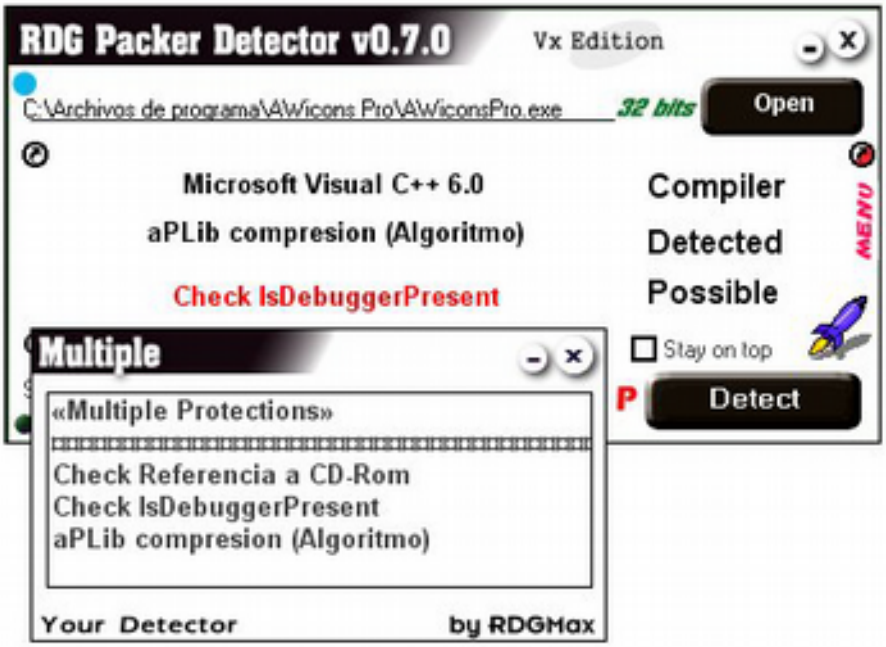
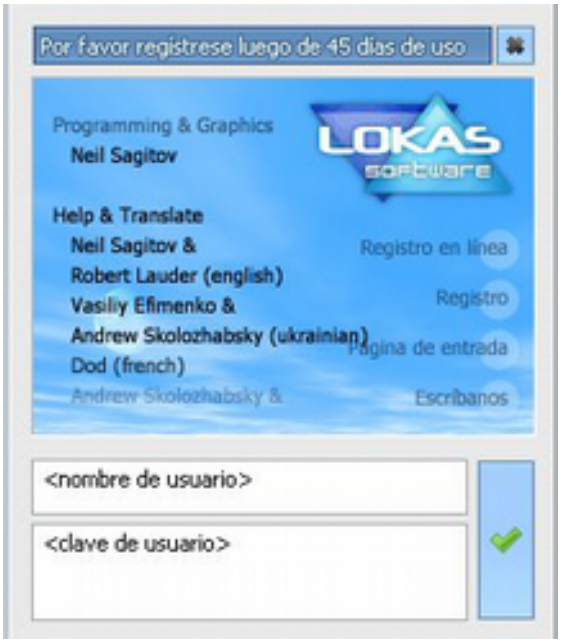
Victima	AWiconsPro
Url	http://www.awicons.com/
Herramientas	Olly
Fecha	11 – agosto - 2013
Cracker	Alberto Fernández
Dificultad	ninguna

Hola, Nunca me había encontrado con una protección como esta. Quizá haya acertado el número de serie a la primera, ya lo veremos.

Bien, RDG nos dice, que no tiene nada, pero si seleccionamos en la opción M-B nos muestra:



Bueno, vamos haber que nos pide el programa, lo ejecutaremos haber que hace.



Para que salga la parte del formulario de registro, deberemos pulsar la opción Registro, introducimos los datos, “nombre de usuario : Alberto Fernandez” , “clave de usuario : 989898” y pulsamos en el botón.

Bien, esto era de esperar. Cerremos el programa para poder cargarlo en el Olly, al cerrarlo nos muestra una nag.

Lo cargamos en el Olly, vamos haber las String References, para encontrar lo del mensaje que nos a mostrado antes.

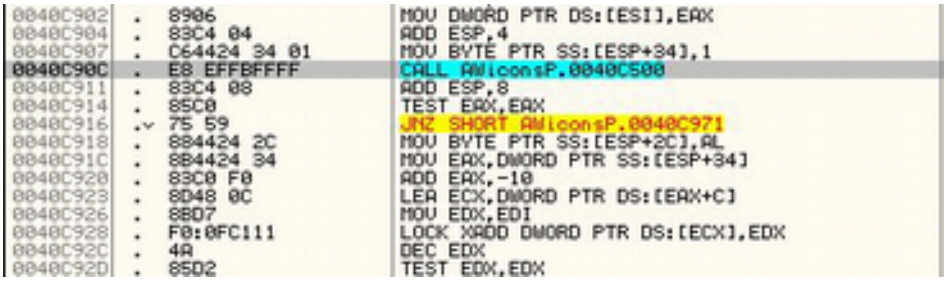
```
00408B6C PUSH AWiconsP.005EE4F0          ASCII "LOGO"
00408DAF PUSH AWiconsP.005EE4E0          ASCII "About"
00409521 PUSH AWiconsP.005EE660          ASCII "<code>"
00409534 PUSH AWiconsP.005EE650          ASCII "About dialog"
00409730 PUSH AWiconsP.005EE834          ASCII "Registration key accepted. Thank you for your purchase!"
00409741 PUSH AWiconsP.005EE82C          ASCII "key_ok"
00409779 PUSH AWiconsP.005EE7F0          ASCII "That name/key combination is not valid. Please try again."
0040978A PUSH AWiconsP.005EE7E4          ASCII "key_invalid"
004097A8 PUSH AWiconsP.005EE4E0          ASCII "About"
004097E1 PUSH AWiconsP.005EE7DC          ASCII "DEFAULT"
00409867 PUSH AWiconsP.005EE7DC          ASCII "DEFAULT"
00409896 PUSH AWiconsP.005EE8DC          ASCII "Please register after the 45 days of use"
004098A7 PUSH AWiconsP.005EE8D0          ASCII "please_reg"
004098BD PUSH AWiconsP.005EE4E0          ASCII "About"
00409915 PUSH AWiconsP.005EE8BC          ASCII "Registered to:"
```

Pulsaremos dos veces sobre 00409779, que es donde sale el mensaje que nos ha salido antes, si miramos un poco más arriba veremos, que esta la parte que acepta la key introducida y un salto colocado en “00409714 74 49 JE SHORT AWiconsP.0040975F”.

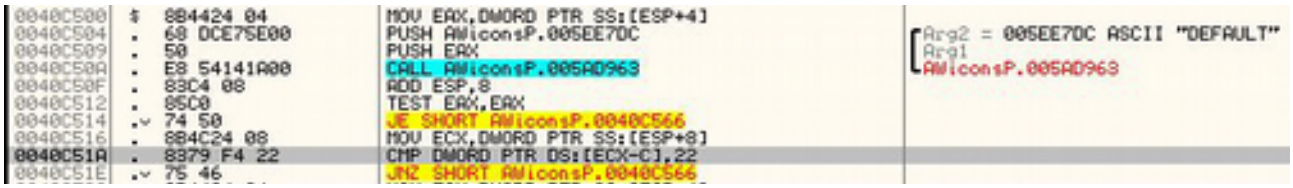
```
004096B8  .  6A 01              PUSH 1
004096BA  .  E8 2E700A00        CALL AWiconsP.004B06ED
004096BF  .  8B86 3C050000      MOV EAX,DWORD PTR DS:[ESI+53C]
004096C5  .  51                 PUSH ECX
004096C6  .  83E8 10            SUB EAX,10
004096C9  .  896424 18          MOV DWORD PTR SS:[ESP+18],ESP
004096CD  .  8BFC               MOV EDI,ESP
004096CF  .  50                 PUSH EAX
004096D0  .  E8 0B99FFFF        CALL AWiconsP.00402FE0
004096D5  .  83C0 10            ADD EAX,10
004096D8  .  8907               MOV DWORD PTR DS:[EDI],EAX
004096DA  .  8B86 40050000      MOV EAX,DWORD PTR DS:[ESI+540]
004096E0  .  83E8 10            SUB EAX,10
004096E3  .  896424 20          MOV DWORD PTR SS:[ESP+20],ESP
004096E7  .  8BFC               MOV EDI,ESP
004096E9  .  50                 PUSH EAX
004096EA  .  C74424 34 00000000 MOV DWORD PTR SS:[ESP+34],0
004096F2  .  E8 E998FFFF        CALL AWiconsP.00402FE0
004096F7  .  83C0 10            ADD EAX,10
004096FA  .  8907               MOV DWORD PTR DS:[EDI],EAX
004096FC  .  83CF FF            OR EDI,FFFFFFFF
004096FF  .  83C4 04            ADD ESP,4
00409702  .  897C24 30          MOV DWORD PTR SS:[ESP+30],EDI
00409706  .  E8 95300000        CALL AWiconsP.0040C7A0
0040970B  .  83C4 08            ADD ESP,8
0040970E  .  6A 00              PUSH 0                          Arg1 = 00000000
00409710  .  8BCE               MOV ECX,ESI
00409712  .  85C0               TEST EAX,EAX
00409714  .v 74 49              JE SHORT AWiconsP.0040975F
00409716  .  E8 CBE10A00        CALL AWiconsP.004B78E6          AWiconsP.004B78E6
0040971B  .  6A 01              PUSH 1
0040971D  .  68 B1000000        PUSH 0B1
00409722  .  51                 PUSH ECX
00409723  .  896424 24          MOV DWORD PTR SS:[ESP+24],ESP
00409727  .  8BDC               MOV EBX,ESP
00409729  .  51                 PUSH ECX
0040972A  .  8BCC               MOV ECX,ESP
0040972C  .  896424 28          MOV DWORD PTR SS:[ESP+28],ESP
00409730  .  68 34E85E00        PUSH AWiconsP.005EE834          ASCII "Registration key accepted.
00409735  .  E8 7684FFFF        CALL AWiconsP.00404BB0
0040973A  .  51                 PUSH ECX
0040973B  .  8BCC               MOV ECX,ESP
0040973D  .  896424 28          MOV DWORD PTR SS:[ESP+28],ESP
00409741  .  68 2CE85E00        PUSH AWiconsP.005EE82C          ASCII "key_ok"
00409746  .  C74424 40 01000000 MOV DWORD PTR SS:[ESP+40],1
0040974E  .  E8 5D84FFFF        CALL AWiconsP.00404BB0
00409753  .  51                 PUSH ECX
00409754  .  C64424 40 02       MOV BYTE PTR SS:[ESP+40],2
00409759  .  896424 34          MOV DWORD PTR SS:[ESP+34],ESP
0040975D  .v EB 47              JMP SHORT AWiconsP.004097A6
0040975F  >  E8 82E10A00        CALL AWiconsP.004B78E6          AWiconsP.004B78E6
00409764  .  6A 01              PUSH 1
00409766  .  68 B1000000        PUSH 0B1
0040976B  .  51                 PUSH ECX
0040976C  .  896424 28          MOV DWORD PTR SS:[ESP+28],ESP
00409770  .  8BDC               MOV EBX,ESP
00409772  .  51                 PUSH ECX
00409773  .  8BCC               MOV ECX,ESP
00409775  .  896424 2C          MOV DWORD PTR SS:[ESP+2C],ESP
00409779  .  68 F0E75E00        PUSH AWiconsP.005EE7F0          ASCII "That name/key combination
0040977E  .  E8 2D84FFFF        CALL AWiconsP.00404BB0
00409783  .  51                 PUSH ECX
00409784  .  8BCC               MOV ECX,ESP
00409786  .  896424 2C          MOV DWORD PTR SS:[ESP+2C],ESP
0040978A  .  68 E4E75E00        PUSH AWiconsP.005EE7E4          ASCII "key_invalid"
```

Por encima del salto hay 4 CALL, las tres primeras recogen el nombre y número de serie, la cuarta es la que realmente nos interesa.

Entraremos en la rutina que está en 00409706 E8 95300000 CALL AWiconsP.0040C7A0 y nos colocará en la posición correcta para poder registrarlo, pulsaremos “F8” hasta la posición:



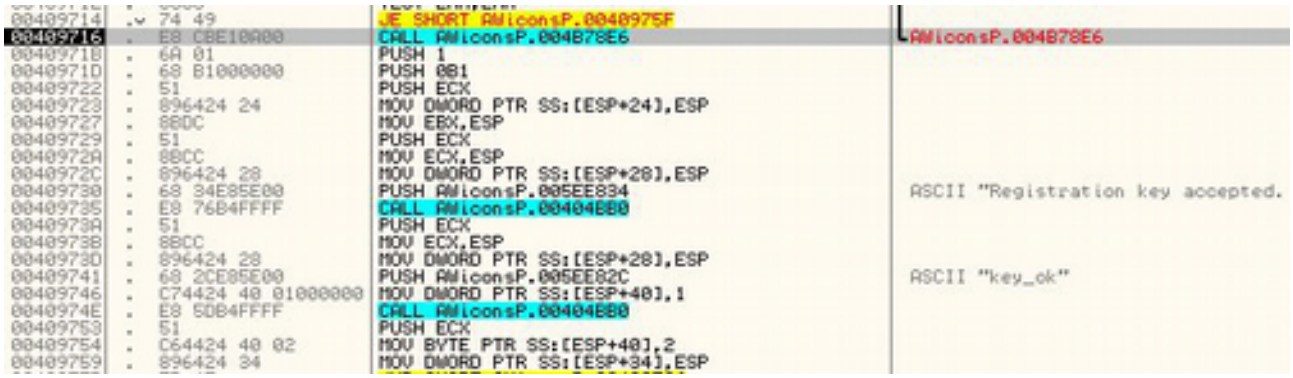
Entraremos en esta rutina.



Como podemos observar, compara nuestro serial con “DEFAULT” en la CALL situada en 0040C50A, recorre nuestro serial para conocer el largo, que después lo compara en la linea seleccionada el la imagen con “0x22 = 34 en decimal”.

Vale, cambiamos los valores introducidos anteriormente por :
Nombre de usuario: Alberto Fernandez
Clave de usuario : 01234567891123456789212345678931 23

Como vemos en la imagen anterior, si el valor de “DS” es inferior, nos dice que no es un número valido, y si es igual es valido. como muestra la imagen siguiente.



Que, ¿tanto por ciento, resulta de colocar un número cualquiera y acertarlo?. O acaso solo mira el largo de la cadena, comprobemos lo desde la entrada del registro de windows situada en :

HKEY_CURRENT_USER\Software\Lokas Ltd\AWicons Pro
valor RegKey REG_SZ: modificamos el primer 0 con una a.

Lo ejecutamos, y sigue registrado como muestra el about, podemos adelantar el reloj 46 días o un año y sigue igual.

Gracias por leerlo hasta aquí, es muy buena señal.

Alberto Fernández