



Victima	FreshDownload
Url	http://www.freshdevices.com/freshdown.html
Herramientas	Olly
Fecha	01/09/11
Cracker	Alberto Fernández (ZiKaTRiZ)
Dificultad	Demasiado leve

Cargamos el ejecutable en RDG y comprobamos que no tiene nada importante.



Introducimos el usuario y el código de registro,

Registro De FreshDownload

Ingrese su código de registro a continuación. Si no tiene el código, haga clic [aquí](#) y obtener el código de forma gratuita.

Nombre Del Usuario

Código Del Registro

OK Cancelación

Bueno, no dice nada, veamos si encontramos algo interesante en las string references.

005B5D25	HSCII "FUReg"	
005B5FC8	MOV EAX,fd.005B62F0	UNICODE "FreshDownload has been registered successfully."
005B6003	MOV EDX,fd.005B6358	ASCII "\\Software\FreshDevices\FreshDownload"
005B6016	MOV EDX,fd.005B6388	ASCII "Owner"
005B6029	MOV EDX,fd.005B6398	ASCII "RegCode"
005B6054	MOV EDX,fd.005B63A8	ASCII "Registered"
005B607D	MOV EDX,fd.005B63BC	ASCII "\\htmlfile\shell\open\ddeexec\Topic"
005B60AF	MOV EDX,fd.005B63F4	ASCII "C2"
005B6130	MOV EDX,fd.005B6404	UNICODE "About - [Bussines License]"
005B6143	MOV EDX,fd.005B6440	UNICODE "About - [Personal License]"
005B615D	MOV EDX,fd.005B647C	UNICODE "FreshDownload - [Bussines License]"
005B6170	MOV EDX,fd.005B64C8	UNICODE "FreshDownload - [Personal License]"
005B61F9	MOV EDX,fd.005B6358	ASCII "\\Software\FreshDevices\FreshDownload"
005B620C	MOV EDX,fd.005B6388	ASCII "Owner"
005B621F	MOV EDX,fd.005B6398	ASCII "RegCode"
005B624A	MOV EDX,fd.005B63A8	ASCII "Registered"
005B6259	MOV EDX,fd.005B6518	ASCII "\\Software\Microsoft\Multimedia\Audio\WaveFormats"
005B628B	MOV EDX,fd.005B63F4	ASCII "C2"

Vemos que si el registro es valido, nos muestra un mensaje como podemos ver en 005B5FC8 de que el registro está aceptado.

En la imagen que a continuación coloco es la responsable de generar los números de serie de las distintas licencias.

005B5E88	E8 9FFDFFFF	CALL fd.005B5D2C
----------	-------------	------------------

Aunque en las string references muestra dos tipos de licencias, genera tres tipos.

Licencia personal, que pasa 4 veces y por lo tanto genera 4.

005B5DE9	. FF57 0C	CALL DWORD PTR DS:[EDI+C]
005B5DEC	. 8B55 EC	MOV EDX,DWORD PTR SS:[EBP-14]
005B5DEF	. 58	POP EAX
005B5DF0	. E8 8304E5FF	CALL fd.00406278
005B5DF5	. 75 0A	JNZ SHORT fd.005B5E01
005B5DF7	. C705 5C345C00 FFFF	MOV DWORD PTR DS:[5C345C],-1
005B5E01	> 46	INC ESI
005B5E02	. 66:FFCB	DEC BX
005B5E05	. 75 B9	JNZ SHORT fd.005B5DC0
005B5E07	> 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]
005B5E0A	. 8B80 84030000	MOV EAX,DWORD PTR DS:[EAX+384]
005B5E10	. 8B80 80020000	MOV EAX,DWORD PTR DS:[EAX+280]
005B5E16	. 8B10	MOV EDX,DWORD PTR DS:[EAX]
005B5E18	. FF52 14	CALL DWORD PTR DS:[EDX+14]
005B5E1B	. 8BD8	MOV EBX,EAX

Stack SS:[0012EC8C]=001A640C, (UNICODE "7T4F4-HAC2-TFA9-962E")
EDX=00000000

Licencia personal, que pasa me parece que unas 90 veces y por lo tanto genera tantas como veces pasa.

005B5E26	> 8D45 E8	LEA EAX,DWORD PTR SS:[EBP-18]
005B5E29	. 8B15 64345C00	MOV EDX,DWORD PTR DS:[5C3464]
005B5E2F	. E8 0003E5FF	CALL fd.00406134
005B5E34	. 8B45 E8	MOV EAX,DWORD PTR SS:[EBP-18]
005B5E37	. 50	PUSH EAX
005B5E38	. 8D4D E4	LEA ECX,DWORD PTR SS:[EBP-1C]
005B5E3B	. 0FBFD6	MOVSX EDX,SI
005B5E3E	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]
005B5E41	. 8B80 84030000	MOV EAX,DWORD PTR DS:[EAX+384]
005B5E47	. 8B80 80020000	MOV EAX,DWORD PTR DS:[EAX+280]
005B5E4D	. 8B38	MOV EDI,DWORD PTR DS:[EAX]
005B5E4F	. FF57 0C	CALL DWORD PTR DS:[EDI+C]
005B5E52	. 8B55 E4	MOV EDX,DWORD PTR SS:[EBP-1C]
005B5E55	. 58	POP EAX
005B5E56	. E8 1D04E5FF	CALL fd.00406278
005B5E58	. 75 0A	JNZ SHORT fd.005B5E67
005B5E5D	. C705 54345C00 FFFF	MOV DWORD PTR DS:[5C3454],-1
005B5E67	> 46	INC ESI
005B5E68	. 66:FFCB	DEC BX
005B5E6B	. 75 B9	JNZ SHORT fd.005B5E26
005B5E6D	> 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]

Stack SS:[0012EC84]=001A6764, (UNICODE "8Q4D6-Q368-CK97-2U7B")
EDX=00000000

Licencia bussines, que pasa 100 y pico veces.

```

005B5E8C > 8D45 E0 LEA EAX,DWORD PTR SS:[EBP-20]
005B5E8F . 8B15 64345C00 MOV EDX,DWORD PTR DS:[5C3464]
005B5E95 . E8 9A02E5FF CALL fd.00406134
005B5E9A . 8B45 E0 MOV EAX,DWORD PTR SS:[EBP-20]
005B5E9D . 50 PUSH EAX
005B5E9E . 8D4D DC LEA ECX,DWORD PTR SS:[EBP-24]
005B5EA1 . 0FBFD6 MOVSX EDX,SI
005B5EA4 . 8B45 FC MOV EAX,DWORD PTR SS:[EBP-4]
005B5EA7 . 8B80 90030000 MOV EAX,DWORD PTR DS:[EAX+390]
005B5EAD . 8B80 80020000 MOV EAX,DWORD PTR DS:[EAX+280]
005B5EB3 . 8B38 MOV EDI,DWORD PTR DS:[EAX]
005B5EB5 . FF57 0C CALL DWORD PTR DS:[EDI+C]
005B5EB8 . 8B55 DC MOV EDX,DWORD PTR SS:[EBP-24]
005B5EBB . 58 POP EAX
005B5EBD . E8 B703E5FF CALL fd.00406278
005B5EC1 . 75 0A JNZ SHORT fd.005B5ECD
005B5EC3 . C705 58345C00 FFFF MOV DWORD PTR DS:[5C3458],-1
005B5EC6 . 46 INC ESI
005B5ECE . 66:FFCB DEC BX
005B5ED1 . 75 B9 JNZ SHORT fd.005B5E8C
005B5ED3 . 33C0 XOR EAX,EAX
005B5ED5 . 5A POP EDX
005B5ED6 . 59 POP ECX
005B5ED7 . 59 POP ECX
005B5ED8 . 64:8910 MOV DWORD PTR FS:[EAX],EDX
005B5EDB . 68 F55E5B00 PUSH fd.005B5EF5
005B5EE0 > 8D45 DC LEA EAX,DWORD PTR SS:[EBP-24]
005B5EE3 . BA 08000000 MOV EDI,8
005B5EE8 . E8 9F00E5FF CALL fd.00405F8C
Stack SS:[0012EC7C]=001A629C, (UNICODE "bu2c3r-4x4bu2b3-6f5t44")
EDX=00000000

```

Se puede comprobar cualquiera de ellas, que las admite todas.



Problema resuelto.

Gracias a todos.

A partir de ahora, firmaré los tutos que escriba bajo mi nombre real, ya me he cansado de salir bajo un nick, que realmente no representa nada.

1-12 - 2011

Alberto Fernández .