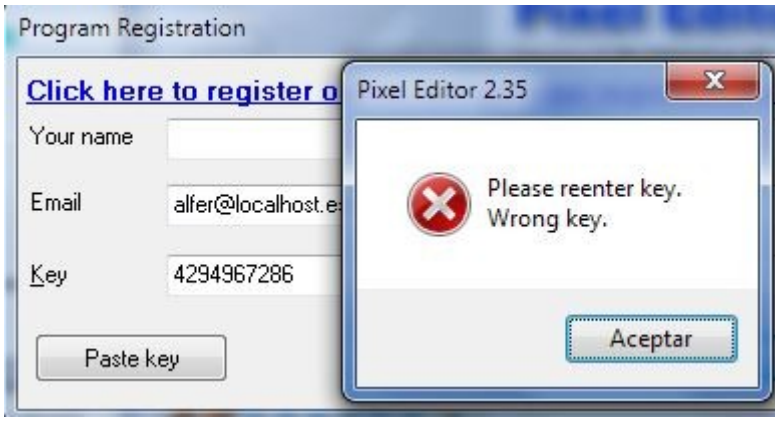
URL	http://www.iconempire.com/
Victima	Pixel Editor
Herramientas	Olly 1.1
Cracker	Alberto Fernández
Dificultad	Un poco complicado
Fecha	4 – 7 - 2016

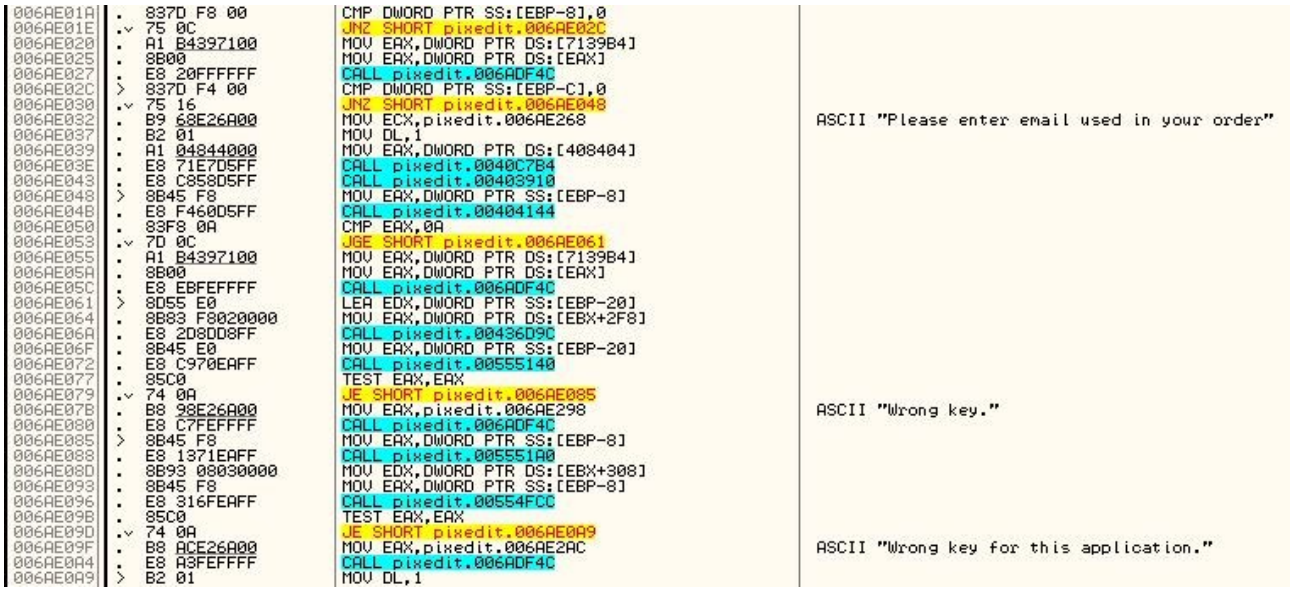
Hola, ya estamos aquí otra vez, primero miramos el tipo de protección que tiene.

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: “2345679qwertyupadfghjkzxcvbnms”.

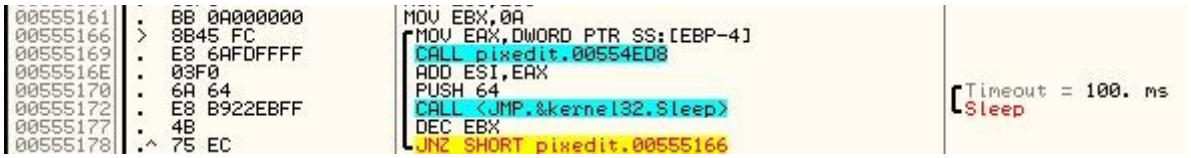
Es preferible no colocar caracteres iguales, ya que al encontrar el carácter correspondiente, no tienes que perder el tiempo averiguando cual de ellos es.



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”.

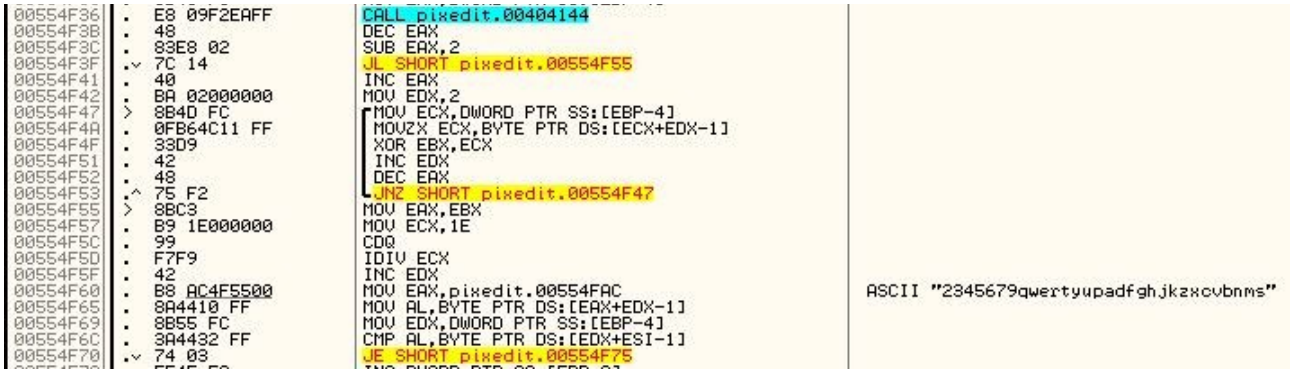
La llamada situada en la dirección 006AE04B comprueba que el largo de la key , y la comparación siguiente que el largo de la key sea, “A” osea 10 en decimal.

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.



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.

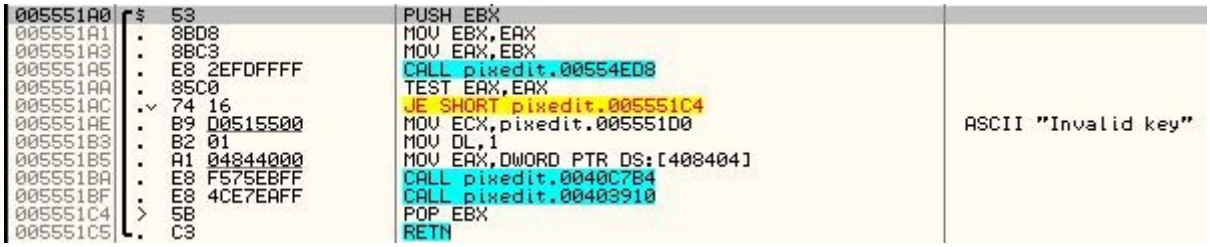


Esta es la zona de generación de nuestro carácter correspondiente, que realmente es el segundo, aunque el segundo lo comprueba después.

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

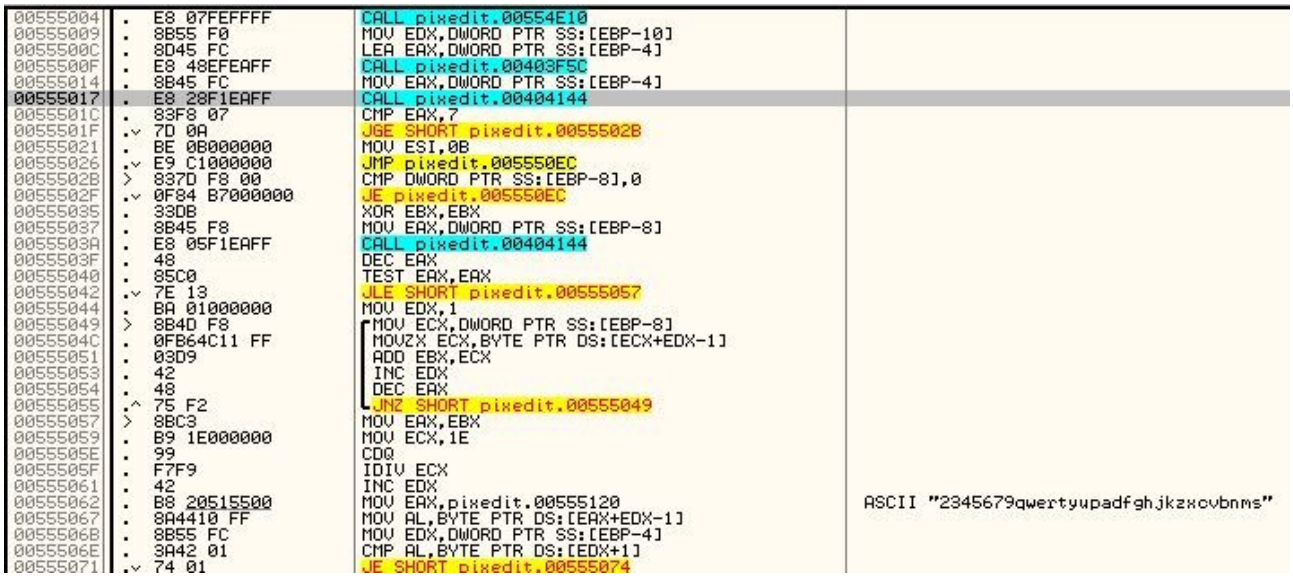
Estando parados en esa dirección, podemos cambiar directamente, el carácter real por el que hemos colocado nosotros a través del dump, en todas las referencias que hay el la pila o stack.

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



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.



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 6º 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 6º 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 “2345679qwertyupadfghjkzxcvbnms” y saldrán unas cuantas entradas.

4 – 7 – 2016.

Alberto Fernández.