



---

# YO PRESTO 3.9

---

Herramienta que gestiona Préstamos con intereses by Apuromafo



25 DE MAYO DE 2018

CLS

Release:25/05/2018

# INDICE

## Contenido

INDICE .....	1
Introducción .....	2
Frase.....	2
Herramientas usadas en el Escrito: .....	2
Analizando la víctima: .....	3
Palabras Finales.....	8

## Introducción

Programa	<b><i>Yo presto 3.9.5361</i></b>
Descarga	<a href="https://www.yopresto.com/es">https://www.yopresto.com/es</a> <a href="http://www.soradev.com">http://www.soradev.com</a>
Dificultad	Depende de quien lo mire.
Objetivo	Registrarnos o que sea funcional.
Información	Archivo .net con packer Confuser Setup en Inno
Herramientas usadas	De4dot, dnspy
Fecha	28/05/2018
Cracker	Apuromafo

## Frase.

"Muchos buscan la felicidad como otros buscan el sombrero:  
lo llevan encima y no se dan cuenta"  
— Nikolaus Lenau

## Herramientas usadas en el Escrito:

<b>Herramienta</b>	<b>Descarga</b>	<b>Utilidad</b>
<b>Procesador de texto</b> <b>Hoja de cálculo</b>	<i>(está incluido con el suite de office)</i>	<b>Para redactar el tutorial</b>
<b>Sharex</b>	<a href="https://getsharex.com/">https://getsharex.com/</a>	<b>Para capturar las imágenes</b>
<b>Everything</b>	<a href="http://www.voidtools.com/">http://www.voidtools.com/</a>	<b>Para buscar los archivos en el pc</b>
<b>Notepad ++ *</b>	<a href="https://notepad-plus-plus.org/">https://notepad-plus-plus.org/</a>	<b>Editar archivos (no hexadecimal)</b>
<b>Cff Explorer</b>	<a href="http://www.ntcore.com/files/ExplorerSuite.exe">http://www.ntcore.com/files/ExplorerSuite.exe</a>	<b>Editor de recursos , explorador de pe header</b>
<b>De4dot</b>	<a href="http://blog.apuromafo.net/?p=695">http://blog.apuromafo.net/?p=695</a>	<b>Desencriptar el exe .net</b>
<b>DNSPY</b>	<a href="http://blog.apuromafo.net/?p=695">http://blog.apuromafo.net/?p=695</a>	<b>Modificar el exe .net</b>
<b>Reflector</b>	<a href="http://blog.apuromafo.net/?p=695">http://blog.apuromafo.net/?p=695</a>	<b>Modificar el exe .net</b>

\* Herramienta opcional

## Historia :

Hola, por mi privado me han pedido ayuda con este programa, como no soy avaro con lo que se, aquí le comparto un breve escrito del hecho .

## Analizando la víctima:

Sin mas comentar es un archivo .net , lo arrastro a de4dot-Support.Reactor5.0-wuhensoft , el que viene con crackers kits, y obtengo un archivo .cleaned.exe hasta aquí no hay complicación.

En lo general : en about vemos

```
' Token: 0x0200009F RID: 159
Public Sub New(licencia As MainWindow.LicenciaTipo)
    Me.InitializeComponent()
    Dim entryAssembly As Assembly = Assembly.GetEntryAssembly()
    Dim name As AssemblyName = entryAssembly.GetName()
    Dim version As Version = name.Version
    Me.version.Content = String.Concat(New Object() { version.Major, ".", version.Minor, ".",
        version.Build })
    Select Case licencia
        Case MainWindow.LicenciaTipo.Demo
            Me.description.Text = "Licencia: Demo"
        Case MainWindow.LicenciaTipo.Principal
            Me.description.Text = "Licencia: Principal"
        Case MainWindow.LicenciaTipo.Caja
            Me.description.Text = "Licencia: Caja"
        Case MainWindow.LicenciaTipo.[Global]
            Me.description.Text = "Licencia: Global"
    End Select
End Sub
```

La validación de la licencia se hace en mainWindow.Licencia Tipo, esta es usada en muchos lugares  
Si intentamos fishear un serial tipo

Validador

```

43 Dim array As String() = New String(serie.Length / 5 + If((serie.Length Mod 5 = 0), 0, 1) - 1) {}
44 For i As Integer = 0 To serie.Length - 1
45     Dim array2 As String() = array
46     Dim array3 As String() = array2
47     Dim num As Integer = i / 5
48     Dim intPtr As IntPtr = CType(num, IntPtr)
49     array2(num) = array3(CInt(intPtr)) + serie(i)
50 Next
51 Dim array4 As ULong() = New ULong(array.Length - 1) {}
52 For j As Integer = 0 To array.Length - 1
53     If j Mod 2 = 0 Then
54         array4(j) = Validador.ToDec(array(j), 36UI)
55     Else
56         array4(j) = Validador.ToDec(array(j), 37UI)
57     End If
58 Next
59 Dim text As String = ""

```

100 %

Locales

Nombre	Valor	Tipo
string.Length.get devuelto	0x00000008	int
Tipo	Principal	yoPresto.Validador.LicenciaTipo
serie	"64960444"	string
array	string[0x00000002]	string[]
array[0]	"64960"	string
array[1]	"444"	string
i	0x00000008	int
array3	null	ulong[]
j	0x00000000	int
text	null	string
array2	string[0x00000002]	string[]
array2[0]	"64960"	string
array2[1]	"444"	string

Podemos apreciar como valida las licencias numéricas, pero para hacer algo mas eterno , intentaré forzar que me diga la licencia que yo quiero, para esto basta analizar el tipo de licencia de donde es usado en dsnp y veamos que tenemos:

LicenciaTipo @0200015E

Exposed By

Extension Methods

Used By

- yoPresto.GClass3..ctor(SetterDataSet.UsersRow, MainWindow.LicenciaTipo) : Void @060007BB
- yoPresto.GClass3.AJMAFFVTNITYHIUNKERYLG() : Void @060007BC
- yoPresto.GClass3.DCMCOWDPNQICWIAJXNVSSK() : Boolean @06000803
- yoPresto.GClass3.ECZSQMKRGSCUEIJCQUZ() : Boolean @060007DC
- yoPresto.GClass3.EYQKDAGIIZUXXOOJWSRTN() : Void @060007CC
- yoPresto.GClass3.IMRBYBSIAHHCHPZGWEXIG(Object, RoutedEventArgs) : Void @06000802
- yoPresto.GClass3.Licencia : MainWindow.LicenciaTipo @1700020D
- yoPresto.GClass3.OWYJYRTISDSQTJZQLOZWOM() : Void @060007D5
- yoPresto.GClass3.RDFMHNTZZWOQTFQEBLPUUR : MainWindow.LicenciaTipo @0400043B
- yoPresto.GClass3.SIAZCMPDBAASJBRFGFJHKG(Object, RoutedEventArgs) : Void @060007E3
- yoPresto.MainWindow.FNHAWYACKSVOQCCEUMJYRE(Object, RoutedEventArgs) : Void @060001
- yoPresto.MainWindow.getLicKey(MainWindow.LicenciaTipo, String) : String @0600178F
- yoPresto.MainWindow.Licencia : MainWindow.LicenciaTipo @1700063C
- yoPresto.MainWindow.NMQPOQANLMMPTFBVYRMX() : Void @06001798
- yoPresto.MainWindow.PGIIRVMXFRBBFLYWFLQRQF(Object, RoutedEventArgs) : Void @060017E2
- yoPresto.MainWindow.RDFMHNTZZWOQTFQEBLPUUR : MainWindow.LicenciaTipo @040009E2
- yoPresto.MainWindow.SAXQALCCQORWGYRGDQWXIM(Object, RoutedEventArgs) : Void @0600
- yoPresto.MainWindow.TGAABLMYSKOUXUWYIGZZKO(Object, RoutedEventArgs) : Void @060017
- yoPresto.MainWindow.Validar(String) : MainWindow.LicenciaTipo @06001790
- yoPresto.MainWindow.ValidarRemota(String) : MainWindow.LicenciaTipo @06001791
- yoPresto.MainWindow.WLAAQXPJBDDGDKAFDHDNSB() : MainWindow.LicenciaTipo @06001796
- yoPresto.MainWindow.XBJFNLGQYAJTHODUVSYLVQ() : Void @0600178D
- yoPresto.winAbout..ctor(MainWindow.LicenciaTipo) : Void @060008FA
- yoPresto.winUsers..ctor(MainWindow.LicenciaTipo) : Void @060008F0
- yoPresto.winUsers.BPDWIHPUXIRYKZLREXKD(Object, RoutedEventArgs) : Void @060008F4
- yoPresto.winUsers.RQXLSRHKYNDRWVERWVRYT : MainWindow.LicenciaTipo @040005E2

licencia

XBJFNLGQYAJTHODUVSYLVQ()

Try

```
Dim entryAssembly As Assembly = Assembly.GetEntryAssembly()
Dim name As AssemblyName = entryAssembly.GetName()
Dim version As Version =
FrameworkElement.LanguageProperty.OverrideMetadata(GetType(FrameworkElement), New FrameworkPropertyMetadata(XmlLanguage.GetLanguage(CultureInfo.CurrentCulture.GetLanguageTag)))
MyBase.Title = String.Concat(New String() { name.Name, ", version:Major.ToString()", version.Minor.ToString() })
Me.SVCORCHFWLUGCATUATRF = "N6352eatMwptans.now.and.then"
```

```
Me.Licencia = MainWindow.LicenciaTipo.Demo
```

```
Me.FOYLPEIPQBDQCZFKAGLQZl)
Me.BNMSXCXSAKUHFHAXHOUPQl)
IF YRGAESDVLDVQFKBUHHOGL[Default].firstTime Then
    Me.GXWWECHFFUJFGGGQZQ = Text
    YRGAESDVLDVQFKBUHHOGL[Default].Upgrade()
    YRGAESDVLDVQFKBUHHOGL[Default].firstTime = false
End If
YRGAESDVLDVQFKBUHHOGL[Default]("sora6045_ydclntesConnectionString" = "server=soradev.com;User Id=sora6045_sora;password=-q9ybfm;database=sora6045_ydclntes
Mybase.Background = New SolidColorBrush(Color.FromInt(YRGAESDVLDVQFKBUHHOGL[Default].BackColorGroundColor, YRGAESDVLDVQFKBUHHOGL[Default].BackColorGroundColor.I))
If File.Exists(YRGAESDVLDVQFKBUHHOGL[Default].Logo) Then
    Me.ImpLogo.Source = New BitmapImage(New Uri(YRGAESDVLDVQFKBUHHOGL[Default].Logo))
End If
Me.THIYOWUKQBJWRBWFNLFT = New DispatcherTimer()
Me.THIYOWUKQBJWRBWFNLFT.Interval = TimeSpan.FromMilliseconds(500.0)
AddHandler Me.THIYOWUKQBJWRBWFNLFT.Tick, AddressOf Me.GLEVBNEVZRWVWFFNLVDI)
Me.popupNotifier.PlacementTarget = Me.MenuMain
Me.popupNotifier.Placement = PlacementMode.Custom
Me.popupNotifier.CustomPopupPlacementCallback = AddressOf Me.placePopupRight
Me.KYPINRUMEJUFVUULFWK = New DispatcherTimer()
Me.KYPINRUMEJUFVUULFWK.Interval = TimeSpan.FromMilliseconds(500.0)
AddHandler Me.KYPINRUMEJUFVUULFWK.Tick, AddressOf Me.LTUHYPRKAENGAWBPEL)
Me.SAEBNEIDIAUJETMJQZ = New BackgroundWorker()
AddHandler Me.SAEBNEIDIAUJETMJQZ.DoWork, AddressOf Me.NXNMZAFZAZIDEHNMNLTV
AddHandler Me.SAEBNEIDIAUJETMJQZ.RunWorkerCompleted, AddressOf Me.OQPDGDEEEXQWHDLPNQMY
```

Me.Licencia = Me.WLAAQXPJBDDGDKAHDNSB()

```
Dim licencia As MainWindow.LicenciaTipo = Me.Licencia
```

```

        licencia <- MainWindow.LicenciaTipo.Caja.Text
        YRRGASOVDLWQFKBUHGOGL[default].globalDir = Environment.CurrentDirectory
        Tr
        End If
        Process.Start(New String[] { "use ""\\YRRGASOVDLWQFKBUHGOGL[default].DB_Server"" / users", YRRGASOVDLWQFKBUHGOGL[default].DB_Server }, Encoding.Default(YRRGASOVDLWQFKBUHGOGL[default].DB_Pass, sharedSecret))
    End If
End Sub

```

```
If MainWindow.ValidarRemota(YRRGAESDVDLWQFKBUHHOGL.[Default].globalDir + "\\lic.key") <> MainWindo
```

w.LicenciaTipo.Principal Then

Me.AXXNBXJZDHRTFYDNGERPQ = True

```

End If
End If
If Me.Licenses < MainWindow.LicenciaTipo (Global Then
    If Me.AXNBKZ0HRTYONGERPO Then
        Datos.Connected = False
    Else
        YRGAESDVLWQFKBUHHOGL (Default) ("yoPConnectionString") = String.Concat (New String () { "data source="; YRGAESDVLWQFKBUHHOGL (Default) GlobalId; ", Archives\yoP.db3; Password="; Char.ConvertFromUTF32 (34); Me.SVQRCFHFWLUGGATUATRF; Char.ConvertFromUTF32 (34);
        YRGAESDVLWQFKBUHHOGL (Default) ("SetConnectionString") = String.Concat (New String () { "data source="; YRGAESDVLWQFKBUHHOGL (Default) GlobalId; ", Archives\Set.db3; Password="; Char.ConvertFromUTF32 (34); Me.SVQRCFHFWLUGGATUATRF; Char.ConvertFromUTF32 (34);
        YRGAESDVLWQFKBUHHOGL (Default) ("LogConnectionString") = String.Concat (New String () { "data source="; YRGAESDVLWQFKBUHHOGL (Default) GlobalId; ", Archives\Logs.db3; Password="; Char.ConvertFromUTF32 (34); Me.SVQRCFHFWLUGGATUATRF; Char.ConvertFromUTF32 (34);
        Datos.Connected = True
    }
}

```

End If

```
If Me.Licencia = MainWindow.LicenciaTipo.Principal OrElse Me.Licencia = MainWindow.LicenciaTipo.Demo Th
```

en

Me.NRUEGMQHPLNQEGGJYCHWMK()

Me.DNCGNLVRMYJYQPNASGMDY()

If Me.CSWWJEEYFCFLIJFGGGGZOX Then

End If

[illegible]

el lugar que valida la licencia claramente establece el tipo de licencia, así que si retorna demo, todos los demás lugares saben que es demo, pero si cambiamos que diga otro tipo de licencia, las demás también heredarán esa licencia:

```

53 008D ldarg.0
54 008E ldstr      "N6352FeatMYpants,now,and,theN"
55 0093 stfld      string yoPresto.MainWindow::SCVQRCFHFKWLUCGATUATRF
56 0098 ldarg.0
57 0099 ldc.i4.1
58 009A call       instance void yoPresto.MainWindow::set_Licencia(valuetype yoPresto.MainWindow/LicenciaTipo)

```

El bloque queda así

```
Me.Licencia = MainWindow.LicenciaTipo.Principal
```

El ldc.i4.0 carga demo, si dejamos a 4.1 entonces queda principal y así suma y sigue las licencias.

También se puede modificar en reflexil (reflector)

The screenshot shows the Reflexil application interface. On the left, a list of assemblies is shown, with 'yoPresto 3.9' selected. The main area displays the 'Method definition' for 'set\_Licencia'. The 'Instructions' tab is active, showing a table of instructions:

Offset	OpCode	Op
82	202	stloc.s ->
83	204	leave.s ->
84	206	ldc.i4.1
85	207	stloc.s ->
86	209	ldloc.s ->
87	211	ret

The 'Method definition' tab shows the following code:

```

Dim str5 As String = MainWindow.getLicKey(DirectCast(Integer.Parse(ch.ToString), LicenciaTipo), driv
If (((str5 = str3) AndAlso (str3 <> "")) AndAlso (str5 <> "")) Then
    Dim num As Integer = Integer.Parse(INKZHCWCPYMOORLWTDZTEI.Chars(0).ToString)
    If ((num < 4) AndAlso MainWindow.CITYWKDDWCRZVAIWJYNOGI(driveId, INKZHCWCPYMOORLW
        Return DirectCast(num, LicenciaTipo)
    End If
End If
End If
Catch obj1 As Object
    Return LicenciaTipo.Principal
End Try
Return LicenciaTipo.Principal
End Function

```

The application window on the right shows the 'yoPresto 3.9' interface with the 'Licencia: Principal' field.

veamos como quedan todos los lugares con licencia tipo principal:

```

        End If
    End If
Catch
    Return MainWindow.LicenciaTipo.Principal
End Try
Return MainWindow.LicenciaTipo.Principal
End Function

Public Shared Function ValidarRemota(licFile As String) As MainWindow.LicenciaTipo
Try
    If File.Exists(licFile) Then
        Dim streamReader As StreamReader = New StreamReader(licFile)
        Dim text As String = streamReader.ReadLine()
        Dim a As String = streamReader.ReadLine()
        If a <> "" AndAlso text.Length > 5 Then
            Return CType(Integer.Parse(text(0).ToString()), MainWindow.LicenciaTipo)
        End If
    End If
Catch
    Return MainWindow.LicenciaTipo.Principal
End Try
Return MainWindow.LicenciaTipo.Principal
End Function

Public Shared Function DecTo(num As ULong, baseNum As UInteger) As String
Dim text As String = ""
While num <> 0UL
    Dim num2 As ULong = num Mod CULng(baseNum)
    Dim str As String = num2.ToString()


```



Cuando modificamos (demo a principal ) queda así:  
y eso es todo.



Respecto a sus licencias debería tener subscripcion quien lo necesite usarlo de forma cotidiana:




Prueba

- ✓ 10 préstamos
- ✓ Compras, Ventas y Apartados
- ✓ Algunos reportes

**Gratis**

No requiere tarjeta de crédito

Seleccionar




YoPresto Mensual

- ✓ Préstamos y Clientes ilimitados
- ✓ Compras, Ventas y Apartados
- ✓ Todos los reportes
- ✓ Empleados ilimitados

**599 MXN / mes**

Por sucursal

Seleccionar



YoPresto Anual

- ✓ Préstamos y Clientes ilimitados
- ✓ Compras, Ventas y Apartados
- ✓ Todos los reportes
- ✓ Empleados ilimitados
- ✓ **Dos meses de descuento**

599-MXN

**499 MXN / mes**

Cobrado anualmente por sucursal

Seleccionar

Todos los precios se muestran en Pesos Mexicanos (MXN).

Eso es todo.

#### Palabras Finales

El programa esta protegido, al desproteger se logra apreciar que tiene muchas cadenas interesantes en .net , pero dejar todo manejado en un solo lugar como demo deja para pensar que cambiará con el tiempo.

Saludos Cordiales Apuromafo CLS

