

# 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	Yo presto 3.9.5361
Descarga	https://www.yopresto.com/es
	http://www.soradev.com
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:

Herramienta	Descarga	Utilidad
Procesador de texto Hoja de cálculo	(está incluido con el suite de office)	Para redactar el tutorial
Sharex	https://getsharex.com/	Para capturar las imágenes
Everything	http://www.voidtools.com/	Para buscar los archivos en el pc
Notepad ++ *	https://notepad-plus-plus.org/	Editar archivos (no hexadecimal)
Cff Explorer	http://www.ntcore.com/files/Exp lorerSuite.exe	Editor de recursos , explorador de pe header
De4dot	http://blog.apuromafo.net/?p=69	Desencriptar el exe .net
DNSPY	http://blog.apuromafo.net/?p=69	Modificar el exe .net
Reflector	http://blog.apuromafo.net/?p=69	Modificar el exe .net

<sup>\*</sup> 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 .

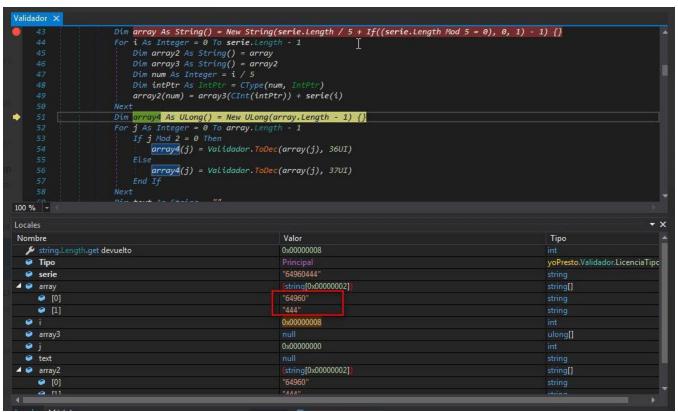
#### Analizando la víctima:

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

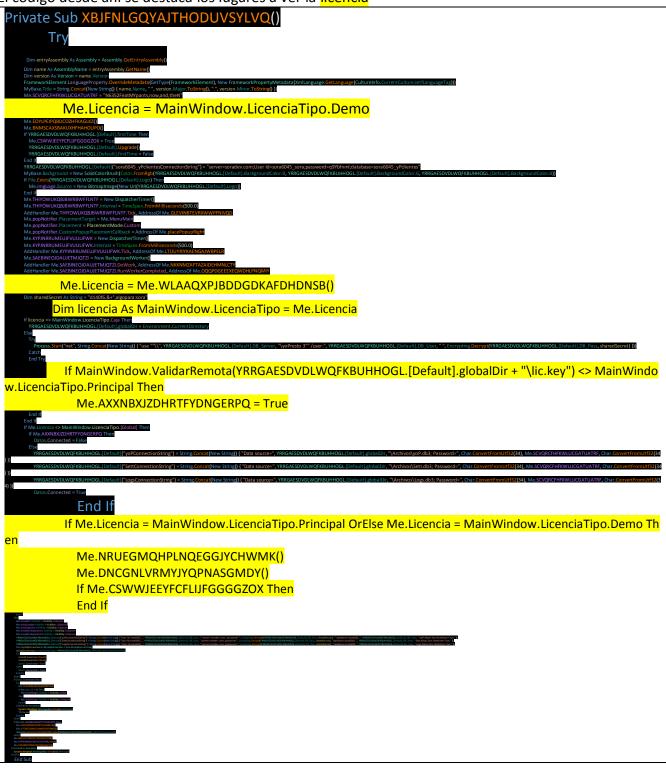
```
Public Sub New(licencia As MainWindow.LicenciaTipo)
   Me.InitializeComponent()
   Dim entryAssembly As Assembly = Assembly.GetEntryAssembly()
   Dim name As AssemblyName = entryAssembly.GetName()
   Dim version As Version = name.Version
   Me.version.Content = String.Concat(New Object() { version.Major, ".", 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



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 dsnpy y veamos que tenemos:

El código desde ahí se destaca los lugares a ver la licencia



el lugar que valida la licencia claramente establece el tipo de licencia, asi 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

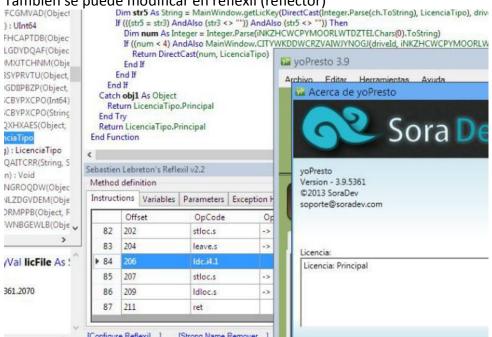
57 0099 ldc.i4.1

58 009A call instance void yoPresto.MainWindow::set_Licencia(valuetype yoPresto.MainWindow/LicenciaTipo)
```

El bloque queda asi

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)



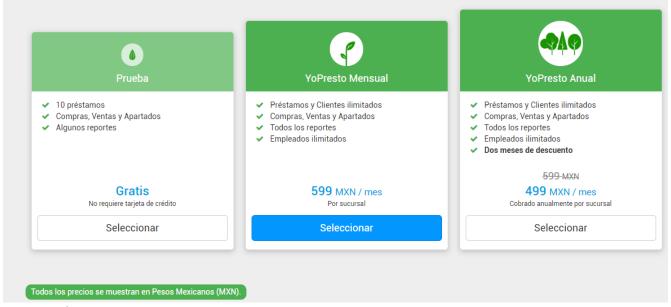
veamos como quedan todos los lugares con licencia tipo principal:

```
End If
        End If
        Return MainWindow.LicenciaTipo.Principal
 Return MainWindow.LicenciaTipo.Principal
Public Shared Function ValidarRemota(licFile As String) As MainWindow.LicenciaTipo
        If File.Exists(licFile) Then
           Dim streamReader As StreamReader = New StreamReader(licFile)
           Dim text As String = streamReader.ReadLine()
           Dim a As String = streamReader.ReadLine()
                Return CType(Integer.Parse(text(0).ToString()), MainWindow.LicenciaTipo)
            End If
       End If
       Return MainWindow.LicenciaTipo.Principal
   Return MainWindow.LicenciaTipo.Principal
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:



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

