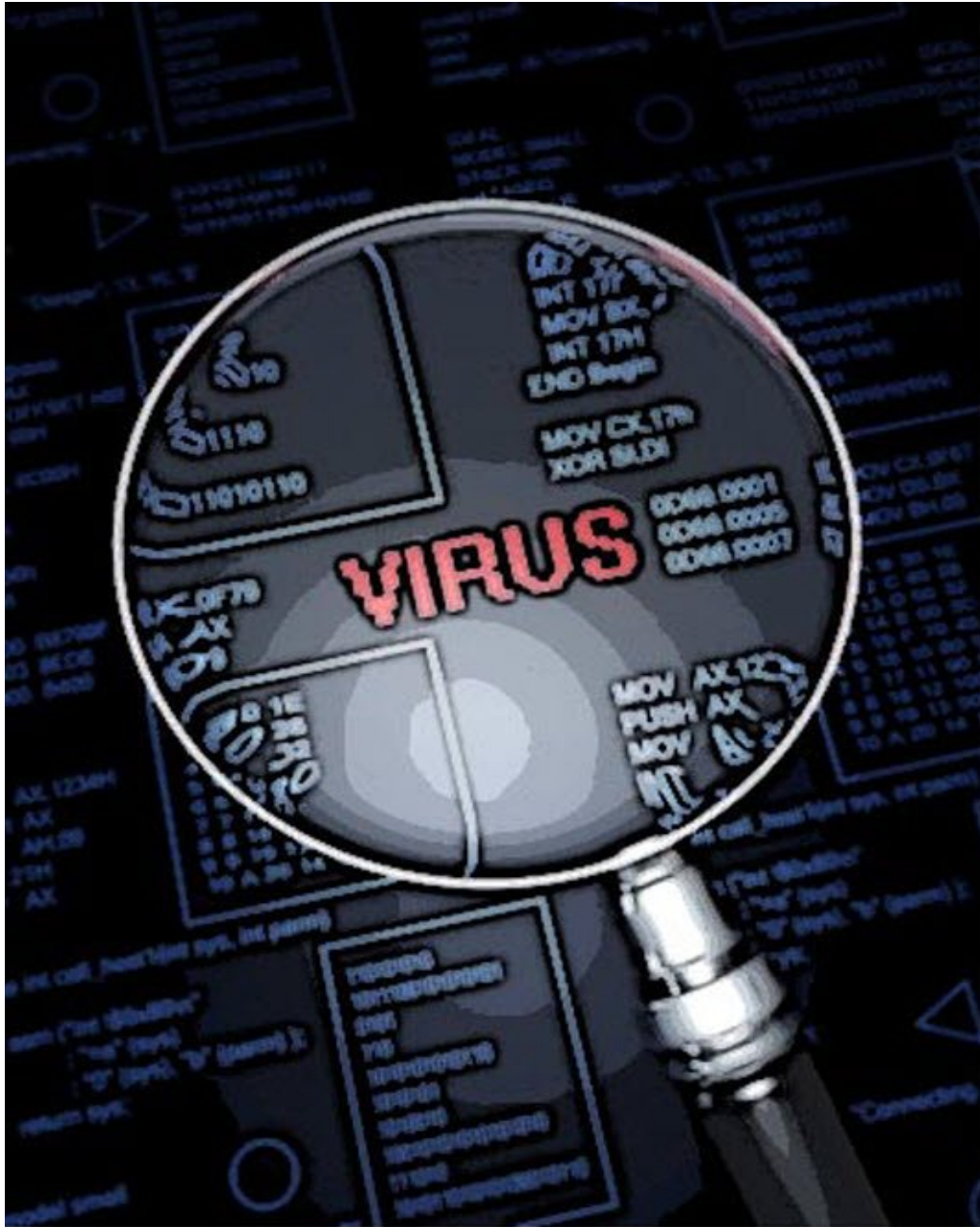


Indetectando Malwares Cercando Firmas



BY ANTRAX

www.underc0de.com.ar

1. Introducción:

Hola a todos, soy ANTRAX. En este tutorial les enseñare a dejar indetectables sus Malwares con este método que es muy sencillo. El método consiste en cercar las firmas detectadas y taparlas. Para que quede indetectable.

Las herramientas necesarias podrán encontrarlas en mi blog.

Utilizare vscan para ir verificando si queda indetectable o no.

Lo que necesitaremos para este tutorial será:

SignatureZero

Editor Hexadecimal

Stub a modificar

Intentare ser lo más claro posible para explicarles. Como en todos mis tutoriales, pondré varias imágenes para que puedan guiarse de manera correcta.

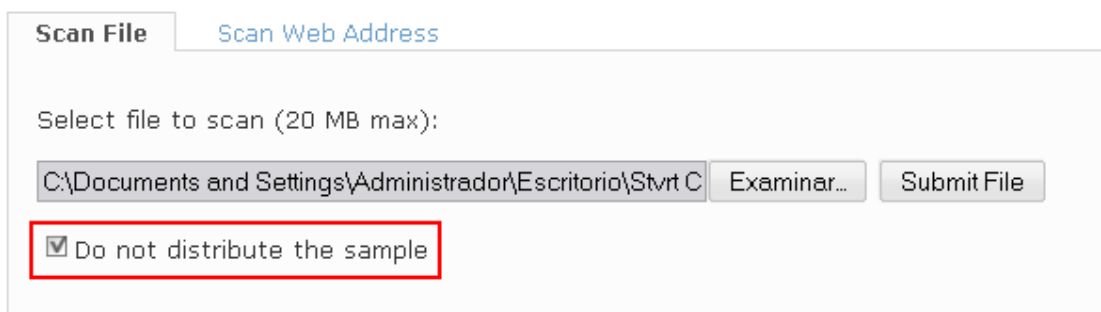
El scanner online que usare será: <http://vscan.novirusthanks.org>

Notaran que le faltan varios AVs, pero por el momento es el más seguro ya que no envía muestras.

Sin nada más que decir, nos pondremos a trabajar.

2. Stub inicial:

Scanneare el Stub con el que trabajare.



The screenshot shows the vscan web interface. At the top, there are two tabs: 'Scan File' (selected) and 'Scan Web Address'. Below the tabs, there is a text input field with the placeholder text 'Select file to scan (20 MB max):'. The input field contains the path 'C:\Documents and Settings\Administrador\Escritorio\Stvt C'. To the right of the input field are two buttons: 'Examinar...' and 'Submit File'. Below the input field, there is a checkbox labeled 'Do not distribute the sample' which is checked. This checkbox is highlighted with a red rectangular box.

Siempre recuerden marcar la opción "Do not Distribute the sample"

Underc0de

Esto es para que no envíe muestras de nuestro archivo a las empresas de antivirus.

ANTES:

File information	
Report date:	2011-03-10 06:43:27 (GMT 1)
File name:	stub-exe
File size:	20480 bytes
MD5 hash:	1db3d970693da9b44ec23818432c1070
SHA1 hash:	39e3e442cbf99620e8adf7e56931a7a3c1dc41b2
Detection rate:	6 on 9 (67%)
Status:	INFECTED

Antivirus	Database	Engine	Result
Avast	10/03/2011	5.0	Win32:Malware-gen
AVG	10/03/2011	10.0.0.1190	Dropper.Generic.ATQY
ClamAV	10/03/2011	0.97	
Comodo	10/03/2011	4.0	TrojWare.Win32.Refroso.bfi
Emsisoft	10/03/2011	5.1.0.2	Virus.Win32.VBInjectLIK
F-Prot	10/03/2011	6.3.3.4884	
Ikarus	10/03/2011	T31001097	Virus.Win32.VBInject
TrendMicro	10/03/2011	9.200.0.1012	TROJ_Generic.DIT
Zoner	10/03/2011	0.2	

Como podrán ver, lo detectan 6 de 9 antivirus. Y a esto debemos añadirle que le faltan antivirus importantes como Nod32, Avira, Etc. Por el momento no nos importara esto, sino que nos centraremos en el método. Una vez que lo aprendamos, los antivirus irán saliendo solos.

Después de un rato de moddeo, logre dejarlo así:

Underc0de

File information	
Report date:	2011-03-10 14:28:57 (GMT 1)
File name:	stub.exe
File size:	20480 bytes
MD5 hash:	9cb6af240f002890e8fef46feb3b477a
SHA1 hash:	6b91993816ace385dd4a460f8550ab548abfa775
Detection rate:	1 on 9 (11%)
Status:	INFECTED

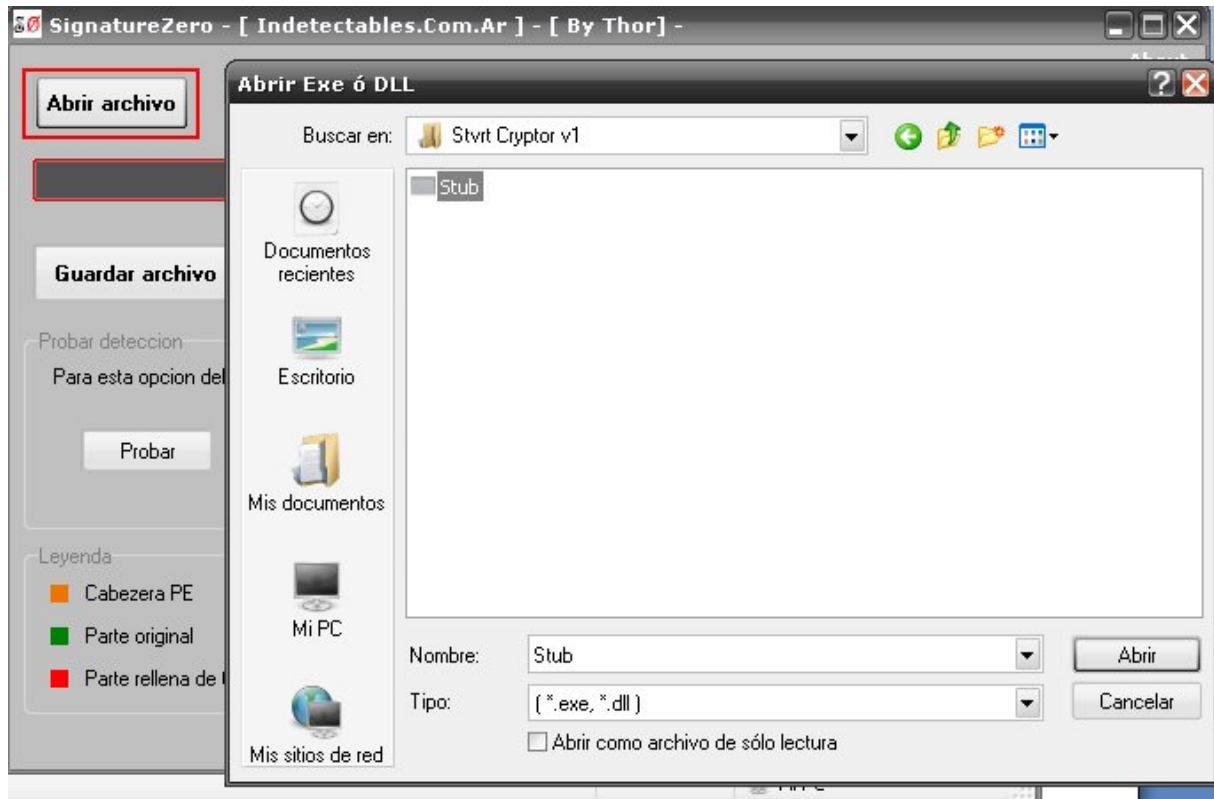
Antivirus	Database	Engine	Result
Avast	10/03/2011	5.0	
AVG	10/03/2011	10.0.0.1190	Injector.BKZ
ClamAV	10/03/2011	0.97	
Comodo	10/03/2011	4.0	
Emsisoft	10/03/2011	5.1.0.2	
F-Prot	10/03/2011	6.3.3.4884	
Ikarus	10/03/2011	T31001097	
TrendMicro	10/03/2011	9.200.0.1012	
Zoner	10/03/2011	0.2	

Bueno, ahora les enseñare como saque las firmas anteriores, y como sacare esa que falta...

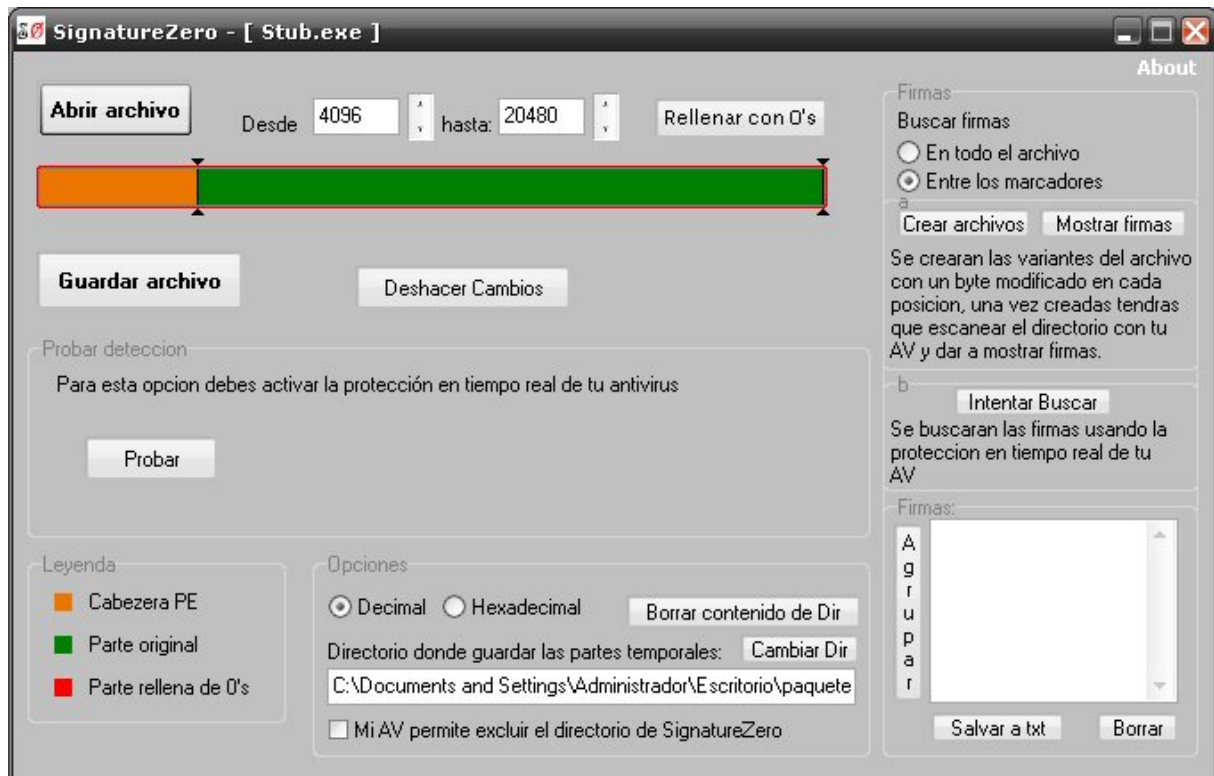
3. Cercando firmas con SZ:

Abriamos el Stub con el SignatureZero

Underc0de



Veremos al go como lo siguiente:



Bueno, este es el SignatureZero.

Underc0de

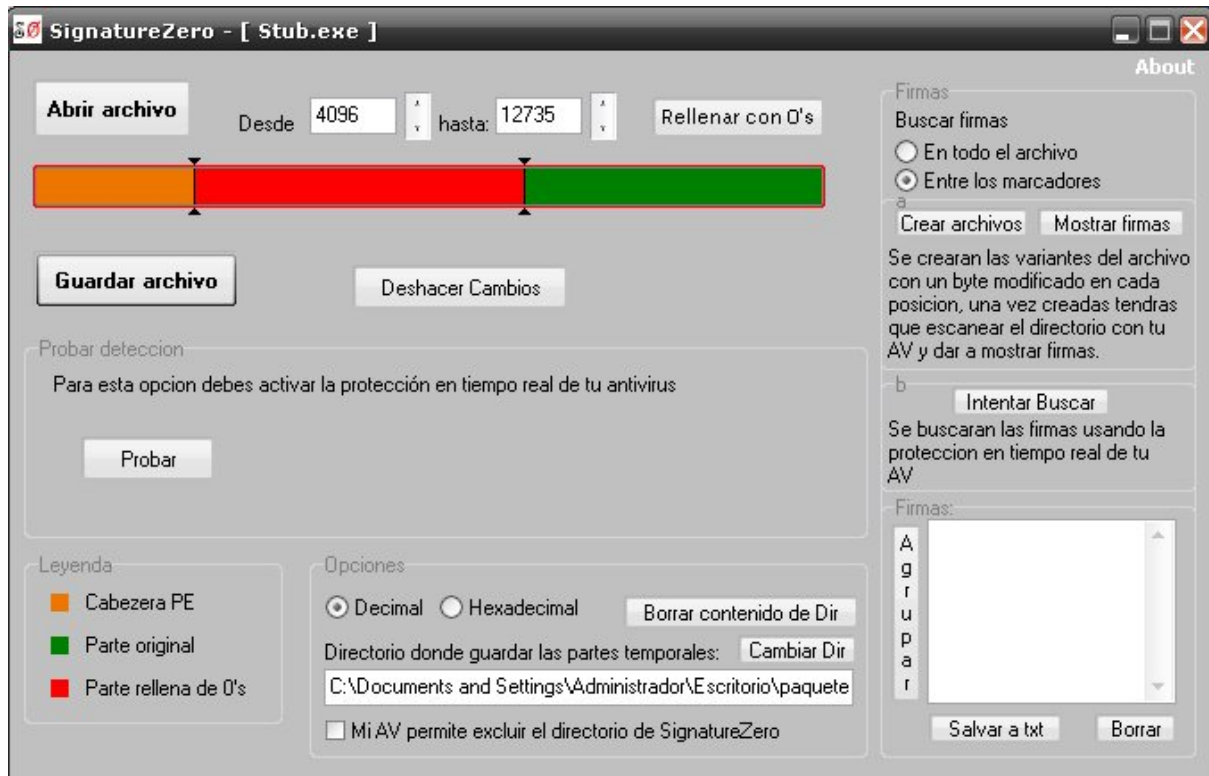
Como podrán ver tenemos una línea de colores.

Lo naranja no se toca, ya que es la cabecera PE. La cabecera esta contiene información del sistema operativo.

Lo verde es lo original

Lo rojo es lo que nosotros llenaremos de ceros.

Para poder modificar algo, tenemos como dos barras con flechitas.



Bueno lo que hice acá fue mover la barrita y rellenar con ceros. Seguido a esto guardamos y analizamos el archivo.

Este fue el resultado:

Undercode

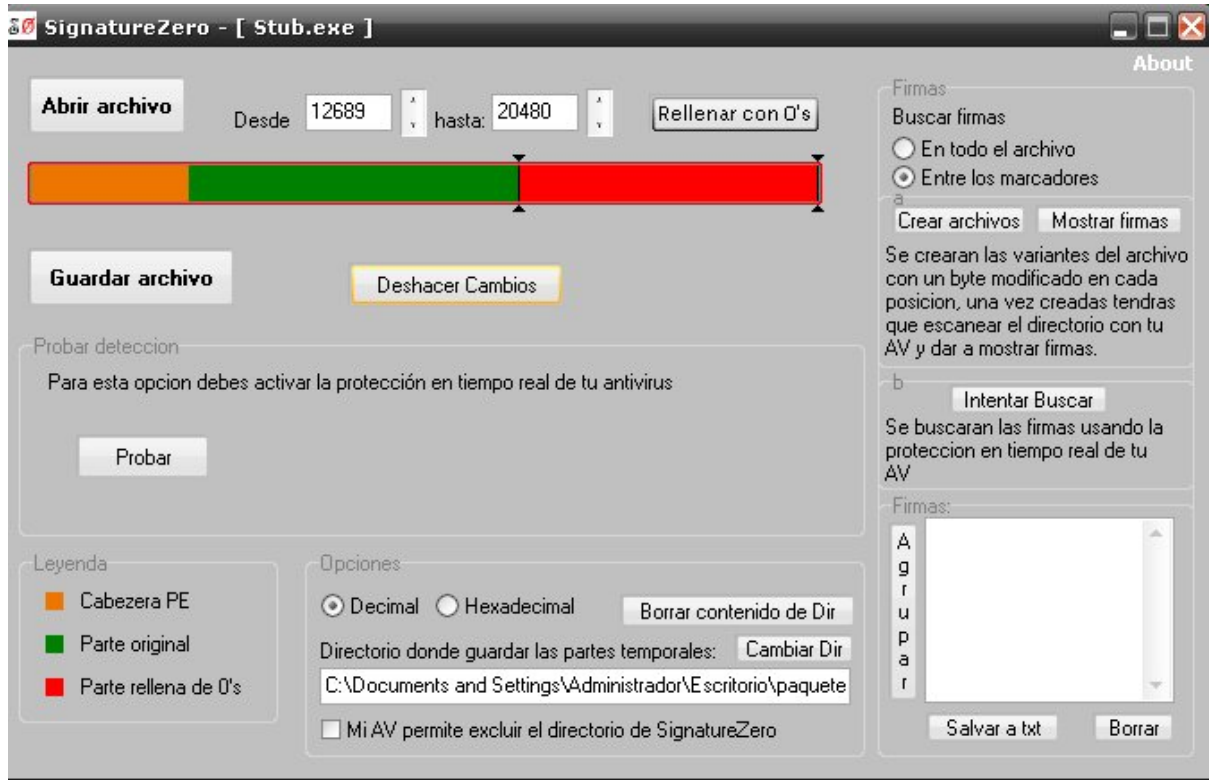
File information	
Report date:	2011-03-10 16:01:22 (GMT 1)
File name:	antrax1-exe
File size:	20480 bytes
MD5 hash:	5571a1c7eeae0b261f4d015815c19d5e
SHA1 hash:	49b0dabf31dfbaade3195579cde06a34fc994a8d
Detection rate:	0 on 9 (0%)
Status:	CLEAN

Antivirus	Database	Engine	Result
Avast	10/03/2011	5.0	
AVG	10/03/2011	10.0.0.1190	
ClamAV	10/03/2011	0.97	
Comodo	10/03/2011	4.0	
Emsisoft	10/03/2011	5.1.0.2	
F-Prot	10/03/2011	6.3.3.4884	
Ikarus	10/03/2011	T31001097	
TrendMicro	10/03/2011	9.200.0.1012	
Zoner	10/03/2011	0.2	

Esto quiere decir que el offset detectado está en la mitad roja.

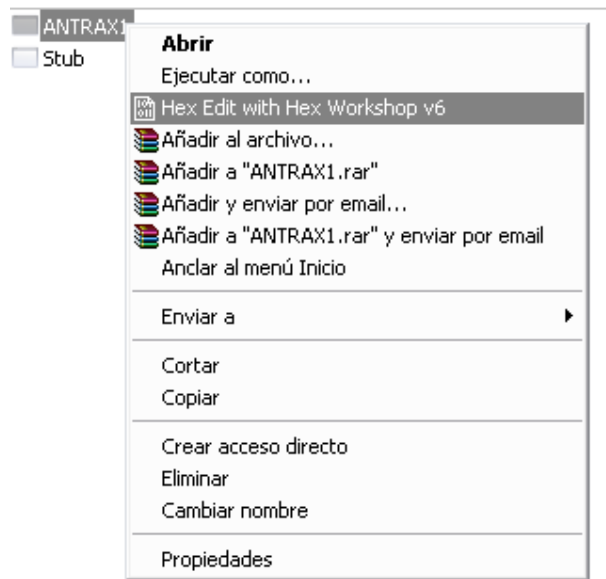
Cambiaremos de lugar las barras para comenzar a editar con el editor hexadecimal.

Underc0de



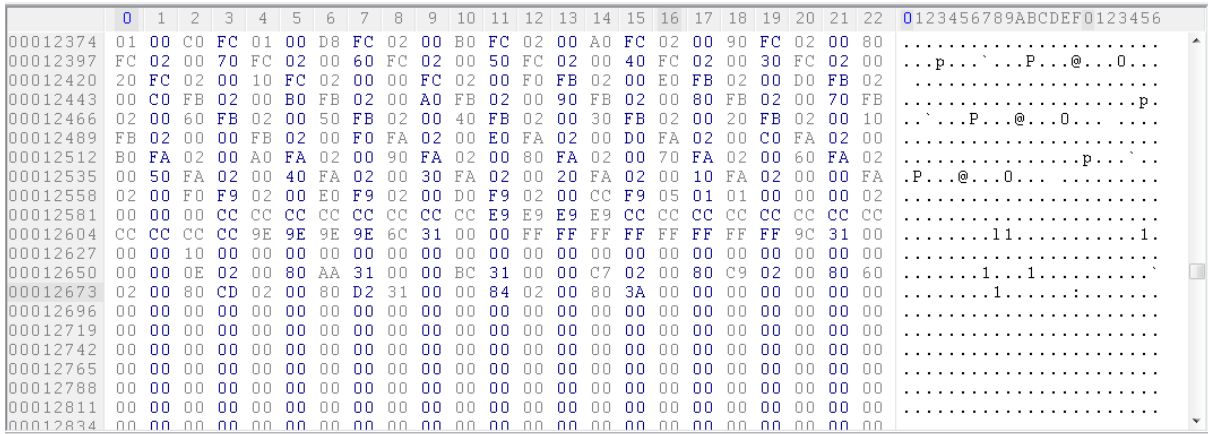
Guardamos con un nombre cualquiera y lo abrimos con un editor hexadecimal.

4. Cercando firmas con Hex WorkShop:



Underc0de

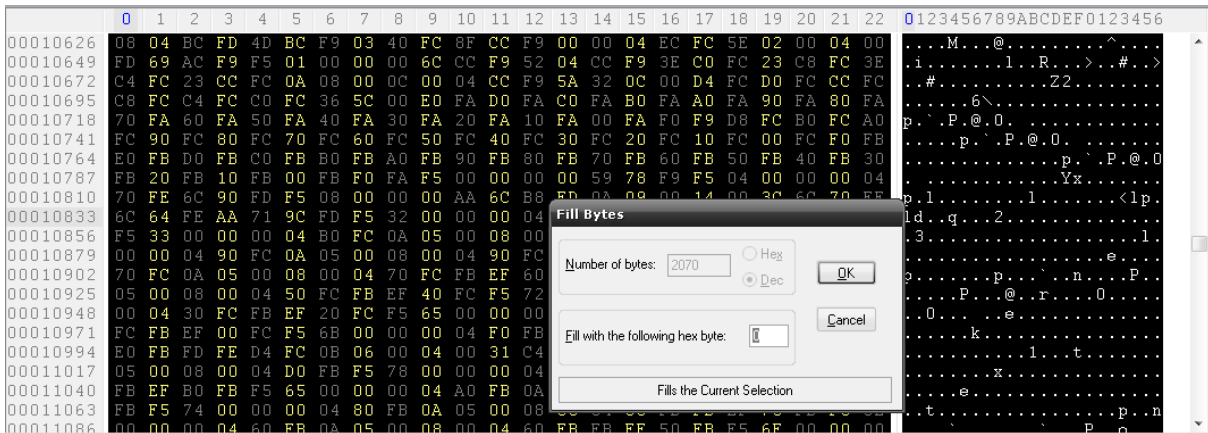
Como verán en el archivo, tendrán muchísimos ceros, estos son los ceros que llenamos con el SignatureZero.



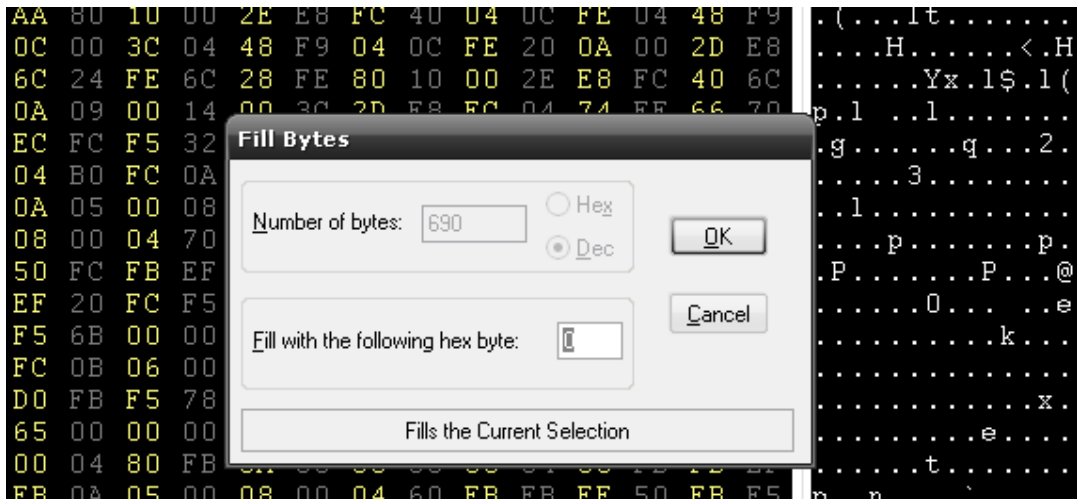
```
00012374 01 00 C0 FC 01 00 D8 FC 02 00 B0 FC 02 00 A0 FC 02 00 90 FC 02 00 80
00012397 FC 02 00 70 FC 02 00 60 FC 02 00 50 FC 02 00 40 FC 02 00 30 FC 02 00
00012420 20 FC 02 00 10 FC 02 00 00 FC 02 00 F0 FB 02 00 E0 FB 02 00 D0 FB 02
00012443 00 C0 FB 02 00 B0 FB 02 00 A0 FB 02 00 90 FB 02 00 80 FB 02 00 70 FB
00012466 02 00 60 FB 02 00 50 FB 02 00 40 FB 02 00 30 FB 02 00 20 FB 02 00 10
00012489 FB 02 00 00 FB 02 00 F0 FA 02 00 E0 FA 02 00 D0 FA 02 00 C0 FA 02 00
00012512 B0 FA 02 00 A0 FA 02 00 90 FA 02 00 80 FA 02 00 70 FA 02 00 60 FA 02
00012535 00 50 FA 02 00 40 FA 02 00 30 FA 02 00 20 FA 02 00 10 FA 02 00 00 FA
00012558 02 00 F0 F9 02 00 E0 F9 02 00 D0 F9 02 00 C0 F9 05 01 01 00 00 00 02
00012581 00 00 00 CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC
00012604 CC CC CC CC 9E 9E 9E 6C 31 00 00 FF FF FF FF FF FF 9C 31 00
00012627 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00012650 00 00 0E 02 00 80 AA 31 00 00 BC 31 00 00 C7 02 00 80 C9 02 00 80 60
00012673 02 00 00 CD 02 00 80 D2 31 00 00 84 02 00 80 3A 00 00 00 00 00 00
00012696 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00012719 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00012742 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00012765 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00012788 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00012811 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00012834 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Lo que debemos hacer ahora es ir rellenando con ceros en el editor hexadecimal hasta llegar a la firma detectada.

Para ello vamos seleccionando trozos y presionamos CTRL + INSERT y nos aparecerá un cartel como este:



```
00010626 08 04 BC FD 4D BC F9 03 40 FC 8F CC F9 00 00 04 EC FC 5E 02 00 04 00
00010649 FD 69 AC F9 F5 01 00 00 00 6C CC F9 52 04 CC F9 3E C0 FC 23 C8 FC 3E
00010672 C4 FC 23 CC FC 0A 08 00 0C 00 04 CC F9 5A 32 0C 00 D4 FC D0 FC CC FC
00010695 C8 FC C4 FC C0 FC 36 5C 00 E0 FA D0 FA C0 FA B0 FA A0 FA 90 FA 80 FA
00010718 70 FA 60 FA 50 FA 40 FA 30 FA 20 FA 10 FA 00 FA F0 F9 D8 FC B0 FC A0
00010741 FC 90 FC 80 FC 70 FC 60 FC 50 FC 40 FC 30 FC 20 FC 10 FC 00 FC F0 FB
00010764 E0 FB D0 FB C0 FB B0 FB A0 FB 90 FB 80 FB 70 FB 60 FB 50 FB 40 FB 30
00010787 FB 20 FB 10 FB 00 FB F0 FA F5 00 00 00 59 78 F9 F5 04 00 00 04
00010810 70 FE 6C 90 FD F5 08 00 00 00 AA 6C B8 FD 0A 08 00 14 00 3C 60 70 FE
00010833 6C 64 FE AA 71 9C FD F5 32 00 00 00 04
00010856 F5 33 00 00 00 04 B0 FC 0A 05 00 08 00
00010879 00 00 04 90 FC 0A 05 00 08 00 04 90 FC
00010902 70 FC 0A 05 00 08 00 04 70 FC FB EF 60
00010925 05 00 08 00 04 50 FC FB EF 40 FC F5 72
00010948 00 04 30 FC FB EF 20 FC F5 65 00 00 00
00010971 FC FB EF 00 FC F5 6B 00 00 00 04 F0 FB
00010994 E0 FB FD FE D4 FC 0B 06 00 04 00 31 C4
00011017 05 00 08 00 04 D0 FB F5 78 00 00 04
00011040 FB EF B0 FB F5 65 00 00 00 04 A0 FB 0A
00011063 FB F5 74 00 00 00 04 80 FB 0A 05 00 08
00011086 00 00 00 04 60 EB 0A 05 00 08 00 04 60 EB EB EF 50 EB F5 6E 00 00 00
```



```
AA 80 10 00 2E E8 FC 40 04 0C FE 04 48 F9
0C 00 3C 04 48 F9 04 0C FE 20 0A 00 2D E8
6C 24 FE 6C 28 FE 80 10 00 2E E8 FC 40 6C
0A 09 00 14 00 3C 2D E8 FC 04 74 FE 66 70
EC FC F5 32
04 B0 FC 0A
0A 05 00 08
08 00 04 70
50 FC FB EF
EF 20 FC F5
F5 6B 00 00
FC 0B 06 00
D0 FB F5 78
65 00 00 00
00 04 80 FB
EB 0A 05 00 08 00 04 60 EB EB EF 50 EB F5
```

Underc0de

Dejamos el cero y damos en OK, y se llenara todo con ceros.



Una vez hecho esto, guardamos y scanneamos.

File information	
Report date:	2011-03-10 20:04:37 (GMT 1)
File name:	antrax2-exe
File size:	20480 bytes
MD5 hash:	146eb8809cc9f53cec0014c9a1399c6c
SHA1 hash:	296210a67c0dd9cb93e5dae53da708174375898e
Detection rate:	1 on 9 (11%)
Status:	INFECTED

Antivirus	Database	Engine	Result
Avast	10/03/2011	5.0	
AVG	10/03/2011	10.0.0.1190	Injector.BKZ
ClamAV	10/03/2011	0.97	
Comodo	10/03/2011	4.0	
Emsisoft	10/03/2011	5.1.0.2	
F-Prot	10/03/2011	6.3.3.4884	
Ikarus	10/03/2011	T31001097	
TrendMicro	10/03/2011	9.200.0.1012	
Zoner	10/03/2011	0.2	

Si que apareciendo... Seguimos tapando firmas, hasta que deje de aparecer.

Una vez que ya no aparezca, volvemos atrás y empezamos a tapar de arriba para abajo.

Underc0de

Hasta que deje de aparecer. Entonces llegaremos a un fragmento como el siguiente:

```
00003910 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00003933 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00003956 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00003979 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004002 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004025 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004048 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004071 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004094 00 00 3F 7C 78 72 E5 A0 6A 72 24 46 78 72 1B 7C 79 72 B1 87 79 72 93 ..?|xr..jr$Fxr.|yr..yr.
00004117 0D 78 72 2D 8E 78 72 5D D0 79 72 E5 DC 77 72 5C 54 78 72 A4 35 6A 72 .xr-.xr|.yr..wr\Tsr.5jr
00004140 00 00 00 00 FF 25 04 10 40 00 FF 25 14 10 40 00 FF 25 10 10 40 00 FF .....%..%..%..%..%..%..%..%..%..
00004163 25 24 10 40 00 FF 25 00 10 40 00 FF 25 0C 10 40 00 FF 25 18 10 40 00 %$.@..%..%..%..%..%..%..%..%..%..
00004186 FF 25 20 10 40 00 FF 25 08 10 00 00 FF 25 1C 10 40 00 FF 25 28 10 40 .% .@..%..%..%..%..%..%..%..%..%..
00004209 00 00 00 68 84 11 40 00 E8 EE FF FF FF 00 00 00 00 00 00 00 00 30 00 00 00 ...h..@.....0...
00004232 38 00 00 00 00 00 00 00 B9 67 1D 06 CA D2 18 4A A1 90 4A 3E 04 EA 31 8.....g.....J..J>..1
00004255 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004278 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004301 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004324 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004347 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004370 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Como verán, en mi caso logre acorralarla. La firma detectada debe estar en una de esas líneas, ahora solo basta con ir rellenando una fila por una hasta que demos con ella.

```
00004071 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004094 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004117 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004163 25 24 10 40 00 FF 25 00 10 40 00 FF 25 0C 10 40 00 FF 25 18 10 40 00 %$.@..%..%..%..%..%..%..%..%..%..
00004186 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004209 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004232 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004255 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004278 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Bueno, ahí di con la línea que molestaba. Ahora solo queda modificar. En mi caso es casi obvio. Tiene una secuencia y el símbolo "\$" esta de mas... Lo que hare será rellenarlo con un punto.

```
00004002 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004025 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004048 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004071 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004094 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004117 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004163 25 2E 10 40 00 FF 25 00 10 40 00 FF 25 0C 10 40 00 FF 25 18 10 40 00 %..@..%..%..%..%..%..%..%..%..%..
00004186 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004209 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004232 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004255 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004278 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004301 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Scaneamos y...

Underc0de

File information	
Report date:	2011-03-10 20:20:26 (GMT 1)
File name:	antrax2-exe
File size:	20480 bytes
MD5 hash:	d9de27b4c61d4b4852fabad7f07b8caa
SHA1 hash:	36cac2d7f235d403c08fea2e5376e93cd4835cd7
Detection rate:	0 on 9 (0%)
Status:	CLEAN

Antivirus	Database	Engine	Result
Avast	10/03/2011	5.0	
AVG	10/03/2011	10.0.0.1190	
ClamAV	10/03/2011	0.97	
Comodo	10/03/2011	4.0	
Emsisoft	10/03/2011	5.1.0.2	
F-Prot	10/03/2011	6.3.3.4884	
Ikarus	10/03/2011	T31001097	
TrendMicro	10/03/2011	9.200.0.1012	
Zoner	10/03/2011	0.2	

Quedo Limpio...

Pero no termina acá! Ahora debemos abrir el stub original, buscar la firma y modificarla como hicimos acá.

```
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 0123456789ABCDEF0123456
00003979 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
00004002 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
00004025 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
00004048 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
00004071 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004094 00 00 3F 7C 78 72 E5 A0 6A 72 24 46 78 72 1B 7C 79 72 B1 87 79 72 93 .....
00004117 00 78 72 2D 8E 78 72 5D D0 79 72 E5 DC 77 72 5C 54 78 72 A4 35 6A 72 .....
00004140 00 00 00 00 00 FF 25 04 10 40 00 FF 25 14 10 40 00 FF 25 10 10 40 00 FF .....
00004163 25 2E 10 40 00 FF 25 00 10 40 00 FF 25 0C 10 40 00 FF 25 18 10 40 00 .....
00004186 FF 25 20 10 40 00 FF 25 08 10 00 00 FF 25 1C 10 40 00 FF 25 28 10 40 .....
00004209 00 00 00 68 84 11 40 00 E8 EE FF FF FF 00 00 00 00 00 00 30 00 00 00 .....
00004232 38 00 00 00 00 00 00 00 B9 67 1D 06 CA D2 18 4A A1 90 4A 3E 04 EA 31 .....
00004255 ED 00 00 00 00 00 00 01 00 00 00 0A 70 52 49 56 41 73 54 55 42 2E 50 .....
00004278 45 20 00 00 00 00 06 00 00 00 08 19 40 00 07 00 00 00 D4 18 40 00 07 .....
00004301 00 00 00 8C 18 40 00 07 00 00 00 44 18 40 00 07 00 00 00 F0 17 40 00 .....
00004324 07 00 00 00 A8 17 40 00 07 00 00 00 5C 17 40 00 07 00 00 00 10 17 40 .....
00004347 00 01 00 00 00 F0 14 40 00 00 00 00 00 FF FF FF FF FF FF FF FF 00 00 .....
00004370 00 00 44 15 40 00 00 40 40 00 02 00 00 00 64 11 40 00 0C 00 20 00 00 .....
00004393 00 00 00 34 06 1E 05 34 11 40 00 7C 43 40 00 F4 15 40 00 E4 15 40 00 .....
00004416 04 16 40 00 36 10 40 00 3C 10 40 00 42 10 40 00 48 10 40 00 4E 10 40 .....
00004439 00 78 11 40 00 54 10 40 00 A8 12 40 00 F0 1F 40 00 CC 1A 40 00 BA F0 .....
x @ T @ @ @ @
```

Para finalizar guardamos y scanneamos.

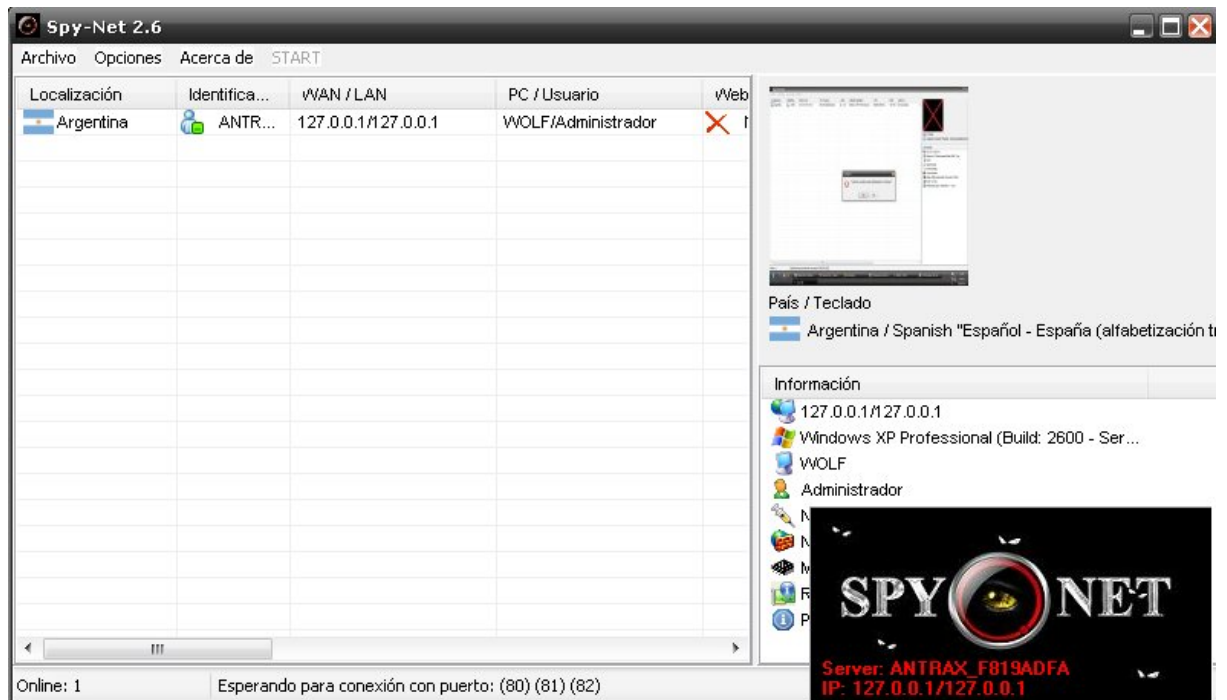
Underc0de

File information	
Report date:	2011-03-10 17:18:22 (GMT 1)
File name:	stub-exe
File size:	20480 bytes
MD5 hash:	a9c0cc90152560a339894c06f5ad25f6
SHA1 hash:	899575061a80087c7f06aa60cc5fcefb336e1ee
Detection rate:	0 on 9 (0%)
Status:	CLEAN

Antivirus	Database	Engine	Result
Avast	10/03/2011	5.0	
AVG	10/03/2011	10.0.0.1190	
ClamAV	10/03/2011	0.97	
Comodo	10/03/2011	4.0	
Emsisoft	10/03/2011	5.1.0.2	
F-Prot	10/03/2011	6.3.3.4884	
Ikarus	10/03/2011	T31001097	
TrendMicro	10/03/2011	9.200.0.1012	
Zoner	10/03/2011	0.2	

5. Test:

Encriptare un server y me infectare:



6. Despedi da:

Espero que les haya gustado el tutorial, este es algo sencillo, es una simple edición hexadecimal. Encontraran otros métodos, mucho más efectivos, pero bueno... La intención es compartir.

Saludos y hasta el próximo tutorial.

ANTRAX