

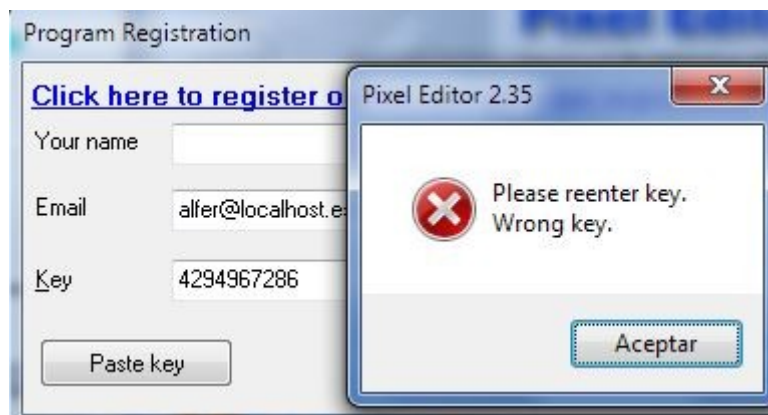


URL	http://www.iconempire.com/
Victima	Pixel Editor
Herramientas	Olly 1.1
Cracker	Alberto Fernández
Dificultad	Un poco complicado
Fecha	4 – 7 - 2016

Hola, ya estamos aquí otra vez, primero miramos el tipo de protección que tiene.



Lo ejecutamos para ver que nos muestra.



Introducir los datos correspondientes, el nombre, email y la key que debe de contener caracteres de la cadena siguiente: “2345679qwertyupadfgjhjxcvbnms”.

Es preferible no colocar caracteres iguales, ya que al encontrar el carácter correspondiente, no tienes que perder el tiempo averiguando cual de ellos es.

006AE01A	837D F8 00	CMP DWORD PTR SS:[EBP-8],0	
006AE01E	75 0C	JNZ SHORT pixedit.006AE02C	
006AE020	A1 B4397100	MOV EAX,DWORD PTR DS:[7139B4]	
006AE025	8B00	MOV EAX,DWORD PTR DS:[EAX]	
006AE027	E8 20FFFFFF	CALL pixedit.006ADF40	
006AE02C	837D F4 00	CMP DWORD PTR SS:[EBP-C],0	
006AE030	75 16	JNZ SHORT pixedit.006AE048	
006AE032	B9 68E26A00	MOV ECX,pixedit.006AE268	ASCII "Please enter email used in your order"
006AE037	B2 01	MOV DL,1	
006AE039	A1 04844000	MOV EAX,DWORD PTR DS:[408404]	
006AE03E	E8 71E7D5FF	CALL pixedit.0040C7B4	
006AE043	E8 C858D5FF	CALL pixedit.00403910	
006AE048	8B45 F8	MOV EAX,DWORD PTR SS:[EBP-8]	
006AE04B	E8 F460D5FF	CALL pixedit.00404144	
006AE050	83F8 0A	CMP EAX,0A	
006AE053	7D 0C	JGE SHORT pixedit.006AE061	
006AE055	A1 B4397100	MOV EAX,DWORD PTR DS:[7139B4]	
006AE05A	8B00	MOV EAX,DWORD PTR DS:[EAX]	
006AE05C	E8 EBFFFFFF	CALL pixedit.006ADF40	
006AE061	8D55 E0	LEA EDI,DWORD PTR SS:[EBP-20]	
006AE064	8B33 F8020000	MOV EAX,DWORD PTR DS:[EBX+2F8]	
006AE06A	E8 2080D8FF	CALL pixedit.00436090	
006AE06F	8B45 E0	MOV EAX,DWORD PTR SS:[EBP-20]	
006AE072	E8 C970EAFB	CALL pixedit.00555140	
006AE077	85C0	TEST EAX,EAX	
006AE079	74 0A	JE SHORT pixedit.006AE085	
006AE07B	B8 98E26A00	MOV EAX,pixedit.006AE298	ASCII "Wrong key."
006AE080	E8 C7FFFFFF	CALL pixedit.006ADF40	
006AE085	8B45 F8	MOV EAX,DWORD PTR SS:[EBP-8]	
006AE088	E8 1371EAFB	CALL pixedit.005551A0	
006AE08D	8B93 08030000	MOV EDI,DWORD PTR DS:[EBX+308]	
006AE093	8B45 F8	MOV EAX,DWORD PTR SS:[EBP-8]	
006AE096	E8 316FEAFB	CALL pixedit.00554FC0	
006AE09B	85C0	TEST EAX,EAX	
006AE09D	74 0A	JE SHORT pixedit.006AE0A9	
006AE09F	B8 ACE26A00	MOV EAX,pixedit.006AE2AC	ASCII "Wrong key for this application."
006AE0A4	E8 A3FFFFFF	CALL pixedit.006ADF40	
006AE0A9	B2 01	MOV DL,1	

En la imagen anterior se ve claramente en la llamada de la dirección 006AE027 comprueba que has introducido un correo electrónico correctamente, con la @ y el “.loquesea”.

La llamada situada en la dirección 006AE04B comprueba que el largo de la key , y la comparación siguiente que el largo de la key sea, “A” osea 10 en decimal.

Si el largo de la key es “A”, pasas el corte del salto situado en la dirección 006AE053.

En la llamada situada en la dirección 006AE072 nos lleva a la imagen siguiente.

00555161	B8 0A000000	MOV EBX,0A	
00555166	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
00555169	E8 6AFDFFFF	CALL pixedit.00554ED8	
0055516E	03F0	ADD ESI,EAX	
00555170	6A 64	PUSH 64	
00555172	E8 B922EBFF	CALL <JMP.&kernel32.Sleep>	[Timeout = 100. ms Sleep
00555177	4B	DEC EBX	
00555178	75 EC	JNZ SHORT pixedit.00555166	

Este bucle es repetido 10 veces, que es el largo de la key.

Dentro de esta call o llamada, hay un bucle que repite la comprobación del primer carácter de la key correcta, que está situada en la llamada de la dirección 00555169, como muestra la imagen siguiente.

00554F36	E8 09F2EAFB	CALL pixedit.00404144	
00554F38	4B	DEC EAX	
00554F3C	83E8 02	SUB EAX,2	
00554F3F	7C 14	JL SHORT pixedit.00554F55	
00554F41	40	INC EAX	
00554F42	BA 02000000	MOV EDI,2	
00554F47	8B4D FC	MOV ECX,DWORD PTR SS:[EBP-4]	
00554F4A	0FB64C11 FF	MOVZX ECX,BYTE PTR DS:[ECX+EDX-1]	
00554F4F	33D9	XOR EBX,ECX	
00554F51	42	INC EDI	
00554F52	4B	DEC EAX	
00554F53	75 F2	JNZ SHORT pixedit.00554F47	
00554F55	8BC3	MOV EAX,EBX	
00554F57	B9 1E000000	MOV ECX,1E	
00554F5C	99	CDQ	
00554F5D	F7F9	IDIV ECX	
00554F5F	42	INC EDI	
00554F60	B8 AC4F5500	MOV EAX,pixedit.00554FAC	ASCII "2345679qwertyupadfg hjkzxcvbnms"
00554F65	8A4410 FF	MOV AL,BYTE PTR DS:[EAX+EDX-1]	
00554F69	8B55 FC	MOV EDI,DWORD PTR SS:[EBP-4]	
00554F6C	304432 FF	CMP AL,BYTE PTR DS:[EDI+ESI-1]	
00554F70	74 03	JE SHORT pixedit.00554F75	

Esta es la zona de generación de nuestro carácter correspondiente, que realmente es el segundo, aunque el segundo lo comprueba después.

Si ponemos un punto de ruptura en la dirección 00554F6C, nos daremos cuenta que compara nuestro carácter falso con el verdadero, que lo coloca en la ultima posición , ya que para comprobar la key elimina, el primer y último carácter.

Estando parados en esa dirección, podemos cambiar directamente, el carácter real por el que hemos colocado nosotros a través del dump, en todas las referencias que hay en la pila o stack.

Si miramos la primera imagen de código, en la llamada situada en 006AE088, nos introduce en la siguiente imagen.

005551A0	53	PUSH EBX	
005551A1	8BD8	MOV EBX,EAX	
005551A3	8BC3	MOV EAX,EBX	
005551A5	E8 2EFDFFFF	CALL pixedit.00554ED8	
005551AA	85C0	TEST EAX,EAX	
005551AC	74 16	JE SHORT pixedit.005551C4	
005551AE	B9 00515500	MOV ECX,pixedit.005551D0	ASCII "Invalid key"
005551B3	B2 01	MOV DL,1	
005551B5	A1 04844000	MOV EAX,DWORD PTR DS:[408404]	
005551BA	E8 F575EBFF	CALL pixedit.0040C7B4	
005551BF	E8 4CE7EAFF	CALL pixedit.00403910	
005551C4	5B	POP EBX	
005551C5	C3	RETN	

En la pila, os daréis cuenta de que hay 6 referencias a la key, tres de ellas pertenecen a la llamada o call anterior y las otras 3 a la llamada situada en la dirección 005551A5 de esta otra imagen. Que realiza la misma operación.

La siguiente comprobación que realiza y la dirección a la llamada situada en 006AE096 correspondiente a la primera imagen, nos introduce en la parte de código que genera el segundo carácter, que realmente debería ser el primer carácter de nuestra key.

00555004	E8 07FEFFFF	CALL pixedit.00554E10	
00555009	8B55 F0	MOV EDX,DWORD PTR SS:[EBP-10]	
0055500C	8045 FC	LEA EAX,DWORD PTR SS:[EBP-4]	
0055500F	E8 48FEFAFF	CALL pixedit.00403F50	
00555014	8045 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
00555017	E8 28F1EAFF	CALL pixedit.00404144	
0055501C	83F8 07	CMP EAX,7	
0055501F	7D 0A	JGE SHORT pixedit.0055502B	
00555021	BE 0B000000	MOV ESI,0B	
00555026	E9 C1000000	JMP pixedit.005550EC	
0055502B	337D F8 00	CMP DWORD PTR SS:[EBP-8],0	
0055502F	0F84 B7000000	JE pixedit.005550EC	
00555035	33DB	XOR EBX,EBX	
00555037	8B45 F8	MOV EAX,DWORD PTR SS:[EBP-8]	
0055503A	E8 05F1EAFF	CALL pixedit.00404144	
0055503F	48	DEC EAX	
00555040	85C0	TEST EAX,EAX	
00555042	7E 13	JLE SHORT pixedit.00555057	
00555044	BA 01000000	MOV EDI,1	
00555049	8B4D F8	MOV ECX,DWORD PTR SS:[EBP-8]	
0055504C	0FB64C11 FF	MOVBX ECX,BYTE PTR DS:[ECX+EDX-1]	
00555051	03D9	ADD EBX,ECX	
00555053	42	INC EDI	
00555054	48	DEC EAX	
00555055	75 F2	JNZ SHORT pixedit.00555049	
00555057	8BC3	MOV EAX,EBX	
00555059	B9 1E000000	MOV ECX,1E	
0055505E	99	CDQ	
0055505F	F7F9	IDIV ECX	
00555061	42	INC EDI	
00555062	B8 20515500	MOV EAX,pixedit.00555120	
00555067	8A4410 FF	MOV AL,BYTE PTR DS:[EAX+EDI-1]	
0055506B	8B55 FC	MOV EDX,DWORD PTR SS:[EBP-4]	
0055506E	3A42 01	CMP AL,BYTE PTR DS:[EDI+1]	
00555071	74 01	JE SHORT pixedit.00555074	ASCII "2345679qwertyupadfg hjkzxcvbnms"

Ante todo decir que la cadena que recoge para generar nuestro carácter es : “Pixel Editor” de la cual solo recorre el bucle hasta la “o”. Cuando a terminado de recorrer el bucle situado entre las direcciones 00555049 y 00555055, divide el resultado de 417 entre 1E en hexadecimal o 1047 entre 30 en decimal.

El resto de esta división pertenece al carácter fijo “n”, que lo sitúa en la 6ª posición de nuestra key. Como se puede comprobar en la dirección 0055506E.

Resumiendo:

Para poder registrar este programa a parte de comprarlo, se debe introducir en la 6ª posición una “n” y después pasar la primera generación del primer carácter, modificando en el dump las referencias que aparecen en la pila o stack, continuando con la ejecución del programa, hasta el momento que sale el mensaje “reinicie la aplicación”, por supuesto la mejor forma de reiniciar el programa, es recargarlo en Olly y pulsar F9.

Donde el resultado es el esperado.



PD: hay varios softwares que utilizan la misma forma de crear la key, no los voy a colocar en este tutorial, pero para el que sea curioso, puede colocar en google la cadena “2345679qwertyupadfg hjkzxcvbnms” y saldrán unas cuantas entradas.

4 – 7 – 2016.

Alberto Fernández.