP+C],0	
0050110A	8B4D 0C	JE SHORT 00501E41	Sin_limi.00501E41
0050110B	898D 4CFAFFFF	MOV ECX,DWORD PTR [EBP+C]	
0050110C	EB 0A	MOV DWORD PTR [EBP-5B4],ECX	
0050110D	C785 4CFAFFFF	JMP SHORT 00501E4B	Sin_limi.00501E4B
0050110E	8D95 C4FAFFFF	MOV DWORD PTR [EBP-5B4],0D89D5C	
0050110F	52	LEA EDX,DWORD PTR [EBP-53C]	
00501110	8B85 4CFAFFFF	PUSH EDX	
00501111	50	MOV EAX,DWORD PTR [EBP-5B4]	
00501112	8B4D 08	PUSH EAX	
00501113	51	MOV ECX,DWORD PTR [EBP+8]	
00501114	68 A88D9000	PUSH ECX	
00501115	8D95 0CFBFFFF	PUSH 0D985A8	UNICODE "%s%s%s"
00501116	52	LEA EDX,DWORD PTR [EBP-4F4]	
00501117	E8 1AD35700	PUSH EDX	
00501118	CALL 00B4F188		Sin_limi.00B4F188
Stack address=0012A038, (UNICODE "XXXX")			
EAX=00000008			

En ebp-58 apunta a 6475 y en ebp-cc apunta a xxxx, por ende mi serial debe ser:
0000000064756010

Vuelvo a colocar el serial y paso a la proxima condicion , reconocida por el test eax,eax y debajo un mov eax,3

005D1E9A	E9 42010000	JMP 005D1FE1	Si
005D1E9F	8D8D 0CFFFFFF	LEA ECX,DWORD PTR [EBP-F4]	
005D1EA5	51	PUSH ECX	
005D1EA6	8D55 CC	LEA EDX,DWORD PTR [EBP-34]	
005D1EA9	52	PUSH EDX	XF
005D1EAA	E8 32065700	CALL 00B4F4E1	Si
005D1EAF	83C4 08	ADD ESP,8	
005D1EB2	85C0	TEST EAX,EAX	
005D1EB4	74 0A	JE SHORT 005D1EC0	Si
005D1EB6	B8 03000000	MOV EAX,3	
005D1EBB	E9 21010000	JMP 005D1FE1	Si
005D1EC0	837D 14 01	CMP DWORD PTR [EBP+14],1	
005D1EC4	7E 52	JLE SHORT 005D1F18	Si
005D1EC6	8B85 30FFFFFF	MOV EAX,DWORD PTR [EBP-D0]	
005D1ECC	83C0 01	ADD EAX,1	
005D1ECF	50	PUSH EAX	
005D1ED0	8D4D CC	LEA ECX,DWORD PTR [EBP-34]	
005D1ED3	51	PUSH ECX	
005D1ED4	8D95 0CFBFFFF	LEA EDX,DWORD PTR [EBP-4F4]	
005D1EDA	52	PUSH EDX	XF
005D1EDB	8B8D 50FAFFFF	MOV ECX,DWORD PTR [EBP-5B0]	Si
005D1EE1	E8 1A010000	CALL 005D2000	Si
005D1EE6	0EB6C0	MOVZX EAX,AL	
Stack address=0012A0D0, (UNICODE "4AC8")			
EDX=02C70001 (xpsp2res.02C70001)			

En EBP-(F4 vs/34)

Vemos la segunda parte del serial, pero esta vez del comienzo

Pero este es el comienzo, 4ac8

4ac80000xxxx6010

Y verifico ahora bien en la rutina

Y ahora es otro numero 4AC80000xxxx6010

Otra vez entro al loop y veo la primera comparacion y ahora es 8727 el correcto y no el otro, pues cambiamos el serial anterior.

4AC8000087276010

Con esto paso todo bien , llevo lo siguiente

1) la fecha X-X-X-X

2) el segundo parametro de verificacion X-X-X-X

3) el primer valor X-X-X-X

4) el segundo parametro de verificacion con el primer valor X-X-X-X

5) ahora falta seguir y encontrar el ultimo, ahora aparece Gracias por registrar, pero retorno del dialogo hasta que vea otro test eax,eax y llego aca

005D1EF2	E9 EA000000	JMP 005D1FE1	Sin_limi.005D1FE1
005D1EF7	8D8D 5CFFFFFF	LEA ECX,DWORD PTR [EBP-A4]	
005D1EFD	51	PUSH ECX	
005D1EFE	8D55 CC	LEA EDX,DWORD PTR [EBP-34]	ultimo
005D1F01	52	PUSH EDX	xpsp2res.02CC0001
005D1F02	E8 DAD55700	CALL 00B4F4E1	Sin_limi.00B4F4E1
005D1F07	83C4 08	ADD ESP,8	
005D1F0A	85C0	TEST EAX,EAX	
005D1F0C	74 0A	JE SHORT 005D1F18	Sin_limi.005D1F18
005D1F0E	B8 03000000	MOV EAX,3	
005D1F13	E9 C9000000	JMP 005D1FE1	Sin_limi.005D1FE1
005D1F18	8B85 50FAFFFF	MOV EAX,DWORD PTR [EBP-5B0]	Sin_limi.00ECAE18
005D1F1E	05 BC9E0000	ADD EAX,9EBC	
005D1F23	50	PUSH EAX	
005D1F24	FF15 08C4C700	CALL NEAR DWORD PTR [C7C408]	ntdll.RtlEnterCrit
005D1F2A	8B4D 10	MOV ECX,DWORD PTR [EBP+10]	
005D1F2D	51	PUSH ECX	
005D1F2E	68 A454DA00	PUSH 0DA54A4	UNICODE "bk%\$"
005D1F33	8D95 E8FAFFFF	LEA EDX,DWORD PTR [EBP-518]	
005D1F39	52	PUSH EDX	xpsp2res.02CC0001
005D1F3A	E8 49D25700	CALL 00B4F188	Sin_limi.00B4F188
005D1F3F	83C4 0C	ADD ESP,0C	
005D1F42	C745 04 000000	MOV DWORD PTR [EBP-5C],0	
Stack address=0326FED4, (UNICODE "E353")			
EDX=02CC0001 (xpsp2res.02CC0001)			

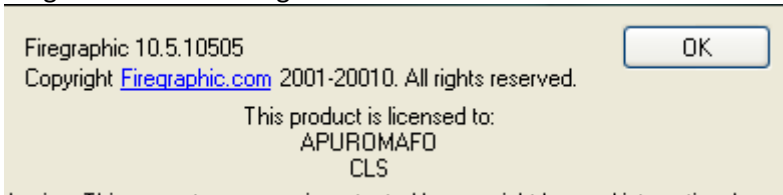
Por lo cual el pseudo serial 1

4AC8e353xxxx6010

Se convierte en el definitivo al pasar por el segundo y mas importante

4AC8e353F9F06010

Luego confirmo si se registro:



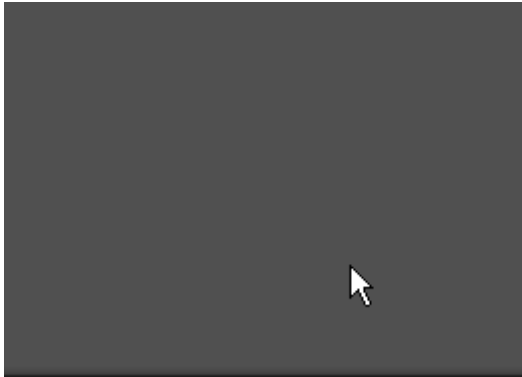
Segundo paso , ya registrado, pues no hay nag de molestias.por ende todo dependia de aquel valor determinaba todo

005D1F42	E9 00000000	JMP 005D1FE1	
005D1F47	833D AC8E0000	CMP DWORD PTR [ECAEAC],4	
005D1F4E	0F85 F4000000	JNZ 004C0F18	

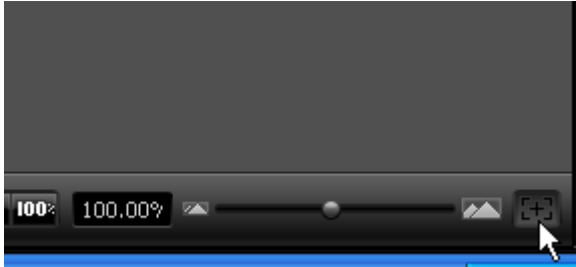
Sigo con la aplicacion y parece interesante pero justo se me ocurre ver un jpg , que habia sacado de un flash



Desde el visor de esta aplicaci3n



no se ve nada, ya lo arreglaran en otra version, pero el tema es lo siguiente:Pulso en grande coloco el navegador:



Para ver los datos que contiene este informe de errores, [haga clic aqu3](#).

DepurarEnviar informes de erroresNo enviar

Y cae la aplicacion

Address: 0x00000000005225ed

Tras varios intentos, logro anular este "bug" , pues analizo y encuentro que el bloque no tiene mayores chequeos de ceros

0052259A	74 08	JE SHORT 005225A4	Sin_lini.005225A4
0052259C	8B4D EC	MOV ECX, [LOCAL.5]	
0052259F	E8 1CA0F4FF	CALL 0046C5C0	Sin_lini.0046C5C0
005225A4	EB 33	JMP SHORT 005225D9	Sin_lini.005225D9
005225A6	8B45 FC	MOV EAX, [LOCAL.1]	
005225A9	2B45 F4	SUB EAX, [LOCAL.3]	
005225AC	8945 C8	MOV [LOCAL.14], EAX	kernel32.7C8399F3
005225AF	8B4D F8	MOV ECX, [LOCAL.2]	kernel32.7C816D58
005225B2	2B4D F0	SUB ECX, [LOCAL.4]	
005225B5	894D C4	MOV [LOCAL.15], ECX	
005225B8	6A 00	PUSH 0	
005225BA	68 FFFFFFF0	PUSH 0FFFFFFF	Arg5 = 00000000
005225BF	8B55 C8	MOV EDX, [LOCAL.14]	Arg4 = 00FFFFFF
005225C2	52	PUSH EDX	
005225C3	8B45 C4	MOV EAX, [LOCAL.15]	Arg3 = 7C91EB94
005225C6	50	PUSH EAX	kernel32.7C816D4C
005225C7	8B4D 08	MOV ECX, [ARG.1]	Arg2 = 00000000
005225CA	51	PUSH ECX	Sin_lini.<ModuleEntryPoint>
005225CB	E8 10F50F00	CALL 00621AE0	Arg1 = 0012FFB0
005225D0	83C4 14	ADD ESP, 14	Sin_lini.00621AE0
005225D3	8B55 C0	MOV EDX, [LOCAL.16]	
005225D6	8942 40	MOV DWORD PTR [EDX+40], EAX	ntdll.7C91E64E
005225D9	8B45 C0	MOV EAX, [LOCAL.16]	ntdll.7C91E64E
005225DC	83C0 48	ADD EAX, 48	
005225DF	50	PUSH EAX	
005225E0	8B4D C0	MOV ECX, [LOCAL.16]	Arg4 = 00000000
005225E3	83C1 44	ADD ECX, 44	ntdll.7C91E64E
005225E6	51	PUSH ECX	
005225E7	8B55 C0	MOV EDX, [LOCAL.16]	Arg3 = 0012FFB0
005225EA	8B42 40	MOV EAX, DWORD PTR [EDX+40]	ntdll.7C91E64E
005225ED	8B48 34	MOV ECX, DWORD PTR [EAX+34]	
005225F0	51	PUSH ECX	Arg2 = 0012FFB0
005225F1	8B55 C0	MOV EDX, [LOCAL.16]	ntdll.7C91E64E
005225F4	8B42 40	MOV EAX, DWORD PTR [EDX+40]	
005225F7	8B48 30	MOV ECX, DWORD PTR [EAX+30]	
005225FA	51	PUSH ECX	Arg1 = 0012FFB0
005225FB	E8 30422800	CALL 007A6830	Sin_lini.007A6830
00522600	DD08	FSTP ST	

Luego de ver como crasheaba una y otra vez, resuelvo en anular estas zonas

005225DF	50	PUSH EAX	
005225E0	8B4D C0	MOV ECX,DWORD PTR [EBP-40]	ntdll.7C91E64E
005225E3	83C1 44	ADD ECX,44	
005225E6	51	PUSH ECX	
005225E7	8B55 C0	MOV EDI,DWORD PTR [EBP-40]	ntdll.7C91E64E
005225EA	8B42 40	MOV EAX,DWORD PTR [EDX+40]	
005225ED	90	NOP	
005225EE	90	NOP	
005225EF	90	NOP	
005225F0	51	PUSH ECX	
005225F1	8B55 C0	MOV EDI,DWORD PTR [EBP-40]	ntdll.7C91E64E
005225F4	8B42 40	MOV EAX,DWORD PTR [EDX+40]	
005225F7	90	NOP	
005225F8	90	NOP	
005225F9	90	NOP	
005225FA	51	PUSH ECX	
005225FB	E8 30422800	CALL 007A6830	Firegrap.007A6830
00522600	DD08	FSTP ST	
00522602	83C4 10	ADD ESP,10	
00522605	8BE5	MOV ESP,EBP	
00522607	5D	POP EBP	
00522608	C2 0400	RETN 4	kernel32.7C816D4F
0052260B	CC	INT3	

Pues la variable en eax, no siempre es posicionada en la misma forma

00522590	8B55 C0	MOV EDI,DWORD PTR [EBP-40]	ntd
00522593	8B42 40	MOV DWORD PTR [EDX+40],EAX	
00522596	837D EC 00	CMP DWORD PTR [EBP-14],0	
0052259A	74 08	JE SHORT 005225A4	Fire
0052259C	8B4D EC	MOV ECX,DWORD PTR [EBP-14]	

No debe valer cero, en 2 comparaciones, y aqui solo verifican el valor de ebp

Siguiendo, con eso ya no crashea, pero no es capaz de abrir la imagen con transparencias

Y como no la vemos, obviamente toda conversion similar, es erronea, desde jpg a bmp y otras.

Por lo que ya revise el tema

Ahora bien

Llega el momento de pensar en app.dat , y veo el recurso, fijemos que contiene inclusive el orden, bienvenida, y los seriales..del formato bk y valor. (puede que el 7cc122xxxx y el otro sea un lista negra, pero no quiero verificar esto, pues solo forzando los saltos o las variables (de 0 a 4), para tener todo en orden desde el comienzo

IDR_BIN	01365A70: 00 80 01 10 50 52 49 4E 54 49 4E 47 54 45 4D 50	.C..PRINTINGTEMP
1	01365A80: 4C 41 54 45 01 00 00 00 90 01 0A 52 45 43 4F 52	LATE....E..RECOR
CursorEntry	01365A90: 44 44 49 53 43 01 00 00 00 00 01 10 52 45 47 49	DDISC....@..REGI
Bitmap	01365AA0: 53 54 52 41 54 49 4F 4E 5F 48 45 59 01 00 00 00	STRATION KEY...
IconEntry	01365AB0: 00 00 10 52 45 47 49 53 54 52 41 54 49 4F 4E 5F	...REGISTRATION
Dialog	01365AC0: 53 45 43 01 00 00 00 E5 00 00 52 45 47 5F 50 41	SEC....@..REG_PA
Cursor	01365AD0: 54 43 01 00 00 00 07 01 00 54 41 47 01 00 00 00	TH.....TAG....
Icon	01365AE0: E0 01 00 54 43 55 40 42 4E 41 49 4C 54 52 41 59	0...THUMBNAI TRAV
Version	01365AF0: 01 00 00 00 38 01 08 54 53 41 59 49 43 4F 4E 01	...@..TRAVICON..
	01365B00: 00 00 00 60 01 07 56 45 45 53 49 4F 4E 01 00 00	...@..VERSION..
	01365B10: 00 84 00 0B 57 45 42 53 49 54 45 5F 55 52 4C 01	...@..WEBSITE URL
	01365B20: 00 00 00 F0 00 00 57 45 4C 43 4F 4D 45 57 49 5A	...@..WELCOME WIZ
	01365B30: 41 52 44 01 00 00 00 D8 01 12 62 68 37 43 43 31	ARD....@..bk7CC1
	01365B40: 32 32 35 31 39 32 42 43 33 34 35 36 01 00 00 00	225192BC3456....
	01365B50: F0 01 12 62 68 42 38 32 31 41 35 37 34 43 35 39	2...bkB821A574C59
	01365B60: 46 39 39 37 35 01 00 00 00 F8 01 00 00 00 00 00	F9975.....@..
	01365B70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00@..

Bk [SERIAL] , por lo cual puede que estos recursos guarden otro misterio, que quizas si se supiera analizar del todo, algo mas se sabria.

que contiene informacion de muy similares características

Ademas el update queda expuesto el serial , nombre y compañía

<http://www.firegraphic.com/update/?version=10505&serial=F2683A0DF0A46010&name=APUROMAFO&companyCRACKSLATINOS&os=5.1>

pero bueno conclusiones

con solo mirar una linea, y buscar, podemos jugar a diferentes mensajes

005202D9 833D ACAEEC00 0>CMP DWORD PTR [ECAEAC],1

0->gracias (no nag)

1-> coloca mas datos(falla el serial de largo 16 o algun valor)

2->expired (2009 o menores osea terminados en e.g . 1234)

3->invalid (falla la verificacion del serial)

Siguiendo teniamos la duda de app.dat

Como string esta aqui

00582183	PUSH 0D985D8	UNICODE "//app.dat"
005821F9	CMP DWORD PTR [EC73E0],1	(Initial CPU selection)
00582202	PUSH 0D985EC	UNICODE "//skin.dat"

Por lo que no estaria si salta

00582170	JMP 00584372	Firegrap.00584372
00582175	JMP 00582276	Firegrap.00582276
0058217A	CMP DWORD PTR [EC73E0],1	
00582181	JLE SHORT 005821F9	Firegrap.005821F9
00582183	PUSH 0D985D8	Arg2 = 00D985D8
00582188	MOV EAX,DWORD PTR [EC73E0]	
0058218D	MOV ECX,DWORD PTR [EAX+4]	
00582190	PUSH ECX	
00582191	CALL 00B4F4E1	Arg1 = 00ECAE1C Firegrap.00B4F4E1

Y depende de los 2 saltos, obviamente de INTERNET.

00581DF5	50	PUSH EAX	
00581DF6	8D45 F4	LEA EAX,DWORD PTR [EBP-C]	
00581DF9	64:A3 000000	MOV DWORD PTR FS:[0],EAX	
00581DFF	68 04010000	PUSH 104	BufSize = 104 (260.)
00581E04	68 2CAFE000	PUSH 0ECAFE00	PathBuffer = Firegrap.00ECAFE00
00581E09	8B45 08	MOV EAX,DWORD PTR [EBP+8]	
00581E0C	50	PUSH EAX	hModule = 4BC0543F
00581E0D	FF15 24C4C700	CALL NEAR DWORD PTR [C7C424]	GetModuleFileNameW
00581E13	8D80 54FCFF	LEA ECX,DWORD PTR [EBP-3AC]	
00581E19	51	PUSH ECX	plWSAData = Firegrap.00ECAFE1C
00581E1A	68 02020000	PUSH 202	RequestedVersion = 202 (2.2.)
00581E1F	FF15 ACC9C700	CALL NEAR DWORD PTR [C7C9AC]	WSAStartup
00581E25	85C0	TEST EAX,EAX	
00581E27	74 07	JE SHORT 00581E30	Firegrap.00581E30
00581E29	33C0	XOR EAX,EAX	
00581E2B	E9 42250000	JMP 00584372	Firegrap.00584372
00581E2D	333D E073EC00	CMP DWORD PTR [EC73E0],1	
00581E30	0F8E 3D030000	JLE 0058217A	Firegrap.0058217A
00581E3D	68 7485D900	PUSH 0D98574	Arg2 = 00D98574
00581E42	8B15 E873EC00	MOV EDI,DWORD PTR [EC73E8]	
00581E48	8B42 04	MOV EAX,DWORD PTR [EDX+4]	
00581E4B	50	PUSH EAX	Arg1 = 4BC0543F
00581E4C	E8 90D65C00	CALL 00B4F4E1	Firegrap.00B4F4E1
00581E51	83C4 08	ADD ESP,8	
00581E54	85C0	TEST EAX,EAX	
00581E56	0F85 1E030000	JNZ 0058217A	Firegrap.0058217A
00581E5C	333D E073EC00	CMP DWORD PTR [EC73E0],7	
00581E63	74 07	JE SHORT 00581E6C	Firegrap.00581E6C
00581E65	33C0	XOR EAX,EAX	
00581E67	E9 06250000	JMP 00584372	Firegrap.00584372
00581E6C	8B0D E873EC00	MOV ECX,DWORD PTR [EC73E8]	
00581E73	8B51 04	MOV EAX,DWORD PTR [ECX+4]	

Proyeccion: Por ende, quizas si accede a internet, posiblemente app.dat actualize alguna lista negra de seriales, para un futuro firegrafic 11 y asi vencer seriales no validos.

Actualmente ahi guarda la rama de regedit, el nombre de una dll, para hacer un mejor efecto y todo lo obtiene de un recurso

Pero si bajo un poco se ven algunas conversiones que puede que sean usadas

00581F25	. 68 9085D900	PUSH 0D98590	; UNICODE "%1X%1X%02X"
00581F4E	. 68 A885D900	PUSH 0D985A8	; UNICODE "%s%s%s"
00581FD9	. 68 5CF2D800	PUSH 0D8F25C	; UNICODE "%s%s"
0058200F	. 68 B885D900	PUSH 0D985B8	; UNICODE "%08X"
00582048	. 68 C485D900	PUSH 0D985C4	; UNICODE "%s%s%s%s"

Proyeccion2:

El usuario y compañía debe ser menor a 89 letras

Agradecimientos

A toda la lista de CLS

Saludos Apuromafo