



ESET CRACKME #35

By CLS



29 DE AGOSTO DE 2017

APUROMAFO

www.apuromafo.net

Índice

Contenido

Índice	1
Introducción	3
Cifrado1:Hexadecimal.....	6
Cifrado2 Binario.....	7
Cifrado3 Base64.....	7
Cifrado4 Decimal/char	7
Cifrado5 Url Encode	7
Conclusión	14

Datos del Programa

Programa	Eset Crackme 35
Descarga	Ahí el reto
Dificultad	Depende de quien lo mire
Información	https://www.welivesecurity.com/la-es/2017/08/28/desafio-entrada-gratuita-para-ekoparty/
Fecha	29/08/2017
Cracker	Apuromafo
Colaboración indirecta (motivación)	DavicoRm, Lior, Nox

Todas las cosas buenas que existen son el fruto de la originalidad. John Stuart Mill (1806 - 1873); filósofo y economista británico

Herramientas:

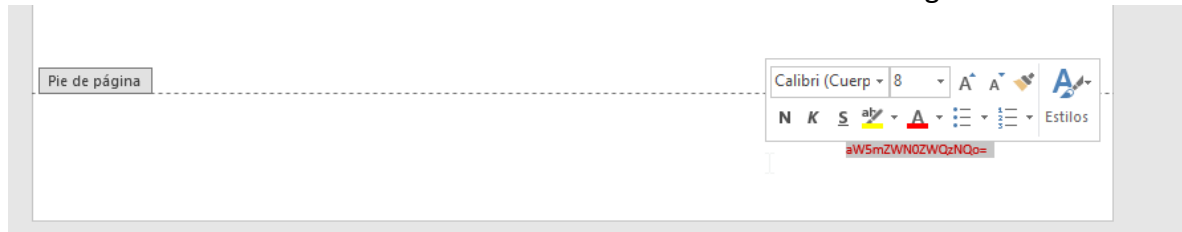
Herramientas	Descarga	Descripción
Procesador de texto	<i>(está incluido con el suite de office)</i>	Para redactar el tutorial
Sharex	https://getsharex.com/	Para capturar las imágenes
Everything	http://www.voidtools.com/	Para buscar los archivos en el pc
Dnsnp	https://ci.appveyor.com/project/0xd4d/dnsnp/build/artifacts	Para archivos .net
De4dot	https://github.com/0xd4d/de4dot	Para desofuscar .net
7zip	http://www.7-zip.org/a/7z1604.exe	decomprimir

Servicios webs

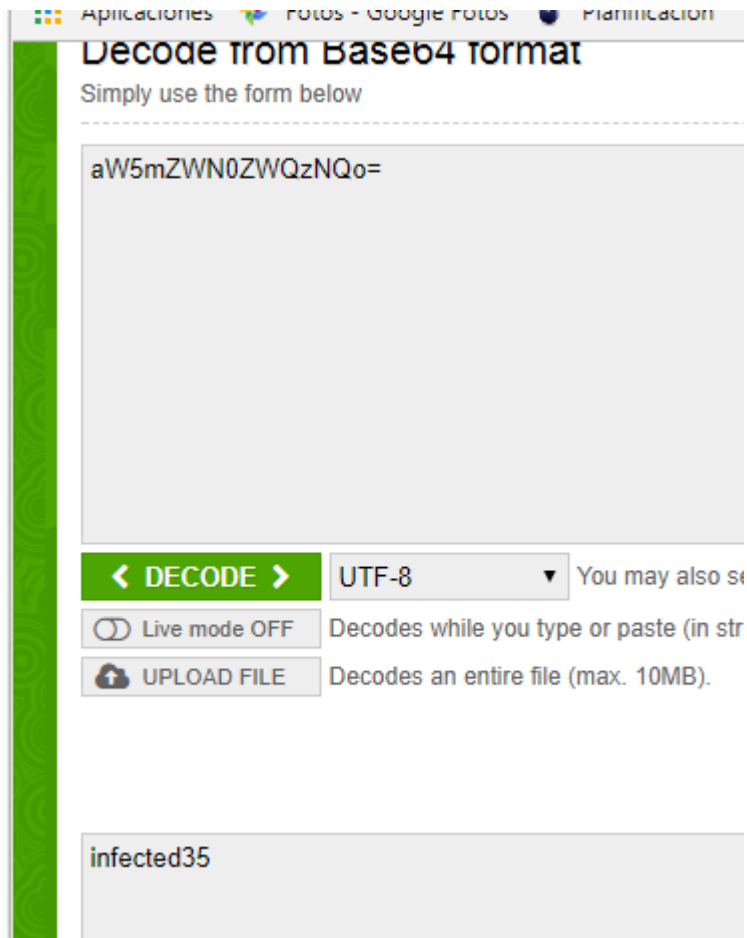
Hex a string	http://string-functions.com/hex-string.aspx
Base64 decode	https://www.base64decode.org/
String reverse	http://string-functions.com/reverse.aspx
Binario a string	http://www.traductorbinario.com/#binario
Decimal a string	https://cryptii.com/decimal/text
Url decode	https://meyerweb.com/eric/tools/dencoder/

Introducción

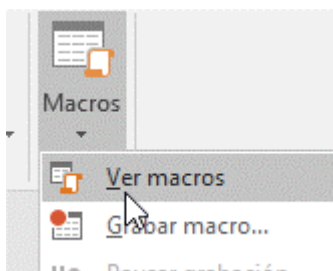
Hola a todos, con un poco de tiempo me he motivado a dejar de recuerdo esta pequeña entrada de un desafio de eset, en la página de información (en la tabla inicial) refiere que debemos descargar el archivo docm (documentos mas macro) del cual tendrá el link de descarga, al abrir el archivo alerta sobre las macros y al verlas tenemos un archivo en blanco, en pie de pagina tenemos una información oculta, al cambiar de color tenemos una string “aW5mZWN0ZWQzNQo=“



primera pagina que decodifique la base64 es



Asumimos que tenemos el password , falta ver el archivo (asumo que esta en las macros)



Al ver la macro tenemos esto

```
Sub downloader()
MsgBox "Busca la URL para la descarga del archivo y la contraseña que lo descomprime"
End Sub

'Function Cifrado1()
'Private Const ALG_CLASS_ANY As Long = 0 Private Const ALG_TYPE_ANY As Long = 0
' 70 69 7a 2e 35 33 5f 54 45 53 45 5f 30 31 46 41 53 33 44
' Private Const ALG_CLASS_HASH As Long = 32768
' Private Const ALG_TYPE_BLOCK As Long = 1536
' Private Const ALG_CLASS_DATA_ENCRYPT As Long = 24576
' Private Const ALG_SID_RC2 As Long = 2
' Private Const ALG_SID_SHA1 As Long = 4
' Private Const CALG_SHA1 As Long = ALG_CLASS_HASH Or ALG_TYPE_ANY Or
ALG_SID_SHA1
' Private Const CALG_RC2 As Long = ALG_CLASS_DATA_ENCRYPT Or
ALG_TYPE_BLOCK Or ALG_SID_RC2
' Private Const PROV_RSA_FULL As Long = 1
' Private Const CRYPT_VERIFYCONTEXT As Long = &HF0000000
' Private Const MS_DEFAULT_PROVIDER As String = "Función de cifrado 1"
' Private Const CRYPT_NO_SALT As Long = &H10
'End Function

'Function Cifrado2()
'Private Const ALG_CLASS_ANY As Long = 0 Private Const ALG_TYPE_ANY As Long = 0
' Private Const ALG_CLASS_HASH As Long = 32768
' Private Const ALG_TYPE_BLOCK As Long = 1536
' Private Const ALG_CLASS_DATA_ENCRYPT As Long = 24576
' Private Const ALG_SID_RC2 As Long = 2
' Private Const ALG_SID_SHA1 As Long = 4
' Private Const CALG_SHA1 As Long = ALG_CLASS_HASH Or ALG_TYPE_ANY Or
ALG_SID_SHA1
' Private Const CALG_RC2 As Long = ALG_CLASS_DATA_ENCRYPT Or
ALG_TYPE_BLOCK Or ALG_SID_RC2
' Private Const PROV_RSA_FULL As Long = 1
' Private Const CRYPT_VERIFYCONTEXT As Long = &HF0000000
```

```
' Private Const MS_DEFAULT_PROVIDER As String = "Función de cifrado 2"
' Private Const CRYPT_NO_SALT As Long = &H10
' 00101111 00111000 00110000 00101111 00110111 00110001 00110000 00110010
'End Function
```

```
'Function Cifrado3()
```

```
'Private Const ALG_CLASS_ANY As Long = 0 Private Const ALG_TYPE_ANY As Long = 0
' Private Const ALG_CLASS_HASH As Long = 32768
' Private Const ALG_TYPE_BLOCK As Long = 1536
' Private Const ALG_CLASS_DATA_ENCRYPT As Long = 24576
' Private Const ALG_SID_RC2 As Long = 2
' Private Const ALG_SID_SHA1 As Long = 4
' Private Const CALG_SHA1 As Long = ALG_CLASS_HASH Or ALG_TYPE_ANY Or
ALG_SID_SHA1
' Private Const CALG_RC2 As Long = ALG_CLASS_DATA_ENCRYPT Or
ALG_TYPE_BLOCK Or ALG_SID_RC2
' Private Const PROV_RSA_FULL As Long = 1
' Private Const CRYPT_VERIFYCONTEXT As Long = &HF0000000
' Private Const MS_DEFAULT_PROVIDER As String = "Función de cifrado 3"
' L3NkYW9schUvdG5ldG5vYy1wdw==
' Private Const CRYPT_NO_SALT As Long = &H10
'End Function
```

```
'Function Cifrado4()
```

```
'Private Const ALG_CLASS_ANY As Long = 0 Private Const ALG_TYPE_ANY As Long = 0
' Private Const ALG_CLASS_HASH As Long = 32768
' Private Const ALG_TYPE_BLOCK As Long = 1536
' Private Const ALG_CLASS_DATA_ENCRYPT As Long = 24576
' Private Const ALG_SID_RC2 As Long = 2
' Private Const ALG_SID_SHA1 As Long = 4
' Private Const CALG_SHA1 As Long = ALG_CLASS_HASH Or ALG_TYPE_ANY Or
ALG_SID_SHA1
' Private Const CALG_RC2 As Long = ALG_CLASS_DATA_ENCRYPT Or
ALG_TYPE_BLOCK Or ALG_SID_RC2
' 47 109 111 99 46 121 116 105 114 117 99 101 115 101 118 105 108 101 119 46 119
119 119
' Private Const PROV_RSA_FULL As Long = 1
' Private Const CRYPT_VERIFYCONTEXT As Long = &HF0000000
' Private Const MS_DEFAULT_PROVIDER As String = "Función de cifrado 4"
' Private Const CRYPT_NO_SALT As Long = &H10
'End Function
```

```
'Sub SetPasswordOptions()
```

```
'Function Cifrado5()
```

```

'Private Const ALG_CLASS_ANY As Long = 0 Private Const ALG_TYPE_ANY As Long = 0
' Private Const ALG_CLASS_HASH As Long = 32768
' Private Const ALG_TYPE_BLOCK As Long = 1536
' Private Const ALG_CLASS_DATA_ENCRYPT As Long = 24576
' Private Const ALG_SID_RC2 As Long = 2
' Private Const ALG_SID_SHA1 As Long = 4
' %2F%2F%3Asptth
' Private Const CALG_SHA1 As Long = ALG_CLASS_HASH Or ALG_TYPE_ANY Or
ALG_SID_SHA1
' Private Const CALG_RC2 As Long = ALG_CLASS_DATA_ENCRYPT Or
ALG_TYPE_BLOCK Or ALG_SID_RC2
' Private Const PROV_RSA_FULL As Long = 1
' Private Const CRYPT_VERIFYCONTEXT As Long = &HF0000000
' Private Const MS_DEFAULT_PROVIDER As String = "Función de cifrado 5"
' Private Const CRYPT_NO_SALT As Long = &H10
'End Function

'Sub SetPasswordOptions()
' ActiveWorkbook.SetPasswordEncryptionOptions _
' PasswordEncryptionProvider:="Microsoft RSA SChannel Cryptographic Provider", _
' PasswordEncryptionAlgorithm:="RC4", _
' PasswordEncryptionKeyLength:=56, _
' PasswordEncryptionFileProperties:=True
'End Sub

```

Cifrado1:Hexadecimal

Dado que encontramos la información un poco confusa vemos que hay varios sub, intentemos decodificar con lo básico

```
'Function Cifrado1()
```

```
'70 69 7a 2e 35 33 5f 54 45 53 45 5f 30 31 46 41 53 33 44
```

Parece hex , convertimos a string con el servicio web obtenemos

```
piz.53_TESE_01FAS3D
```

Cifrado2 Binario

'Function Cifrado2()

'00101111 00111000 00110000 00101111 00110111 00110001 00110000 00110010

Cambiamos de binario a string se obtiene

/80/7102

Cifrado3 Base64

'Function Cifrado3()

' L3NkYW9scHUvdG5ldG5vYy1wdw==

'base 64 a string

/sdaolpu/tnetnoc-pw

Cifrado4 Decimal/char

Function Cifrado4()

' 47 109 111 99 46 121 116 105 114 117 99 101 115 101 118 105 108 101 119 46 119 119 119

'decimal a string

/moc.ytirucesevilew.www

Cifrado5 Url Encode

'Function Cifrado5()

' %2F%2F%3Asptth

'url encoded... al hacer decode

//:sptth

Si vemos todas las partes tenemos cadenas extrañas, la ultima sobre todo, luego meditando necesitamos reversar la string y tenemos entonces la pagina de descarga del programa

En orden de cifrado 5, 4, 3, 2, 1

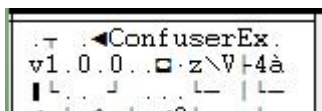
https://www.welivesecurity.com/wp-content/uploads/2017/08/D3SAF10_ESET_35.zip

Al abrir el archivo con la contraseña correcta (ya descrita antes) para todo lo demás además tenemos que lo demás sirve para guardar la contraseña formato rc4

```
'Este ejemplo establece las opciones de cifrado de contraseña para el libro activo.  
'https://msdn.microsoft.com/es-es/library/office/ff196907.aspx  
'Sub SetPasswordOptions()  
' ActiveWorkbook.SetPasswordEncryptionOptions _  
' PasswordEncryptionProvider:="Microsoft RSA SChannel Cryptographic Provider", _  
' PasswordEncryptionAlgorithm:="RC4", _  
' PasswordEncryptionKeyLength:=56, _  
' PasswordEncryptionFileProperties:=True  
'End Sub
```

Comenzamos a explorar el programa que estaba comprimido en zip(usamos 7zip), luego tenemos un archivo en .net

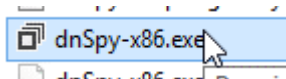
Al ver la propiedad del documento refiere estar ofuscado con



confuserEx 1.0.0. , normalmente tenemos que pensar que nuestro exe será una tela de cebolla, muchas capas y cada una ejecuta una instrucción en particular, tiene detección anti-tamper, por lo que una vez ejecutada una capa, hay que anular la anterior y dumpear ☺, mas menos el proceso son como 3 veces, comenzamos a ver con una herramienta específica...

Para depurar un archivo .net usaremos dnspy, se puede hacer punto de interrupción una vez que tengamos el programa ejecutado y luego ir viendo hasta donde llegamos.

Dado que tenemos un programa en 86 bytes tendremos que usar este



Y porsiacaso tenemos uno a medio desofuscar

```

de4dot v3.1.41592.3405 Copyright (C) 2011-2015 de4dot@gmail.com
Latest version and source code: https://github.com/0xd4d/de4dot

== Support .Net Reactor5.0.0.0 Fixed By Wuhensoft ==

Detected Unknown Obfuscator (C:\Users\PC\Downloads\Comprinidos\D3SAF10_ESET_35\D
3SAF10_ESET_35.exe)
Cleaning C:\Users\PC\Downloads\Comprinidos\D3SAF10_ESET_35\D3SAF10_ESET_35.exe
Renaming all obfuscated symbols
Saving C:\Users\PC\Downloads\Comprinidos\D3SAF10_ESET_35\D3SAF10_ESET_35-cleaned
.exe

Press any key to exit...

```

Recuerden que hay videos en youtube explicando como funciona el unpack a este ofuscador donde muestran los pasos uno de ellos ejemplo este:

https://www.youtube.com/watch?v=X0F_-sE-6GU

Una vez desempacado, logramos leer el form principal (Form1)

```

Imports System
Imports System.ComponentModel
Imports System.Diagnostics
Imports System.Drawing
Imports System.Runtime.CompilerServices
Imports System.Windows.Forms
Imports Microsoft.VisualBasic
Imports Microsoft.VisualBasic.CompilerServices

<DesignerGenerated()>
Public Class Form1
    Inherits Form

    ' Token: 0x02000016 RID: 22
    Public Sub New()
        AddHandler MyBase.Load, AddressOf Me.Form1_Load
        Me.InitializeComponent()
    End Sub

    Private Sub method_0(sender As Object, e As EventArgs)
    End Sub

    Private Sub method_1(sender As Object, e As EventArgs)
        Me.method_2(Me.TextBox1.Text)
        Me.TextBox1.SelectAll()
    End Sub

    Private Function method_2(string_0 As String) As Nullable
        Dim text As String = ""
        Me.method_3(☺)
        ' The following expression was wrapped in a checked-statement

```

```

If string_0.Length <> 15 Then
    Interaction.MsgBox("Bandera incorrecta" & vbCrLf & "Sigue intentando",
MsgBoxStyle.Critical, "D3SAF10 ESET #35")
Else
    Dim num As Integer = string_0.Length - 1
    For i As Integer = 0 To num
        text += Conversions.ToString(Convert.ToChar(Convert.ToInt32(string_0(i)) Xor 31))
    Next
    If Operators.CompareString(text, Me.method_☺), False) <> 0 Then
        Interaction.MsgBox("Bandera incorrecta" & vbCrLf & "Sigue intentando",
MsgBoxStyle.Critical, "D3SAF10 ESET #35")
    Else
        Interaction.MsgBox("Bandera correcta" & vbCrLf & "Acceso garantizado",
MsgBoxStyle.Information, "D3SAF10 ESET #35")
    End If
End If
Dim result As Nullable
Return result
End Function

Private Function method_☺) As String
    Dim text As String = "!#$%&()*+,-
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]_abcdefghijklmnopqrstuvwxyz{|}~"
    Dim array As String() = Strings.Split("85,79,75,29,84,78,89,83,29,84,75,69,76,86,27", ",", -1,
CompareMethod.Binary)
    Dim text2 As String = ""
    ' The following expression was wrapped in a checked-statement
    Dim num As Integer = array.Length - 1
    For i As Integer = 0 To num
        text2 += Conversions.ToString(text(Convert.ToInt32(array(i))))
    Next
    Return text2
End Function

Private Sub Form1_Load(sender As Object, e As EventArgs)
    MyBase.AcceptButton = Me.Button1
    Me.TextBox1.[Select]()
End Sub

Private Sub method_4(sender As Object, e As EventArgs)
End Sub

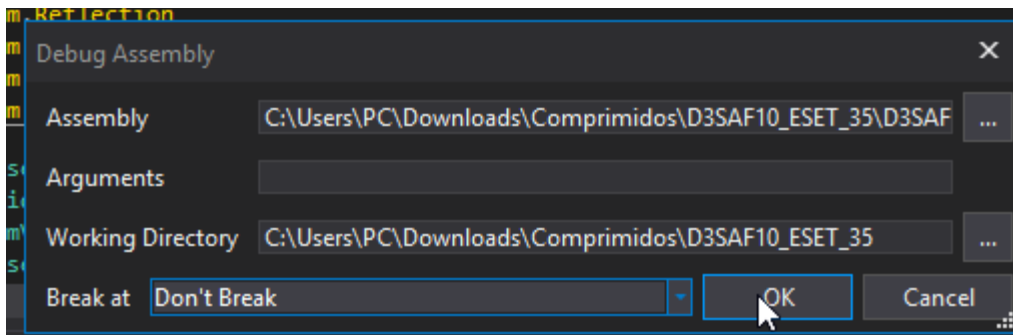
<DebuggerNonUserCode()>
Protected Overridable Sub Dispose(disposing As Boolean)
    Try
        If disposing AndAlso Me.icontainer_0 IsNot Nothing Then
            Me.icontainer_0.Dispose()
        End If
    End Try
End Sub

```

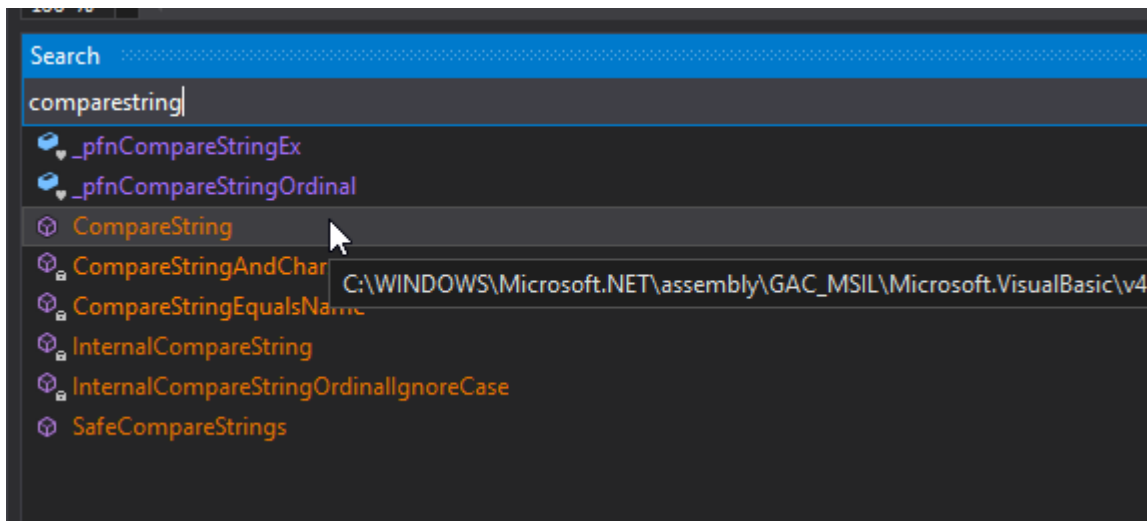
```
Finally  
    MyBase.Dispose(disposing)  
End Try  
End Sub
```

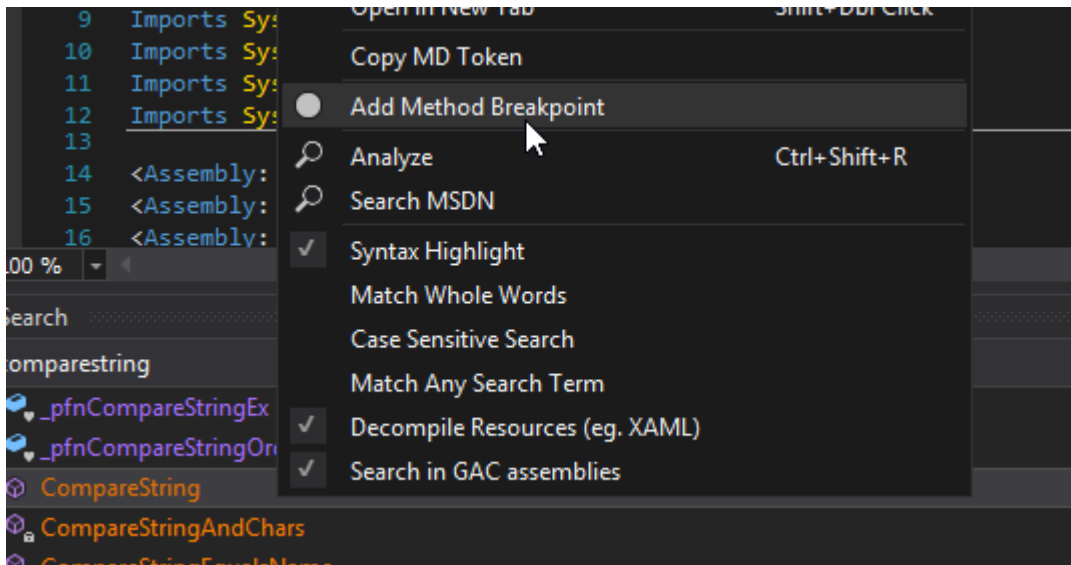
Se resume que el programa valida 15 caracteres , los cuales hace una conversión a decimal, a xor 31 y compara con el valor predeterminado que hace una comparación en binario...por lo que tenemos 1 punto de referencia real “ **If Operators.CompareString**”

Comparestring depuramos el desafio de eset 25

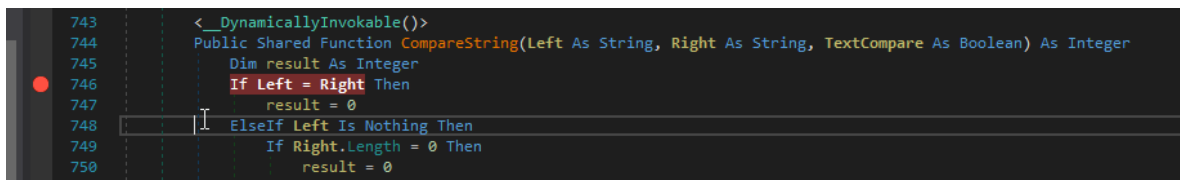


Colocamos a buscar comparestring pues colocaremos bp

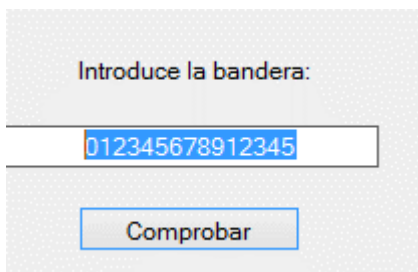




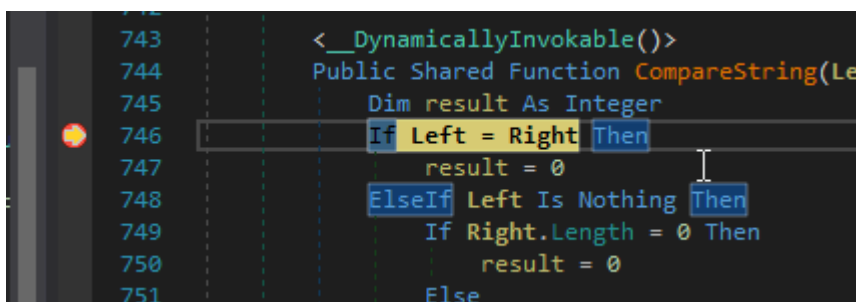
Queda así



Introducimos la bandera (clave) de 15 cifras



Al pulsar comprobar tenemos



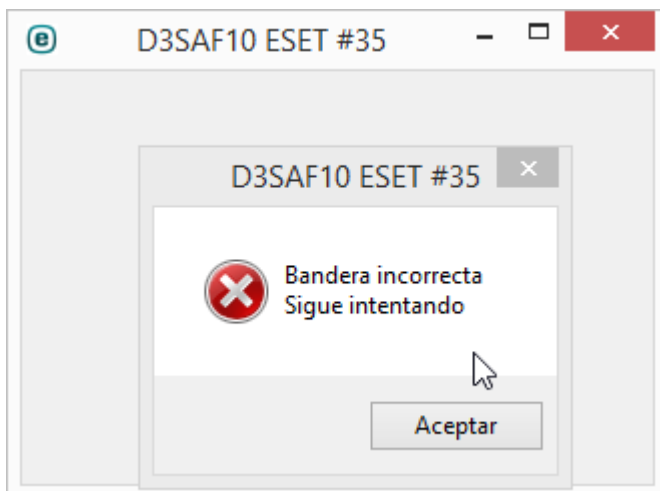
Al cerrar la búsqueda me muestra la comparación de un texto ingresado según un alfabeto especial (posible cifrado caesar/cesar) mas xor 31, versus un string (cifrado)

Locals		
Name	Value	Type
Left	"/./,+*)('&L-,*+""	string
Right	"ztp@ys~x@ypjq{>"	string
TextCompare	false	bool
result	0x00000000	int
num	0x00000000	int

Lo apunto

ztp@ys~x@ypjq{>

Luego



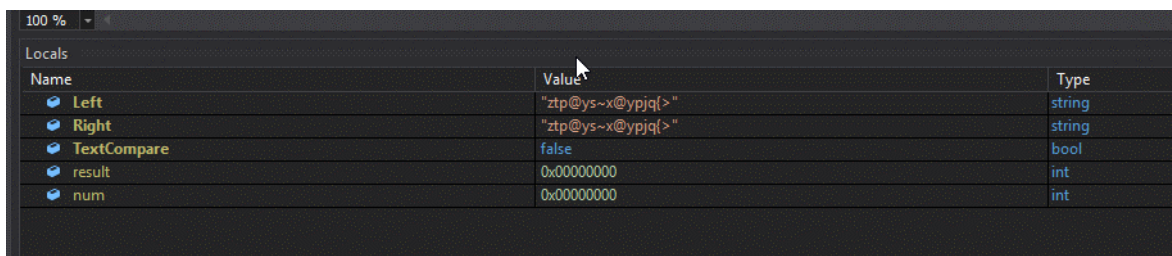
Copio el mismo texto encontrado (si hay xor, dará la vuelta tarde o temprano)

Locals	
Name	Value
Left	"eko_flag_found!"
Right	"ztp@ys~x@ypjq{>"
TextCompare	false
result	0x00000000
num	0x00000000

Me muestra el string mas entendible,

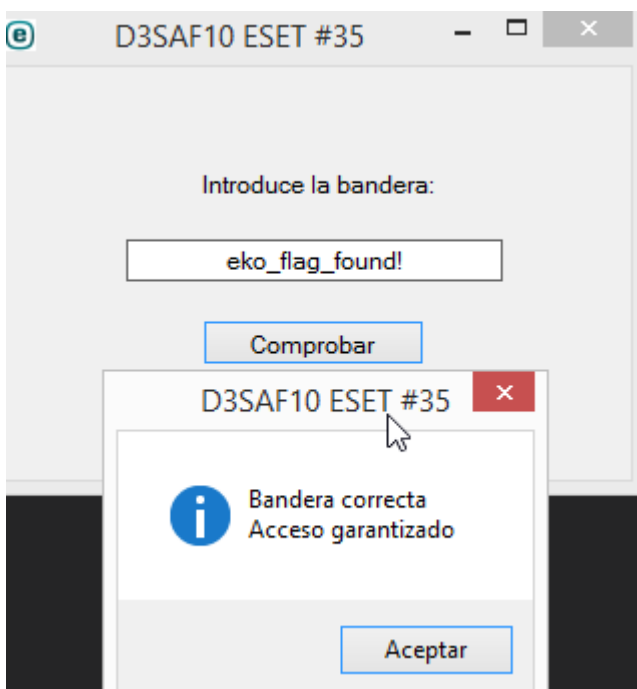
eko_flag_found!

Al ingresar la palabra correcta compara 2 veces lo mismo 😊



Name	Value	Type
Left	"ztp@ys~x@ypjq{>"	string
Right	"ztp@ys~x@ypjq{>"	string
TextCompare	false	bool
result	0x00000000	int
num	0x00000000	int

Llegando a

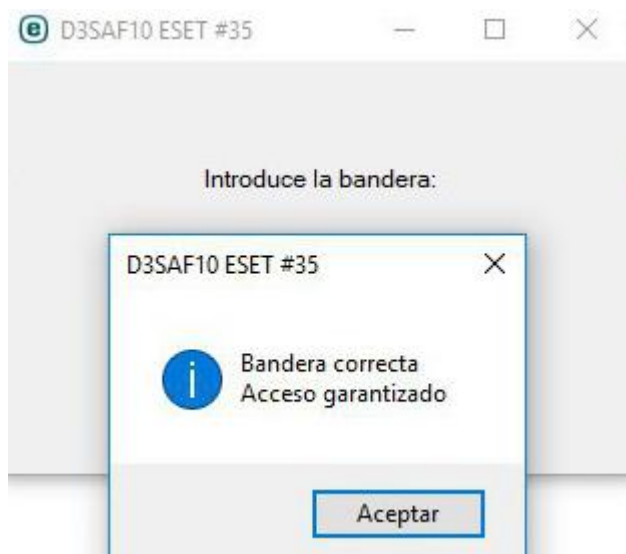


Conclusión

Hemos resuelto un desafío 😊, pero nada de esto sería sin la ayuda de los amigos de siempre que están ahí apoyando que se puede 😊

Un abrazo para Lior, Abel, Davico, Ricardo Narvaja y a todos los que se dedican a tener un poco de tiempo para leer y participar en muchos temas.

Y como no a ti por leer este escrito



Saludos Cordiales



Apuromafo TSKh