

## Manual Modificar Stub's en VBasic

Pongo en VBasic por que solo podran modificar los que esten creados con ese lenguaje xD!.

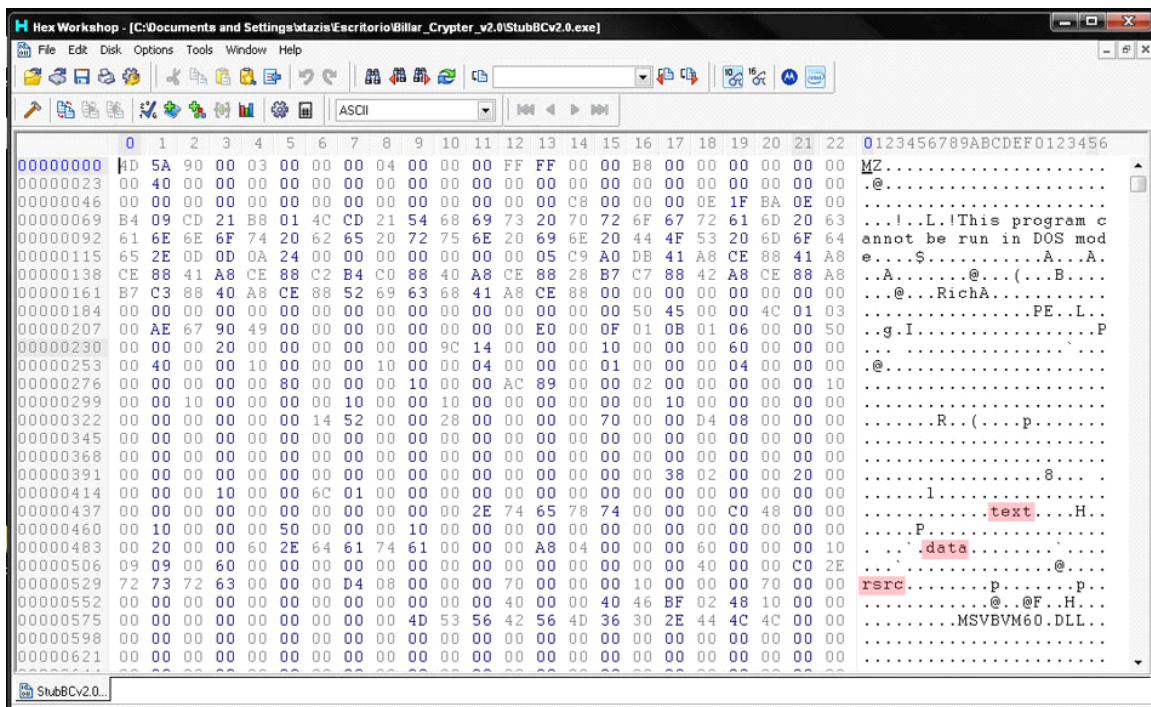
Primero aclarar que esto es para hacer antes de buscar los offsets y todo el procedimiento de firmas,asi siempre se caen algunos antivirus y después hacen el proceso de localizarlas con los manuales que hay en el foro creados para eso.Es para los usuarios nuevos más que nada ya que és muy fácil.

Yo voy hacer la prueba con el stub del **Billar\_Crypter\_v2.0** que sin hacerle nada lo detectan

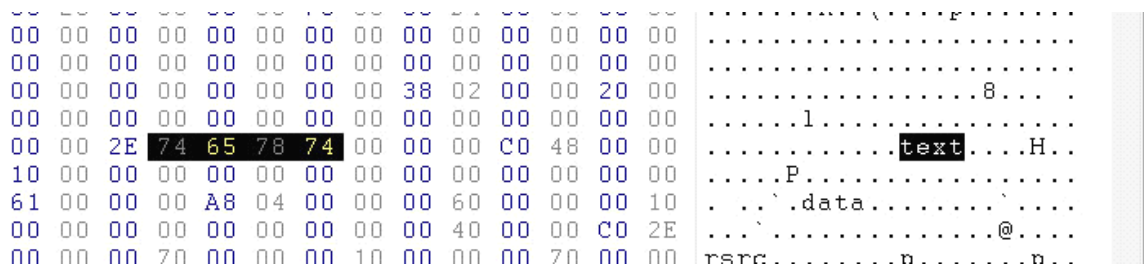
Detection Rate:	9 on 24 (37,5 %)
Status:	INFECTED

Antivirus	Sig version	Engine Version	Result
a-squared	24/03/2009	4.0.0.32	Riskware.Win32.VBInject!IK
Avira AntiVir	7.1.2.208	8.1.2.12	-
Avast	090323-0	4.8.1229	Win32:Trojan-gen (Other)
AVG	270.11.25/2019	8.0.0.0	Dropper.Generic.AJCA
BitDefender	24/03/2009	7.0.0.2555	Trojan.Crypt.VB.M
ClamAV	24/03/2009	0.93.1.0	-
Comodo	1082	3.8	-
Dr.Web	24/03/2009	5.0	Trojan.DownLoader.46203
Ewido	24/03/2009	4.0.0.2	-
F-PROT 6	20090323	4.4.4.56	W32/VBTrojan.2!Generic (damaged)
G DATA	19.3655	2.0.7309.847	-
IkarusT3	24/03/2009	1001044	VirTool.Win32.VBInject
Kaspersky	24/03/2009	8.0.0.357	-
McAfee	24/03/2009	5.1.0.0	-
Malware Hash Registry	24/03/2009	N/A	-
NOD32 v3	3957	3.0.677	-
Norman	2009/03/23	5.92.08	Trojan.W32/Agent.LUUC
Panda	07/02/2009	9.5.1.00	-
QuickHeal	24 March, 2009	10.0	Trojan.Agent2.eeh
Solo Antivirus	24/03/2009	8.0	-
Sophos	24/03/2009	4.32.0	-
TrendMicro		1.1-1001	-
VBA32	24/03/2009	3.12.0.300	-
VirusBuster	10.102.19	1.4.3	-

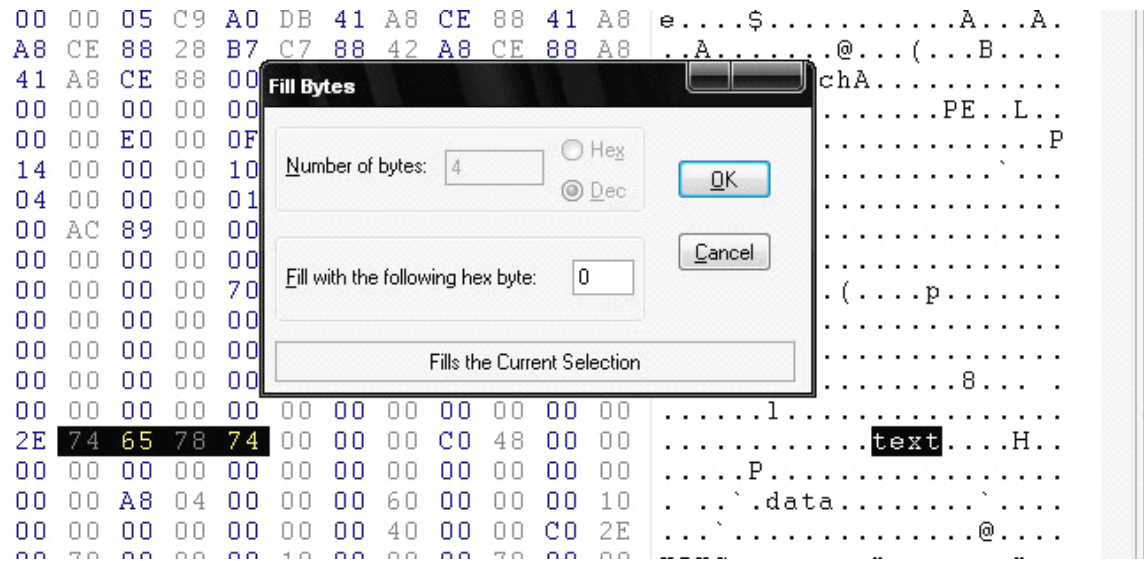
Bien ahora abrimos el stub con el **Hex**



en la parte derecha esta marcado en rojo lo que tenemos que modificar, marcamos el "text" por ejemplo asi



y ahora solo hacemos **Ctrl+Ins** nos saldra esta ventana



figaros que este el " **Fill with the following hex byte:**" a 0,y le damos a **OK** y tendremos esto

```

00 00 AC 09 00 00 02 00 00 00 00 00 10
10 00 00 00 00 00 00 10 00 00 00 00
28 00 00 00 00 70 00 00 D4 08 00 00
00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 38 02 00 00 20 00
00 00 00 00 00 00 00 00 00 00 00 00
00 2E 00 00 00 00 00 00 00 C0 48 00 00
00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 A8 04 00 00 00 00 60 00 00 10
00 00 00 00 00 00 00 00 40 00 C0 2E
.....R..(....p.....
.....8.....
.....l.....
.....H.....
.....P.....
...data.....
...@.....

```

hacemos lo mismo con el "data y el rsr" quedando asi

```

00000299 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 10 00 00 00 00 00
00000322 00 00 00 00 00 00 00 14 52 00 00 28 00 00 00 00 00 70 00 00 D4 08 00 00
00000345 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000368 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000391 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 02 00 00 20 00
00000414 00 00 00 10 00 00 00 6C 01 00 00 00 00 00 00 00 00 00 00 00 00 00
00000437 00 00 00 00 00 00 00 00 00 00 00 00 00 2E 00 00 00 00 00 C0 48 00 00
00000460 00 10 00 00 00 00 50 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00
00000483 00 20 00 00 60 2E 00 00 00 00 00 00 A8 04 00 00 00 60 00 00 00 10
00000506 09 09 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0 2E
00000529 00 00 00 00 00 00 00 D4 08 00 00 00 70 00 00 00 10 00 00 00 70 00
00000552 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 46 RF 02 48 10 00 00
.....R..(....p.....
.....8.....
.....l.....
.....H.....
.....P.....
...data.....
...@.....

```

una vez terminado esto nos vamos más abajo

**NOTA:** No todos los stubs en VBasic estarán igual,me refiero a los textos que vamos a modificar ahora en este caso se llama stub pero eso no importa se hace de la misma forma...

Si los textos estan mayúsculas los ponemos en minúsculas,si estan en minúsculas en mayúsculas

en este caso donde esta el texto "**STUBDOS**" y lo que haremos será poner el texto en



[illegible][illegible]

una vez cambiados estos vamos al texto "VB5" y le ponemos la V en v y al "VB6ES" lo mismo...asi

```
00005488 AC 24 40 00 07 00 00 00 18 23 40 00 07 00 00 00 22 40 00 07 00 00 88 22 40 00 .5@.....#e....."e.
00005516 07 00 00 00 34 22 40 00 07 00 00 EC 21 40 00 07 00 00 A0 21 40 00 07 00 00 00 ..4"e.....!e.....l@.
00005544 08 20 40 00 07 00 00 00 C0 1F 40 00 07 00 00 00 74 1F 40 00 07 00 00 2C 1F 40 00 .e.....e.....t.e.....e.
00005572 07 00 00 00 E4 1E 40 00 07 00 00 00 98 1E 40 00 07 00 00 50 1E 40 00 07 00 00 00 ..e.....e.....P.e.....
00005600 08 1E 40 00 07 00 00 00 C0 1D 40 00 07 76 42 35 21 F0 1F 76 42 36 45 53 2E 44 4C 00 .e.....e.vB5!..vB6ES.DLL.
00005628 00 00 00 00 2A 00 00 00 00 00 00 00 00 00 00 00 0A 00 0A 0C 00 00 09 04 00 00 P*e.....e.....0.....
00005656 50 2A 40 00 CC 17 40 00 00 F0 30 00 00 FF FF FF 08 00 00 01 00 00 00 00 00 00 00 P*e.....e.....0.....
00005684 F9 00 00 00 F4 14 40 00 F4 14 40 00 3A 14 40 00 7A 00 00 00 70 00 00 00 A2 00 00 00
```

y ya esta lo guardamos y cerramos el Hex,el resultado del stub modificado en mí caso este

Detection Rate:	4 on 24 (16,66 %)
Status:	INFECTED

Antivirus	Sig version	Engine Version	Result
a-squared	24/03/2009	4.0.0.32	Riskware.Win32.VBInject!!!K
Avira AntiVir	7.1.2.208	8.1.2.12	-
Avast	090323-0	4.8.1229	-
AVG	270.11.25/2019	8.0.0.0	-
BitDefender	24/03/2009	7.0.0.2555	Trojan.Crypt.VB.M
ClamAV	24/03/2009	0.93.1.0	-
Comodo	1082	3.8	-
Dr.Web	24/03/2009	5.0	Trojan.DownLoader.46203
Ewido	24/03/2009	4.0.0.2	-
F-PROT 6	20090323	4.4.4.56	-
G DATA	19.3655	2.0.7309.847	-
IkarusT3	24/03/2009	1001044	VirTool.Win32.VBInject
Kaspersky	24/03/2009	8.0.0.357	-
McAfee	24/03/2009	5.1.0.0	-
Malware Hash Registry	24/03/2009	N/A	-
NOD32 v3	3957	3.0.677	-
Norman	2009/03/23	5.92.08	-
Panda	07/02/2009	9.5.1.00	-
QuickHeal	24 March, 2009	10.0	-
Solo Antivirus	24/03/2009	8.0	-
Sophos	24/03/2009	4.32.0	-
TrendMicro		1.1-1001	-
VBA32	24/03/2009	3.12.0.300	-
VirusBuster	10.102.19	1.4.3	-

el resultado es notable y el stub si lo modifican tal cual está explicado es funcional 100%,saludos.

**xtazis** para **Portalhacker y level-23.com**