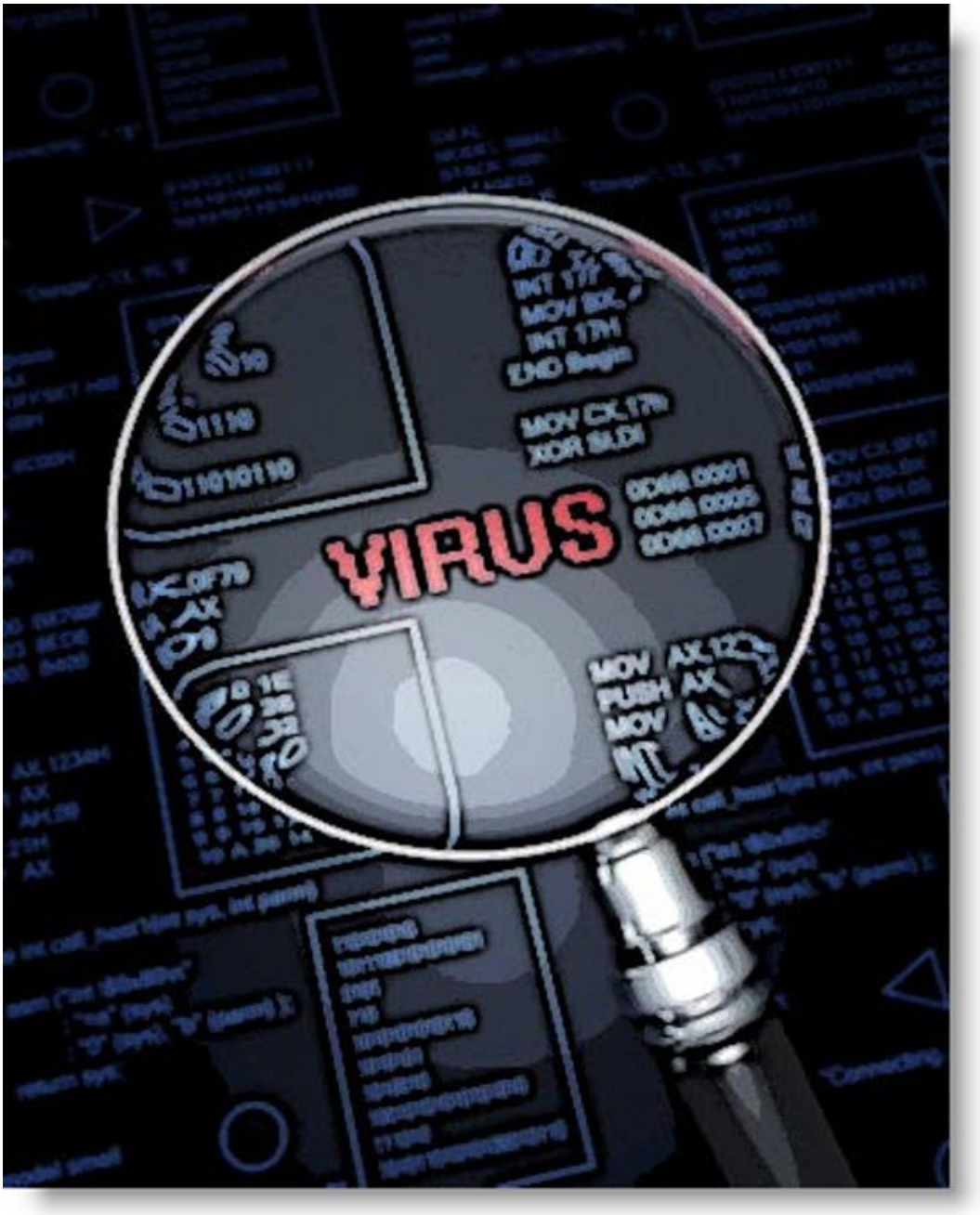
Indetectando Malwares Cercando Firmas



BY ANTRAX

www.underc0de.com.ar

1. Introduccion:

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.

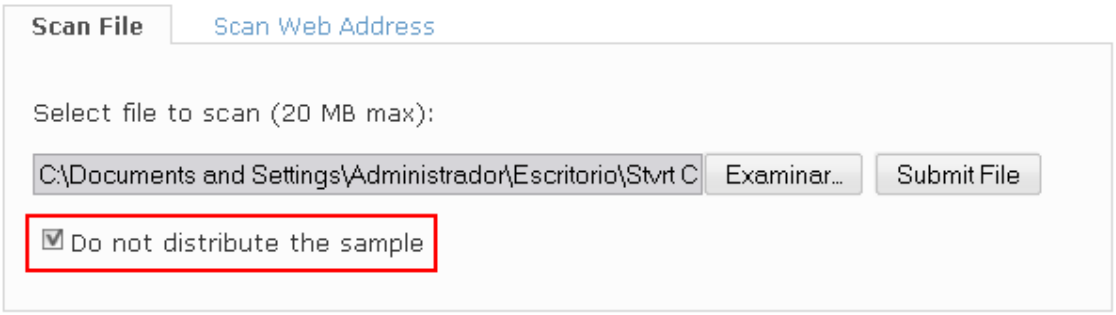
El scanner online que usare será: http://vscan.novirusthanks.org

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.



Siempre recuerden marcar la opción “Do not Distribute the sample”

Esto es para que no envie 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.VBInject!IK
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 adicionarle 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:

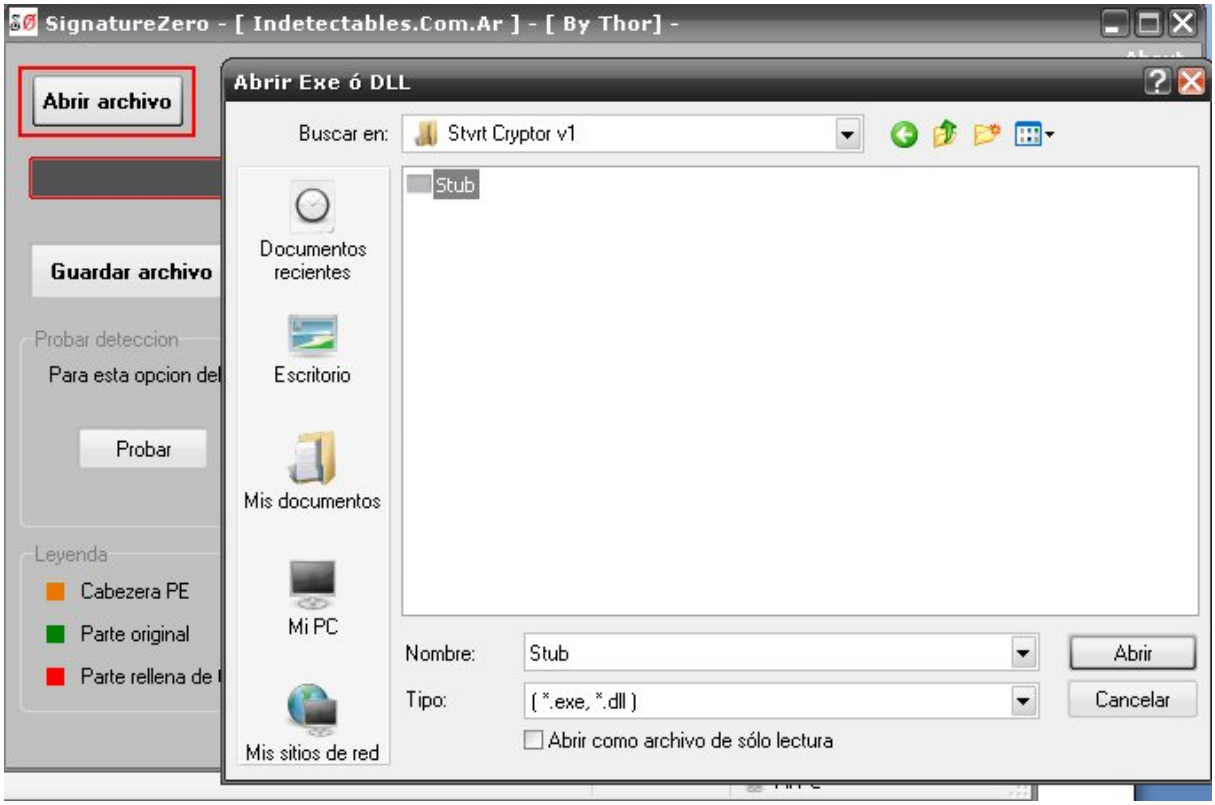
File information	
Report date:	2011-03-10 14:28:57 (GMT 1)
File name:	**stub-exe**
File size:	20480 bytes
MD5 hash:	9cb6af240f002890e8fef46feb3b477a
SHA1 hash:	6b91993816ace385dd4a460f8550ab548abfa775
Detection rate:	1 on 9 (11%)
Status:	INFECTED

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	

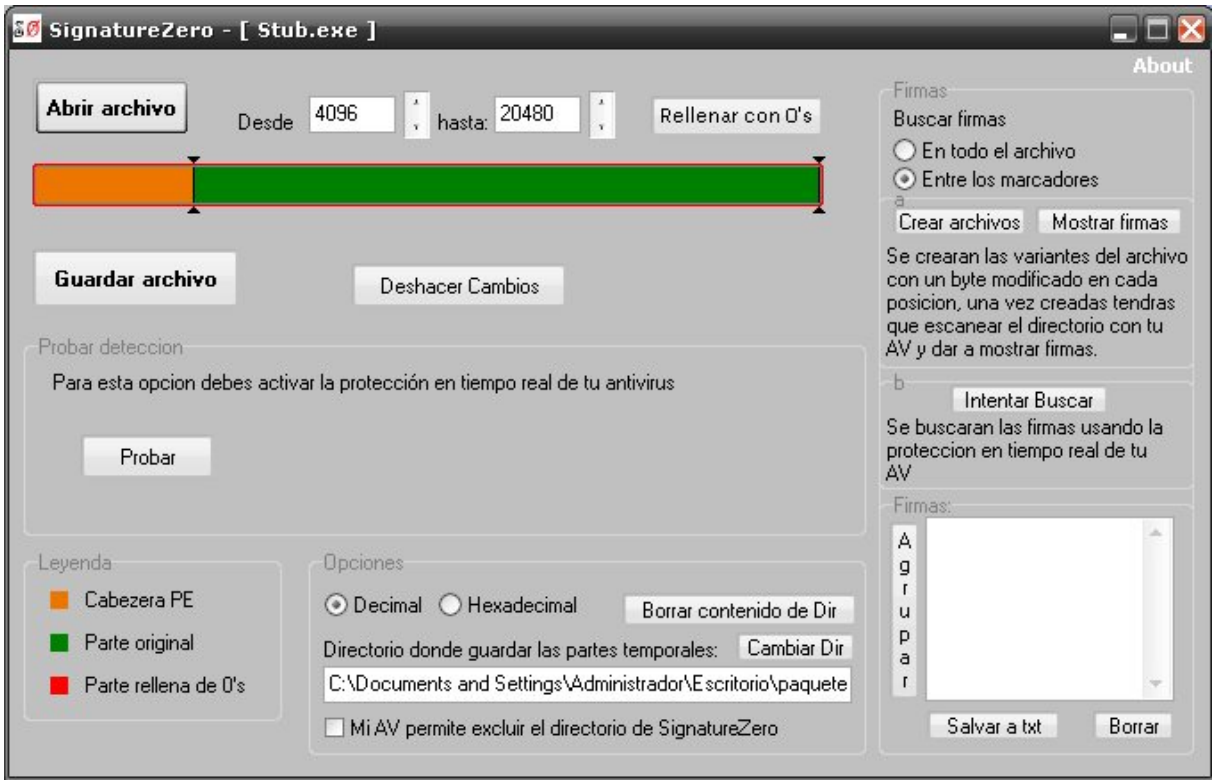
Bueno, ahora les enseñare como saque las firmas anteriores, y como sacare esa que falta…

3. Cercando firmas con SZ:

Abrimos el Stub con el SignatureZero



Veremos algo como lo siguiente:



Bueno, este es el SignatureZero.

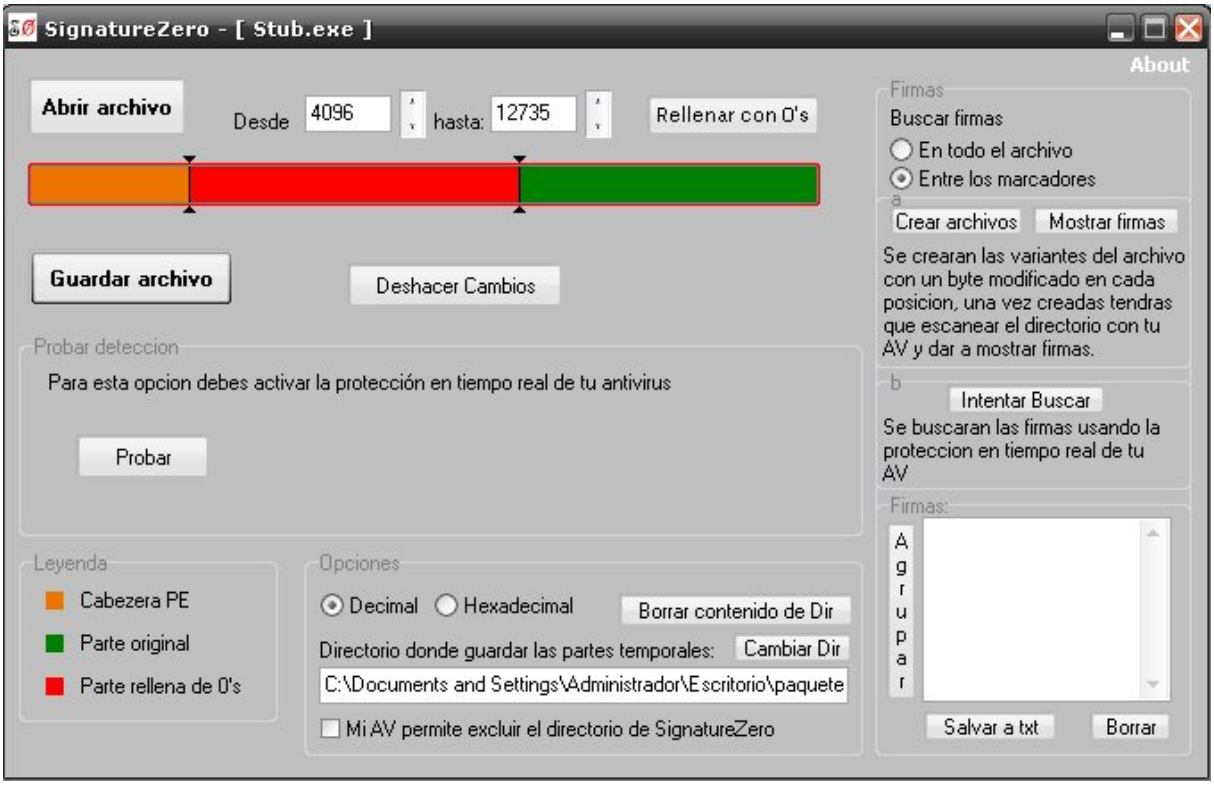
Como podrán ver tenemos una línea de colores.

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.

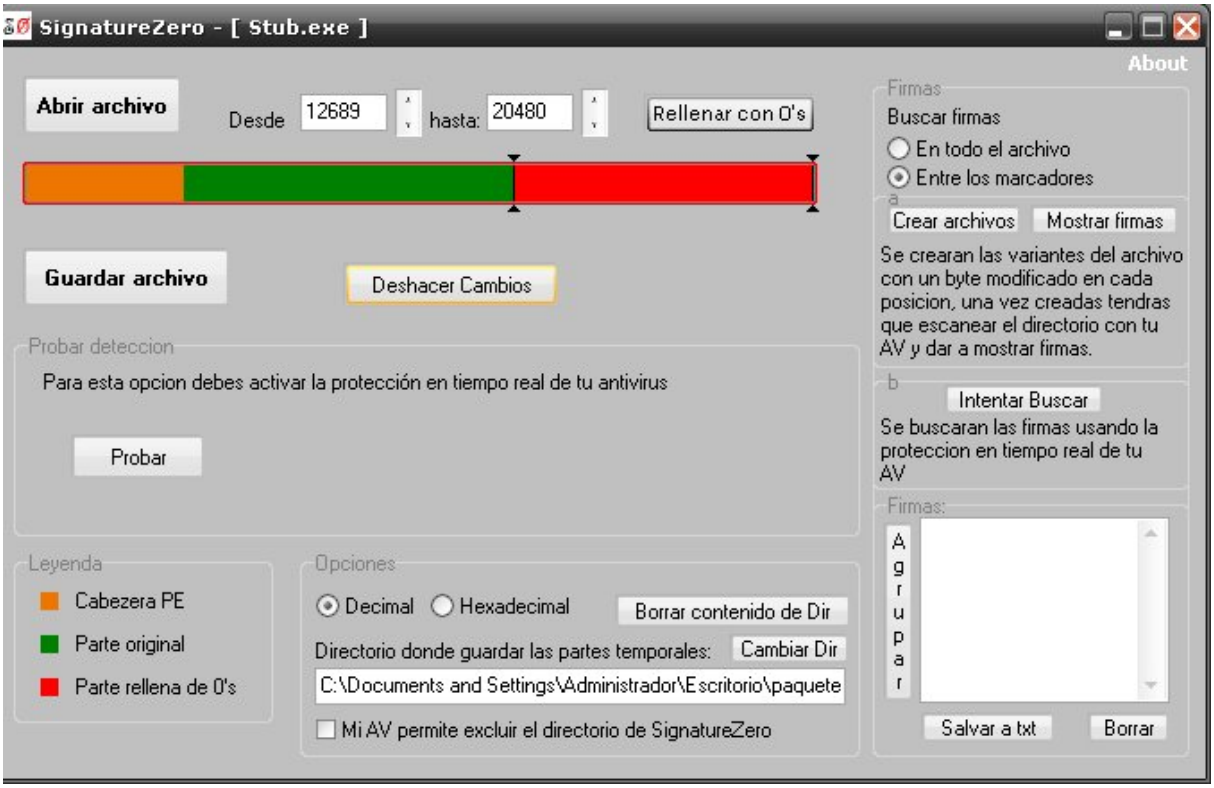
Este fue el resultado:

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	

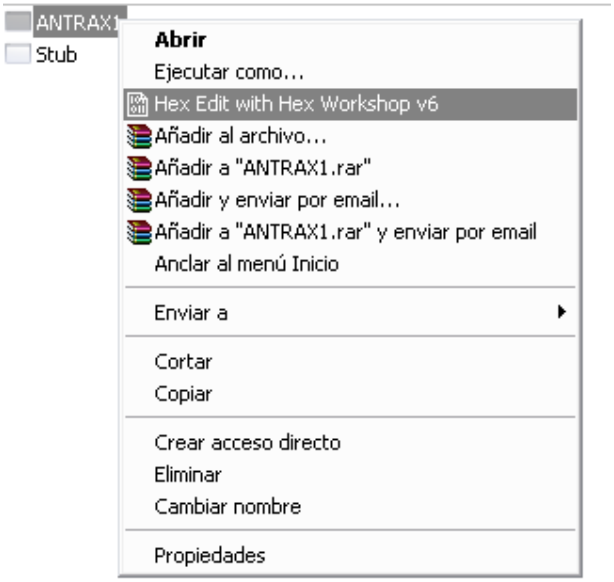
Esto quiere decir que el offset detectado está en la mitad roja.

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

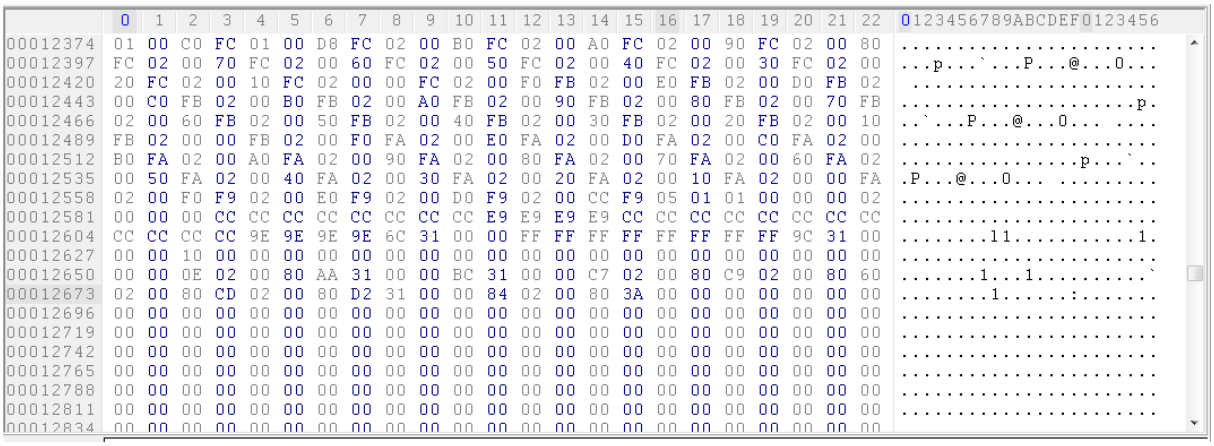


Guardamos con un nombre cualquiera y lo abrimos con un editor hexadecimal.

4. Cercando firmas con Hex WorkShop:

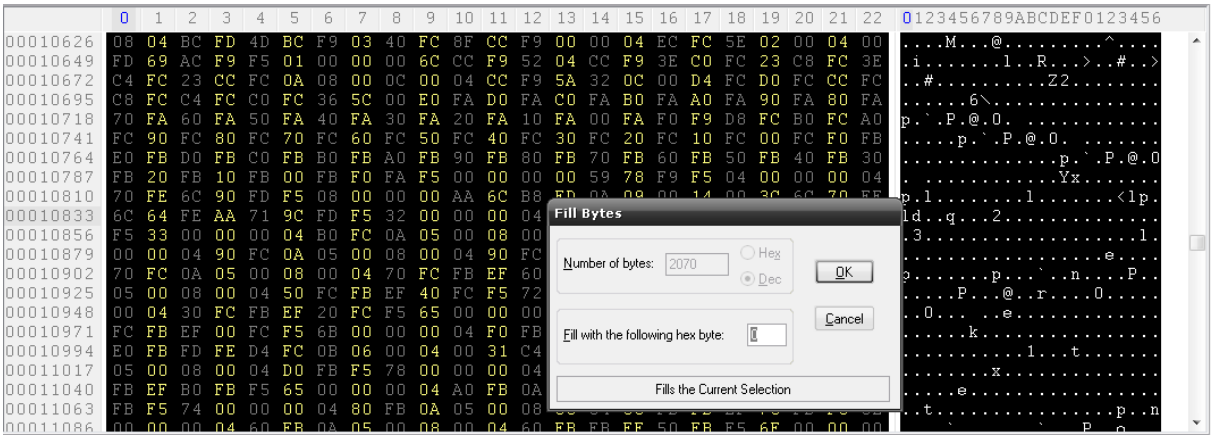


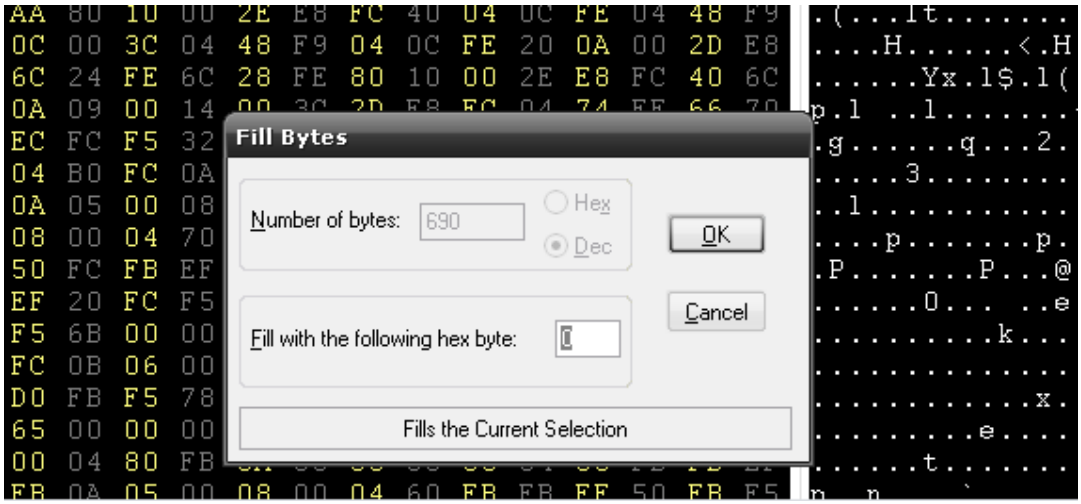
Como verán en el archivo, tendrán muchísimos ceros, estos son los ceros que llenamos con el SignatureZero.



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:





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	

Sigue 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.

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

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.

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.

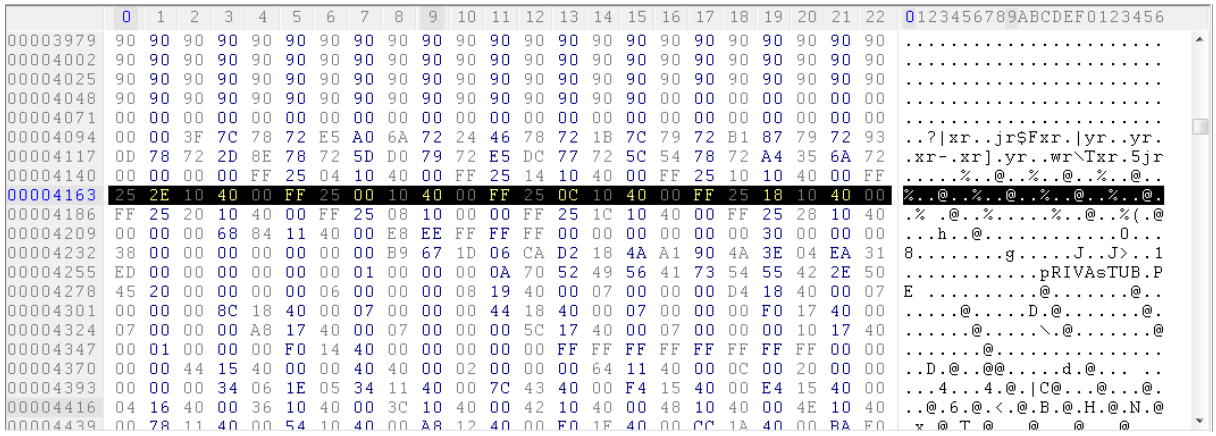
Scanneamos y…

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.



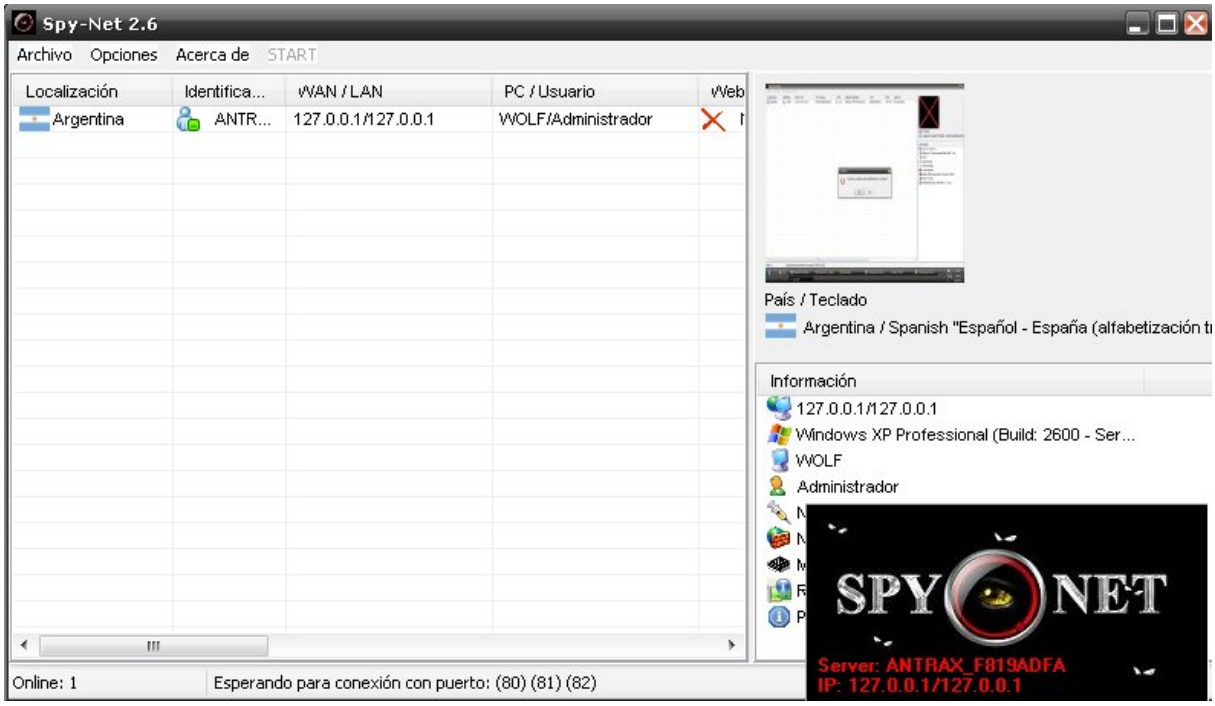
Para finalizar guardamos y scanneamos.

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:	899575061a80087c7f06aa60cc5fcefbb336e1ee
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. Despedida:

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 intensión es compartir.

Saludos y hasta el próximo tutorial.

ANTRAX