HOW TO:
HACER TU TROYANO FAVORITO INDETECTABLE SIN MORIR EN EL INTENTO

BY
OCTALH
08/02/08

__ATENCION: Este manual así como su autor NO__ se hacen responsable en ningún caso de ningún daño que se pudiera causar a un tercero por la lectura de este manual, como consecuencia del uso ilegal o inadecuado del mismo, ni como consecuencia de los contenidos e informaciones accesibles o facilitadas a través de ella, ni de los sitios vinculados a la misma. Los responsables serán los usuarios o terceros causantes de los daños.

Hola una ves mas a toda la comunidad, en esta ocasión quiero hacer el siguiente aporte debido a la constancia con la que veo en distintos foros infinidad de mensajes pidiendo algún método EFECTIVO a la hora de hacer sus aplicaciones favoritas indetectables.

Por desgracia casi no existe buena documentación o en su defecto se encuentra inconclusa o bastante confusa.

Bueno… dejando todo eso de lado espero que disfrutes esta guía y le saques provecho.
A decir verdad llevo utilizando esta técnica un par de años y hasta ahora me sigue siendo funcional.

Dices que podré hacer indetectable lo que quiera pero como funciona tal método?

Bien, en si solo bastara con dar un rápido análisis de cómo opera nuestro enemigo, en este caso nuestro enemigo es el ANTIVIRUS.

Los antivirus funcionan de dos formas: uno es el método de detección por firmas digitales, y el segundo es por sistemas de protección heurística.

El primer método, el más común de todos y es el que vamos a aprender a burlar, se basa en el siguiente procedimiento.

Todos los AV (antivirus) tienen bases de datos que tienen que actualizarse todos los días, estos datos que descarga de los laboratorios son las firmas digitales, y por supuesto se encuentran cifradas para que ni tú ni yo podamos interpretarlas. Las firmas contienen muestras de código, es decir tienen una base de datos con miles de "cadenas de código" que identifican a un virus, es como nuestro código de ADN en los humanos.

De esa forma cuando un antivirus realiza un escaneo, lo que hace realmente es buscar esas cadenas de código dentro del archivo, si contiene alguna cadena que se encuentre en sus bases de datos inmediatamente dará una alarma informando que tienes un virus en tu sistema.

Hasta aquí creo que quedo bastante claro en que se basa el método de firmas.

Para el segundo caso que es el sistema de protección Heurística, que permite detectar virus SIN firmas, es decir no realiza esa búsqueda de cadenas de código dentro del archivo, lo que hace es algo mas inteligente, ejecuta el código sin comprometer a tu sistema y analiza el resultado, de esa forma no le importa como esta conformado dicho archivo sino la acción que realiza, si el antivirus detecta que la acción abre algún puerto o intenta inyectarse en un proceso o alterar el sistema operativo, dará un aviso de alarma.

Bien ahora que sabemos como funciona un antivirus podemos aprender a burlarlo, no importa realmente que antivirus uses, todos funcionan igual, así que nunca estarás protegido realmente, lo recomendable si quieres tener un extra de seguridad es utilizar sistemas operativos mas seguros como GNU/Linux o en su defecto MAC.

Ahora que ya aprendimos que los antivirus no son más que software "tonto" realizando búsquedas inútiles dentro de un archivo, seguro estarán pensando, pues entonces esta bastante fácil solo tendremos que encontrar esas firmas y modificarlas un poco.

Si eso fue lo que pensaste estas en lo correcto, es así de fácil, no hay más misterio más que encontrar esas firmas y cambiarlas un poco, con eso bastara para que el antivirus deje de detectarlas como virus.

Pero aquí te puedes enfrentar a dos problemas si no tienes la documentación correcta, uno es como encontrar las firmas y dos como modificarlas correctamente.

Antes de continuar quiero informarte que este método requiere de tiempo, pues es un poco laborioso pero bastante efectivo, para que no tengas que repetir este proceso una y otra ves con diferentes troyanos lo que haremos será hacer indetectable un "crypter", los crypter son programas que utilizan un algoritmo para cifrar el código de un programa, quiere decir que encriptan tu aplicación y además contienen la información adecuada de cómo desencriptarla, esta sección donde se indica al sistema como debe trabajar con dicha aplicación cifrada y las instrucciones para descifrarla se encuentran en el STUB del crypter.

Cuando tengamos nuestro crypter indetectable podremos hacer indetectable CUALQUIER COSA, sin necesidad de volver a repetir el proceso que haremos a continuación.

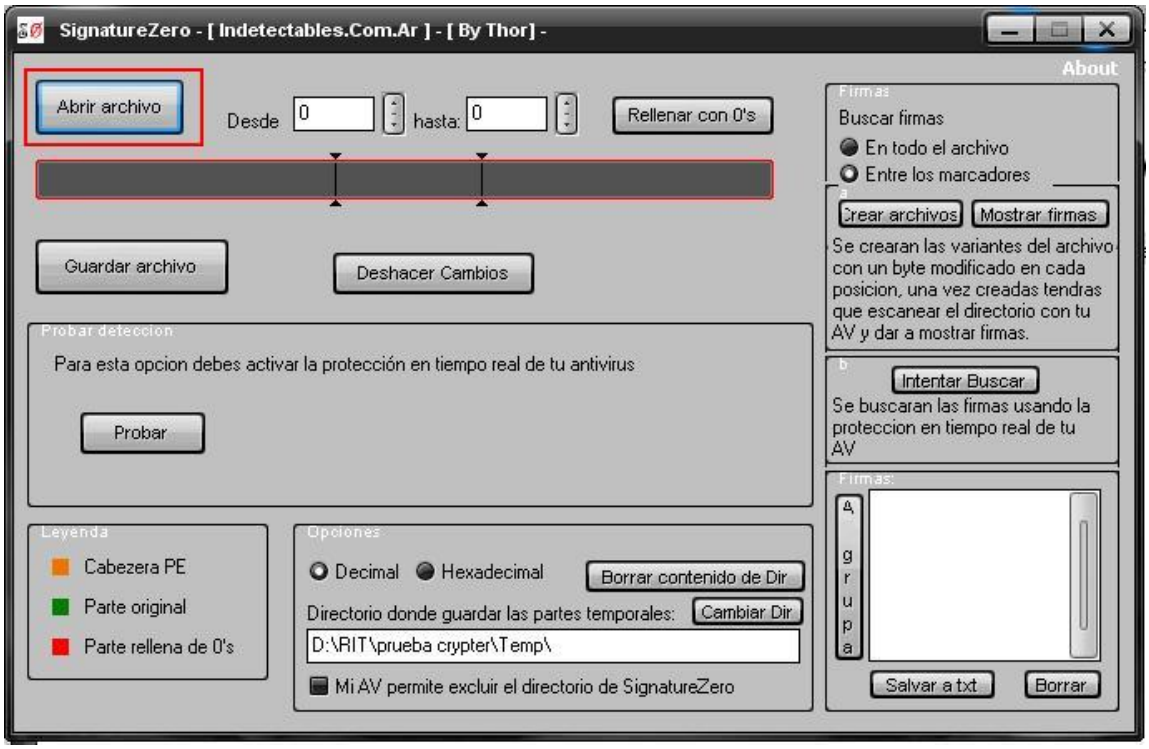
Para esta guía utilizaremos el crypter **X-Crypter.exe** y el conocido troyano **Bifrost**. y el antivirus **kaspersky (KAV)**

Material necesario:

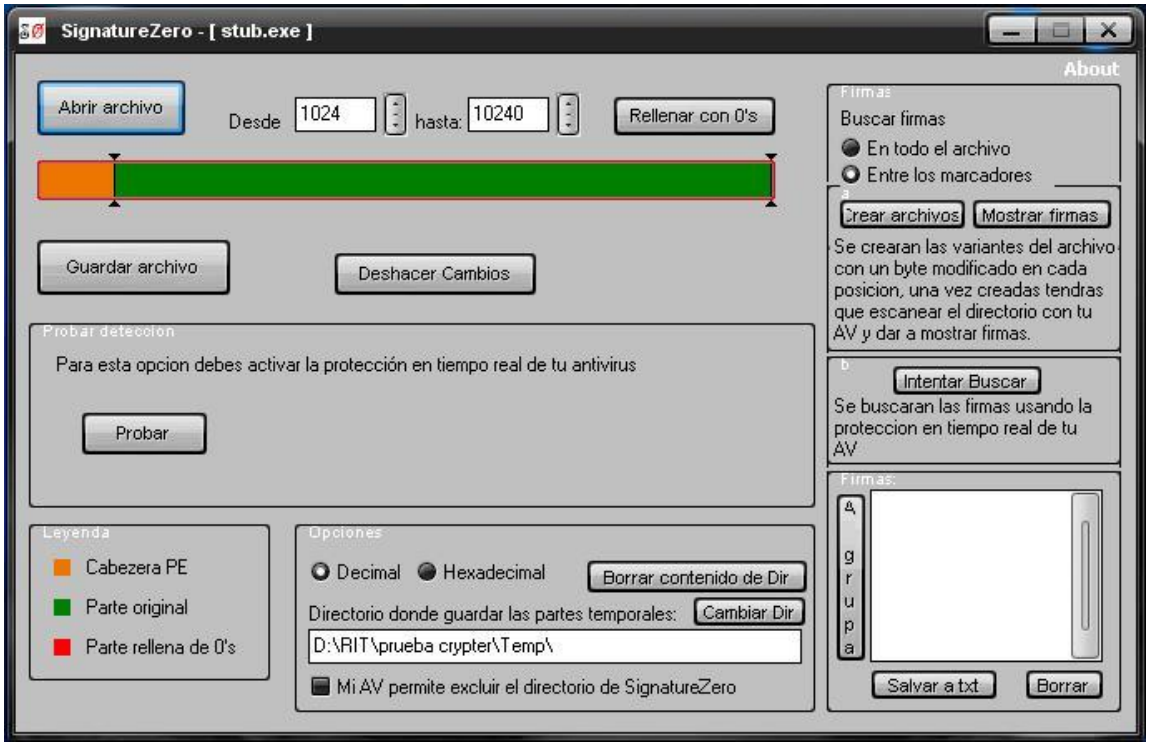
[Bifrost / Hex Workshop / OLLYDBG / Zignature zero / X-Crypter / Topo]

Lo primero será encontrar la firma, podríamos hacerlo manualmente con el editor HEX pero tardaríamos varias horas haciéndolo, por lo que nosotros utilizaremos la herramienta ZignatureZero programada por el mismísimo Thor.

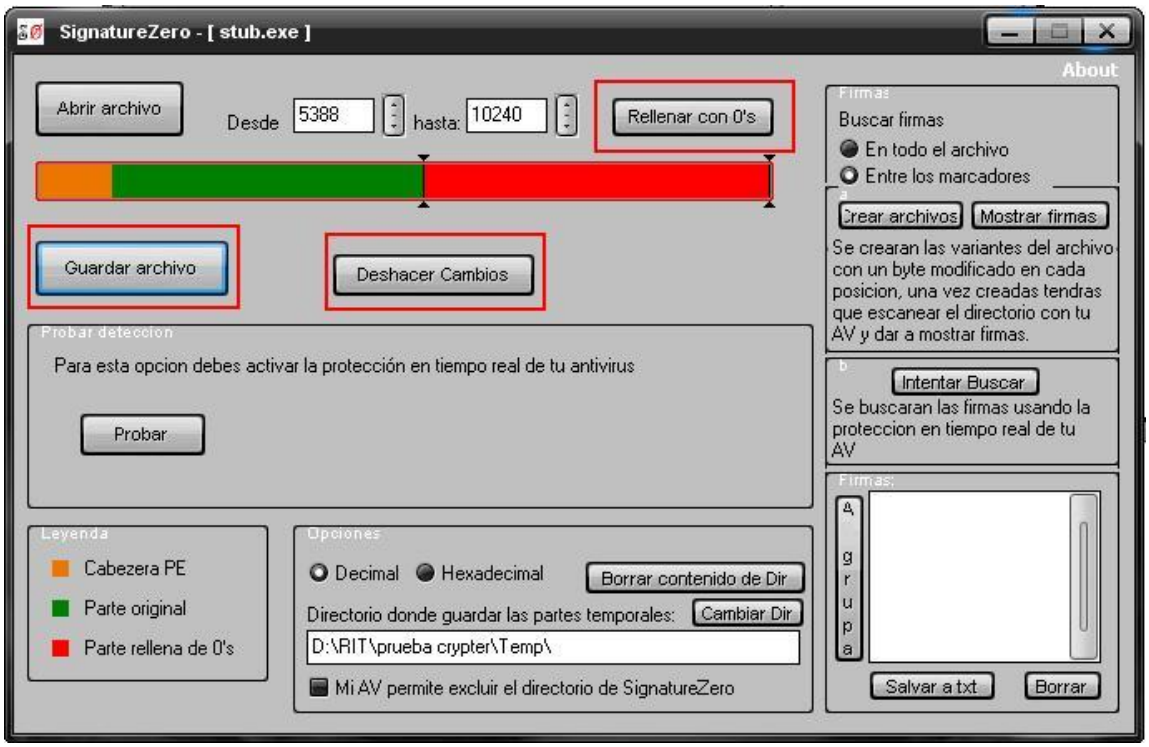
Bien manos a la obra, al ejecutar el programa nos encontraremos con la siguiente pantalla:



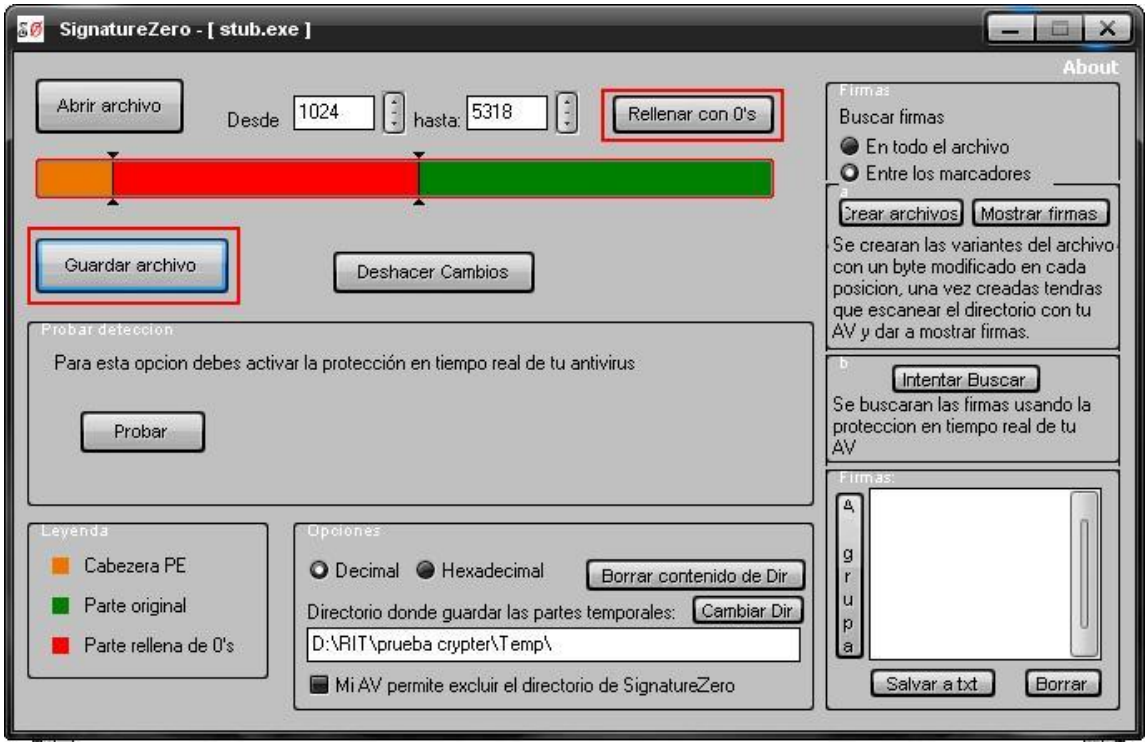
Damos clic en Abrir archivo y seleccionamos el archivo Stub de nuestro crypter.



Como pudiste observar la barra superior se relleno de color naranja y verde, lo de color naranja es la cabecera PE y no la tocaremos puesto que esa es solo información que le indica al Sistema Operativo como debe trabajar dicho archivo, lo verde es la representación visual del tamaño del archivo, lo que haremos será ir acorralando la firma hasta que la encontremos, para conseguirlo llenaremos de ceros una mitad, y guardaremos el archivo, procederemos a escanearlo y si deja de detectar como virus nuestra aplicación, quiere decir que borramos la mitad donde se encontraba la firma, entonces tenemos que regresar los cambios presionando en el botón Deshacer Cambios.

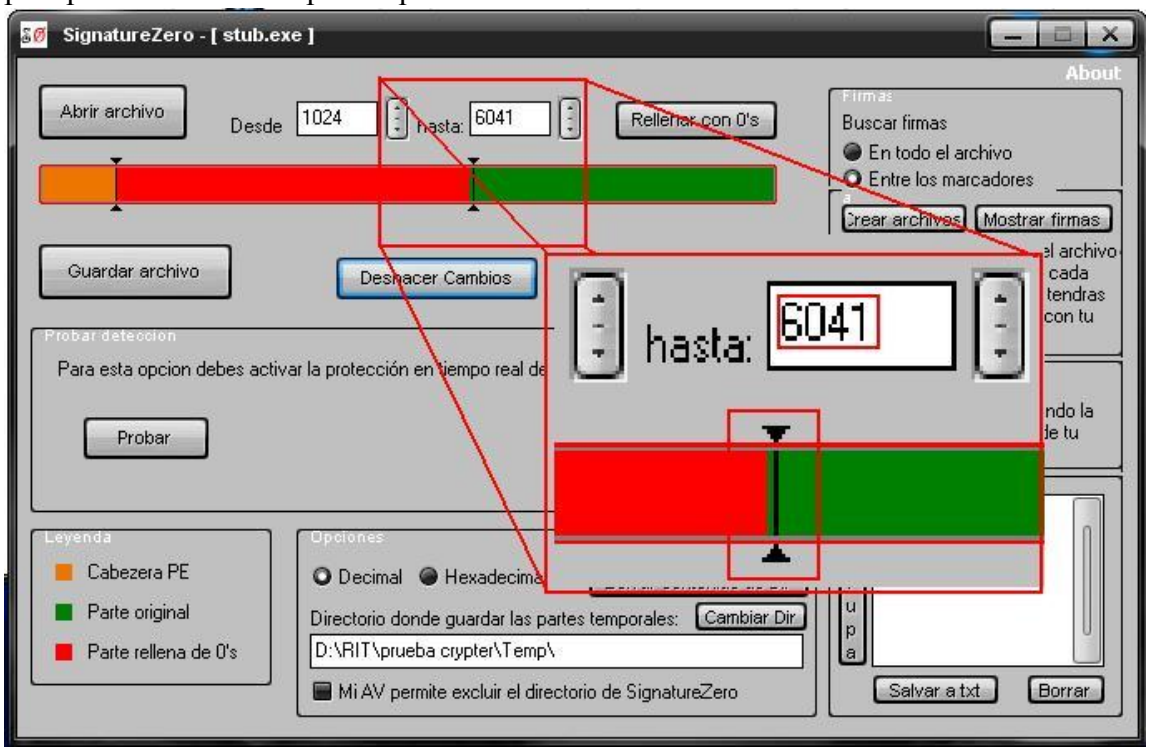


Después de deshacer los cambios, ahora rellene de ceros la mitad de la izquierda, guarde los cambios y volví a escanear el archivo, pero esta ves el antivirus si dio alarma.

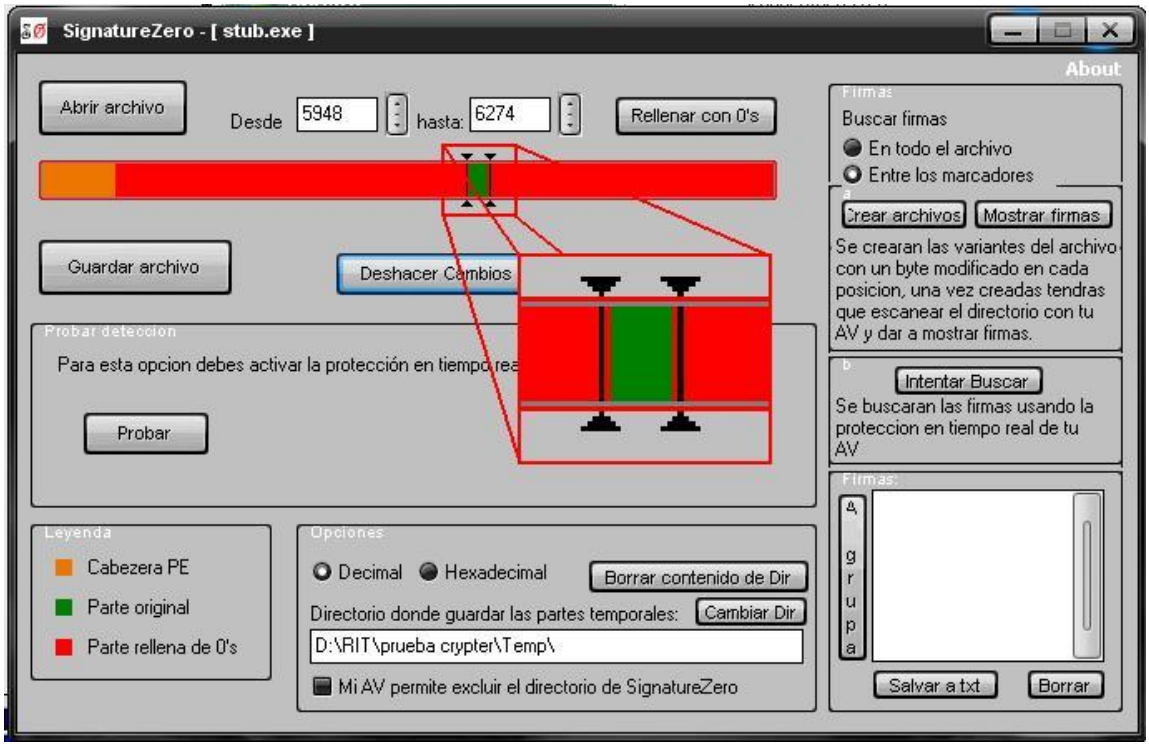


Quiere decir que la firma se encuentra en la mitad de la derecha, pues a pesar de haber llenado de ceros toda la mitad de la izquierda la sigue detectando. Ya es un avance ahora seguiremos avanzando de izquierda a derecha hasta que deje de detectar como virus.

Como pueden ver en la imagen de abajo fui avanzando de izquierda a derecha y aproximadamente por el offset 6041 dejo de detectarme como virus, por lo que deshice los cambios y regrese un poco antes de que me dejara de detectar, ahora que ya sabemos aproximadamente donde inicia la firma ahora haremos lo mismo pero de derecha a izquierda para poder irla cerrando poco a poco.



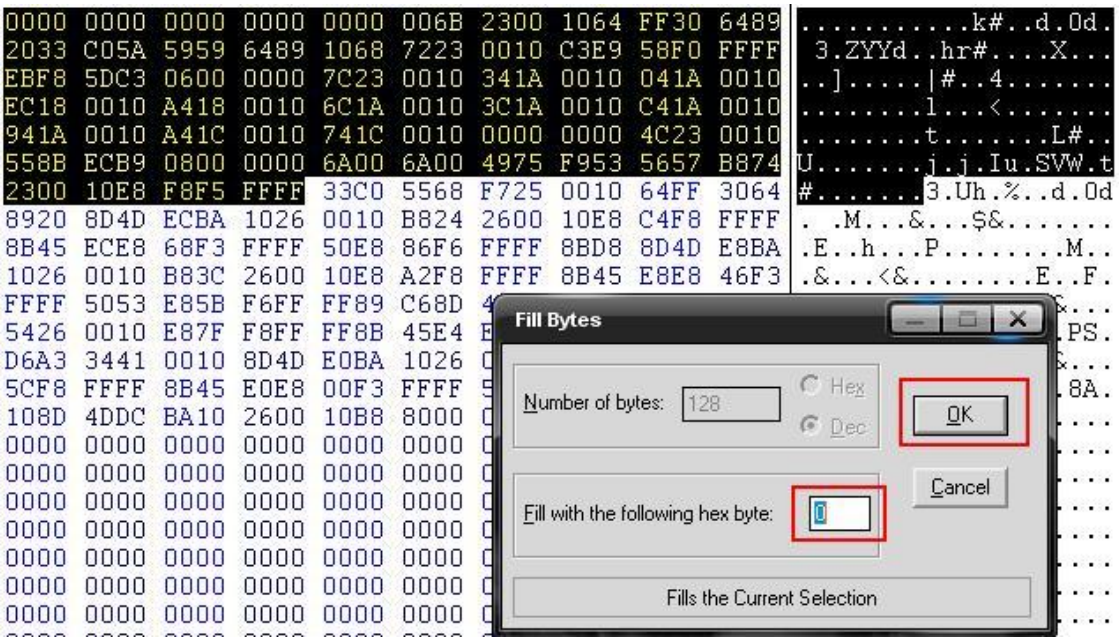
Continué rellenando con ceros de derecha a izquierda y ahora ya tenemos una aproximación de donde esta la firma, pues hemos llenado prácticamente todo el ejecutable de ceros y el antivirus sigue detectando el archivo como virus



Ahora utilizaremos el editor Hexadecimal para poder cercar aun mas la firma.

Al abrir el archivo con el editor Hexadecimal podemos ver que todo el archivo esta lleno de ceros a excepción de esta parte que abarca desde el offset 1748 - 1874
Lo que haremos será tomar líneas y llenarlas de ceros, igual que con ZignatureZero, solo que aquí lo haremos primero de arriba hacia abajo, hasta que deje de detectarlo y luego de abajo hacia arriba hasta que tengamos la firma totalmente cercada

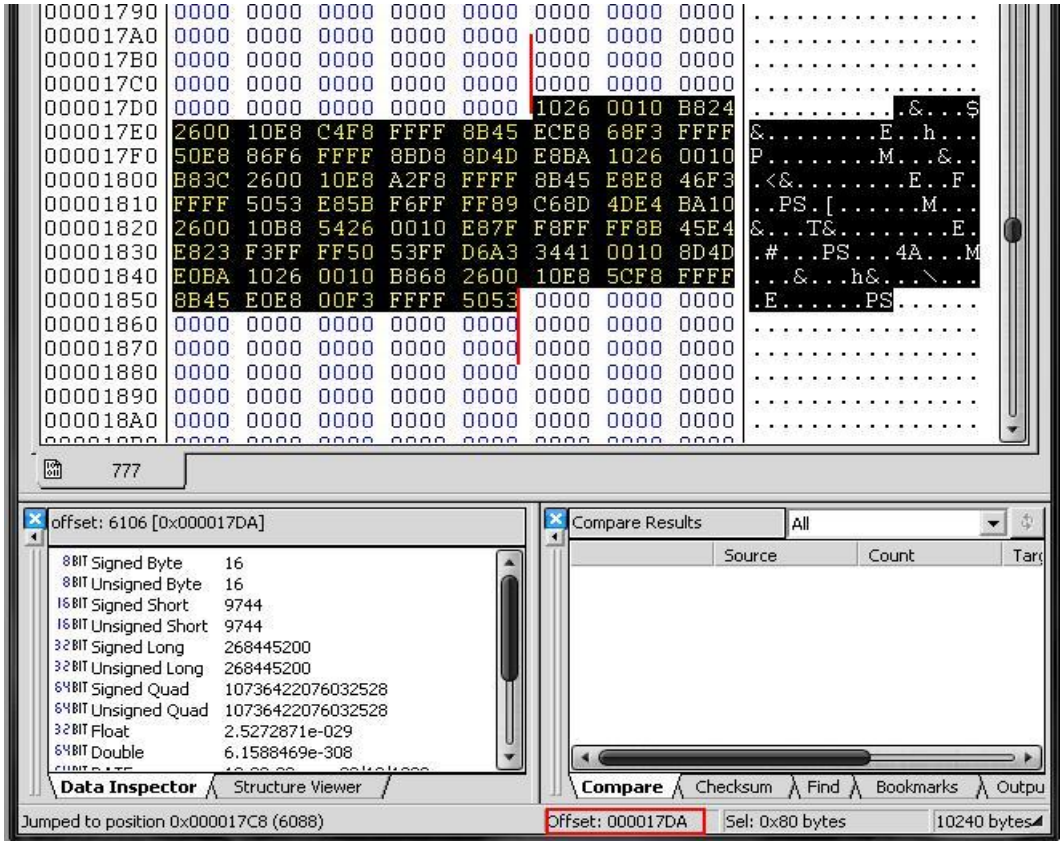
Para hacer eso solo seleccionamos las líneas que queremos llenar de ceros y presionamos CTRL+INSERT, y veremos la siguiente ventana, dejamos el cero y damos en OK.



Como se ve en la imagen de abajo nuestra selección se ha llenado de ceros y ahora procedemos a guardar los cambios y a escasear con el antivirus.

Bien a pesar de llenar de ceros esas líneas el archivo sigue siendo detectado, poco a poco tendremos esa firma.

Volvemos a repetir el método hasta cercar por completo la firma.



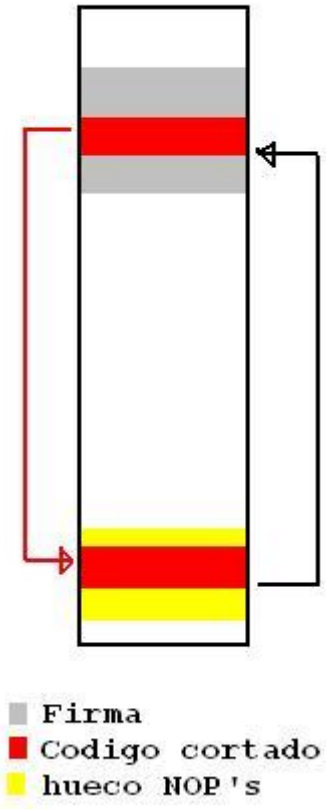
POR FIN!!! FIRMA ENCONTRADA [OFFSET 17DA-185A]

Ya encontramos la firma de KAV que abarca exactamente desde el **OFFSET 17DA al 185A**, verdad que no fue tan difícil??, ahora que ya sabemos la ubicación exacta de la firma procederemos a modificarla. Quizás se te esta ocurriendo modificarla directamente desde el editor Hexadecimal, pero lamento decirte que las compañías de antivirus seleccionan las partes mas sensibles del programa, de forma que si modificas aunque sea un solo OFFSET, lo dejaras inservible en la mayoría de los casos. Por lo que dada la situación te informo que estas a punto de aprender el **METODO RIT.**

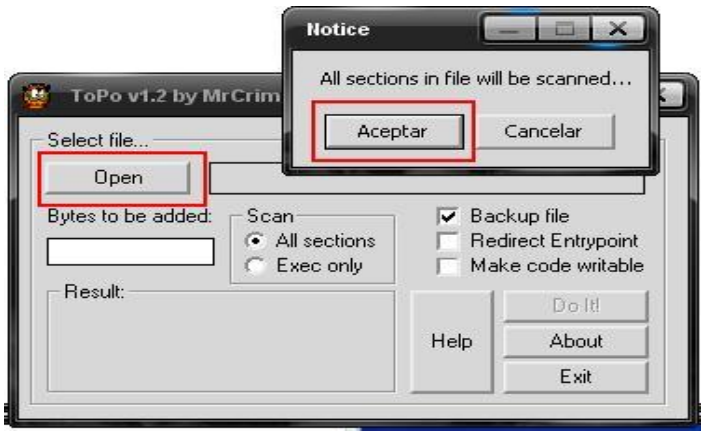
Modificaremos la firma pero SIN alterar el flujo del programa, para eso utilizaremos una conocida herramienta llamada OLLY, que es un depurador en el cual podremos interpretar todo lo que vemos en el editor HEX en lenguaje ensamblador ASM, y de esa forma alteraremos las firmas pero sin echar a perder nuestro software.

Si ya estas listo manos a la obra.

Lo primero es abrir el programa Topo y crearemos un hueco con instrucciones nulas (NOP) en nuestro ejecutable que será donde introduciremos posteriormente trozos de la firma, si no me entiendes no te preocupes es bastante sencillo y no requieres de grandes conocimientos para poder hacerlo, prácticamente lo que haremos será tomar un trozo de código que se encuentre dentro de la firma, la movemos a el hueco que nos hizo topo y luego indicamos una instrucción al final para que regrese desde el punto original donde cortamos, de esa forma alteramos la firma por completo pero respetando el flujo del programa.

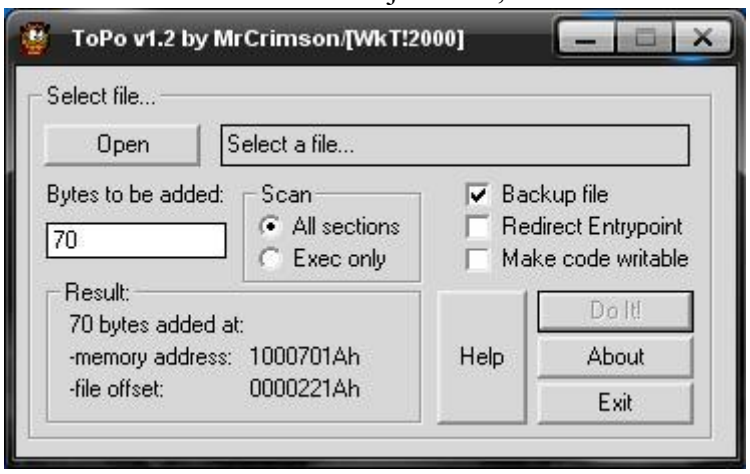


Bueno ahora procedemos a ejecutar topo y damos clic en Open, nos informa que todas las secciones del ejecutable serán escaneadas y damos en aceptar



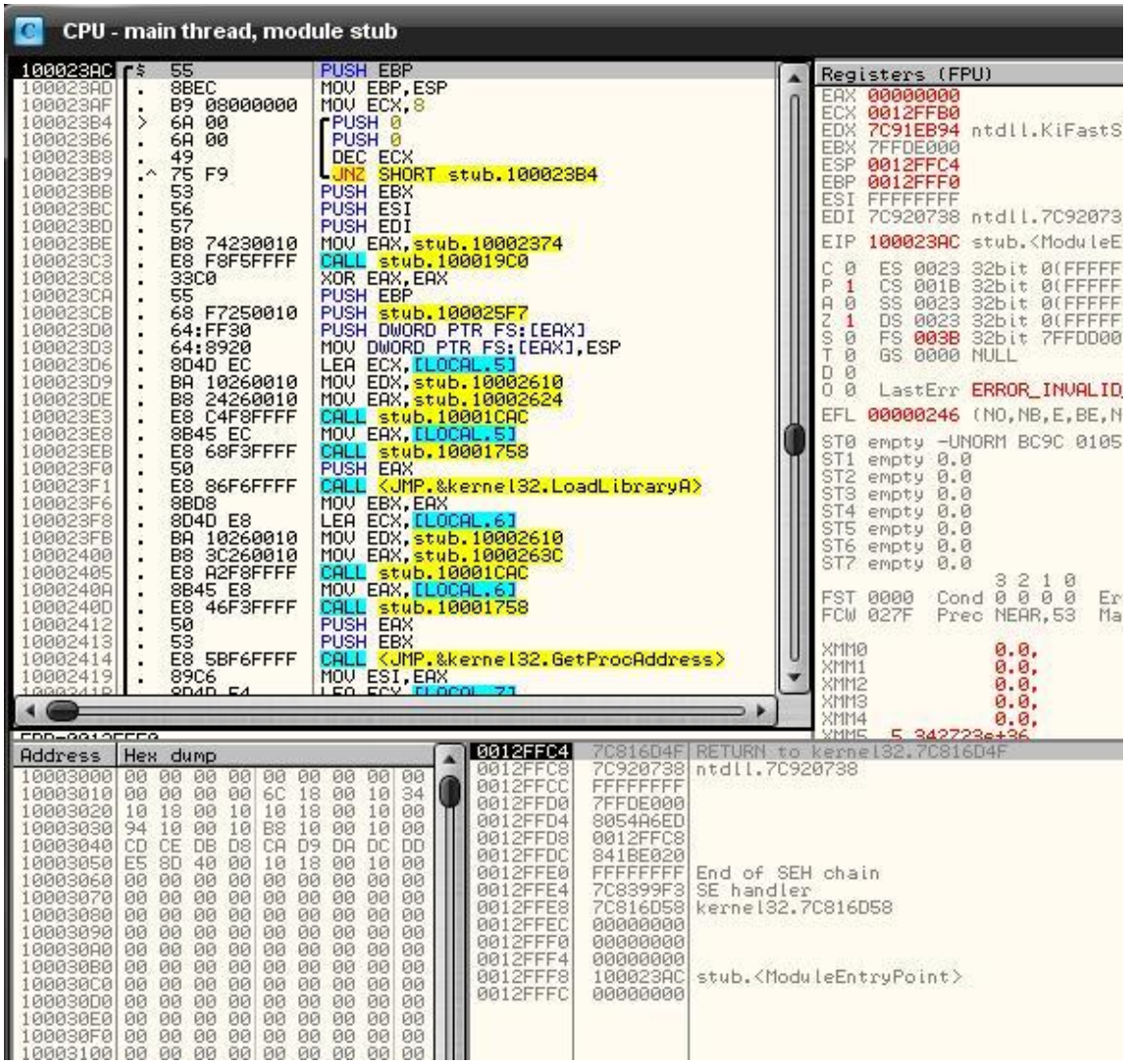
Seleccionamos el archivo STUB.exe y ahora nos pregunta si queremos utilizar una sección dentro del ejecutable o crear una nueva, lo dejamos en la primera opción y damos OK.

Bien ahora le indicamos la cantidad de bytes nulos a agregar, con 70 serán suficientes, pulsamos el botón Do It! Y nos toparemos con la siguiente ventana, en este paso es importante que copies la dirección de memoria que topo te dio, porque será donde ha metido todos esos NOP'S dentro del ejecutable, en este caso la dirección es: 1000701Ah.



Presionamos Exit y ahora estamos listos para el último paso.

Ejecutamos el programa OLLYDBG y arrastramos hacia la ventana de OLLY nuestro archivo stub.exe, una ves hecho nos encontraremos con algo similar a esto.

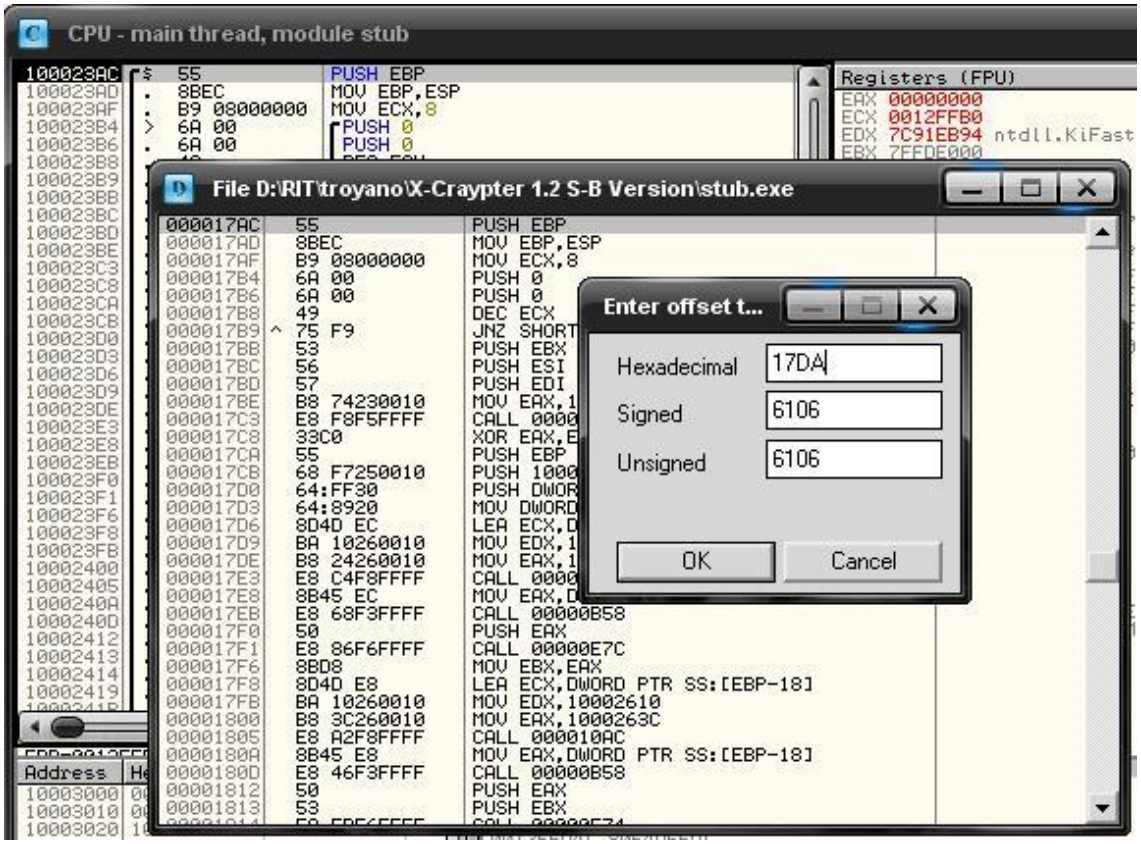


Lo que estas viendo es el programa en lenguaje ensamblador y abajo en Hexadecimal, la diferencia es que aquí todos esos números y letras que veías están interpretados en un lenguaje, por lo cual no estaremos modificando a ciegas.

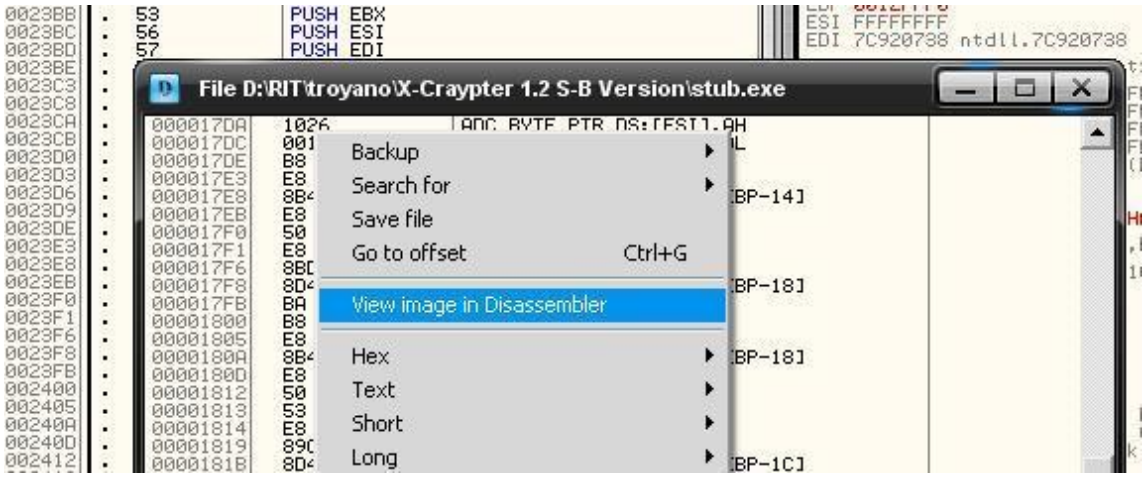
Lo siguiente es dar un clic con el botón derecho del Mouse en la ventana CPU y dar clic en view / executable file.

A continuación se abrirá una nueva ventana como la que se ve en la imagen de abajo

Una ves ubicados en la ventana que se abrió presionamos CTRL+G , que sirve para ir a algún punto dentro del ejecutable, en este caso le escribiremos el offset donde inicia la firma de kaspersky que es el 17DA, para posteriormente modificarla.

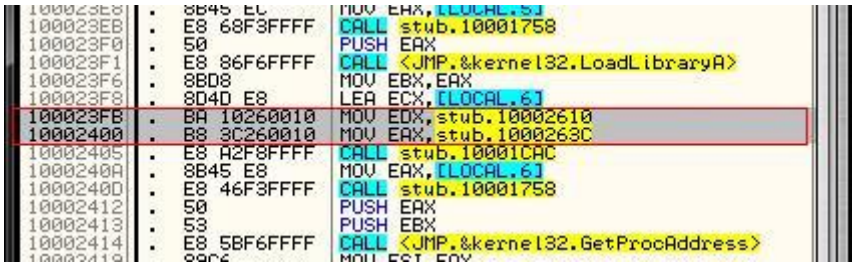


Una ves que presiones en el botón Ok serás enviado a la sección exacta donde se encuentra nuestra firma, das clic en la primer línea con botón derecho del Mouse y seleccionas la opción ***view image in Dissambler***, eso nos acomoda en la ventana de CPU en la ubicación de la firma para su modificación.

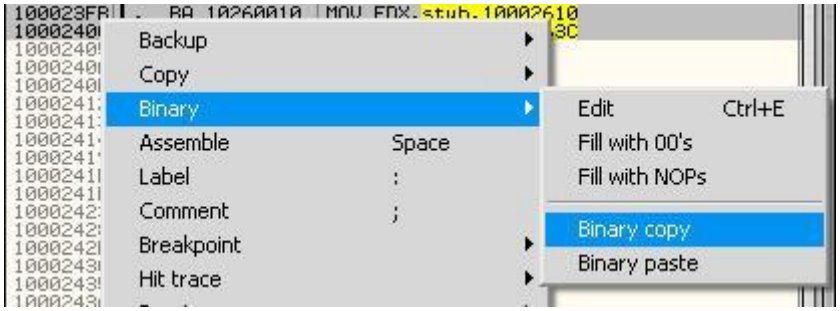


Ahora vamos a elegir el pedazo de código que vamos a modificar, en este caso tomaremos las dos instrucciones MOV que se encuentran en la dirección de memoria:

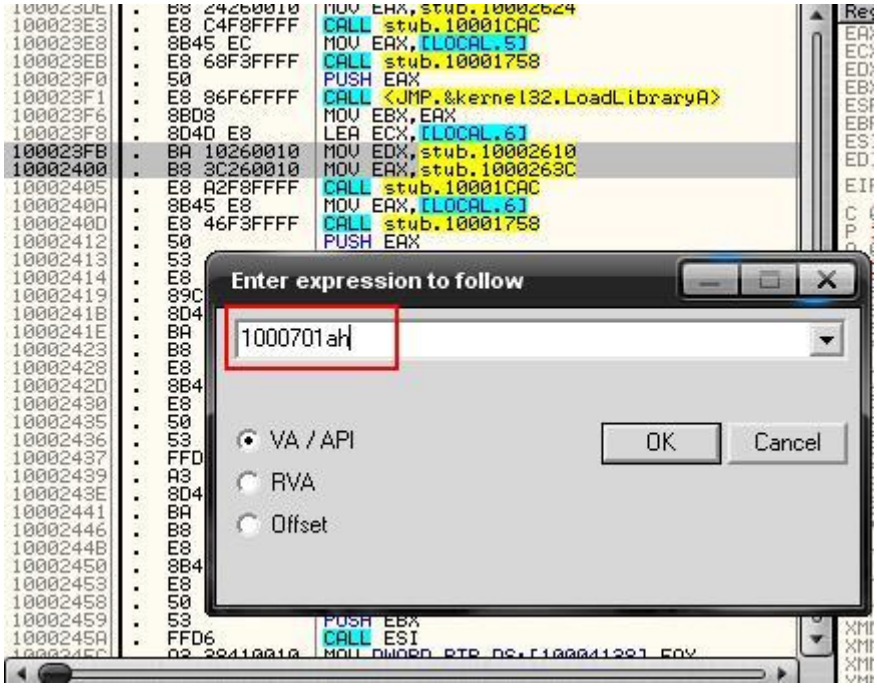
100023FB MOV EDX
10002400 MOV EAX



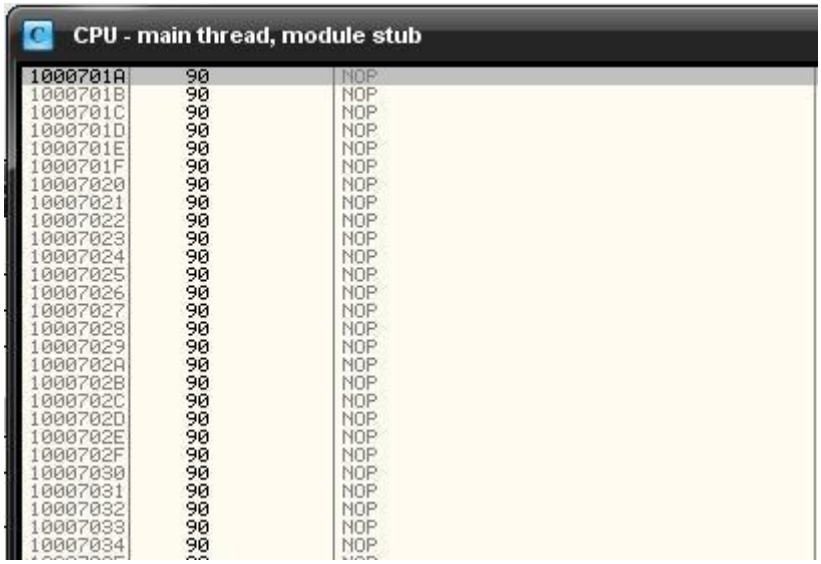
Vamos a copiarlas seleccionándolas y dando clic con botón derecho del Mouse en Binary /Binary copy



Ahora ya hemos copiado la instrucción que queremos mover de lugar, ahora para mandar ese pedazo al hueco que nos creo topo nos tenemos que dirigir a la direccion de memoria que topo nos dio, para eso presionamos CTRL+G y escribimos la direccion de memoria



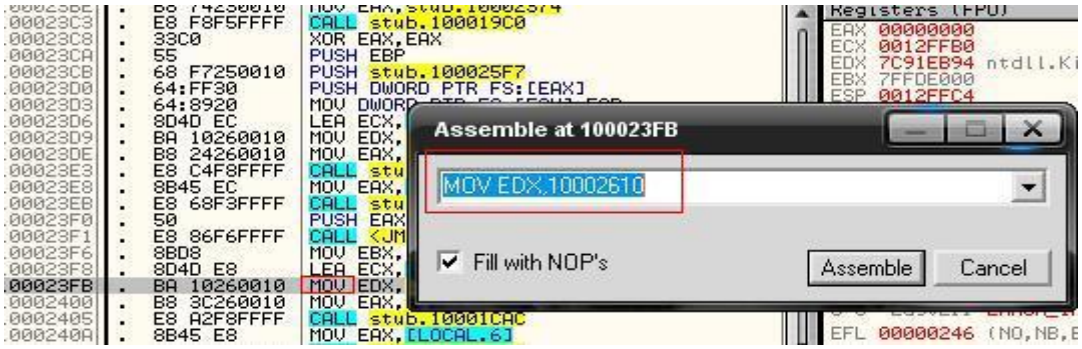
Ahora te encontraras con todos los NOP'S que topo nos creo, que es lugar donde pegaremos el trozo de código que copiamos de las dos instrucciones MOV.



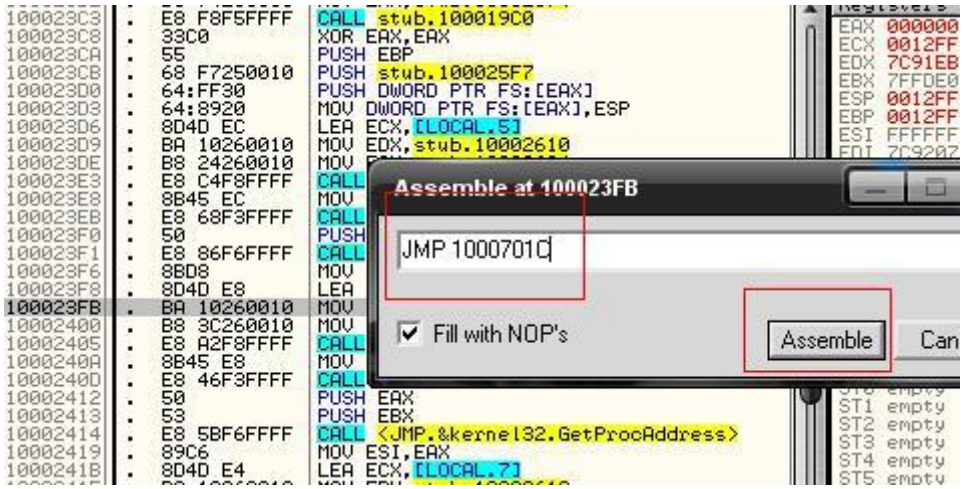
Para eso seleccionamos unos 6 NOP'S y damos clic derecho del Mouse binary / binary paste. Ahora y tenemos los dos MOV en el hueco, pero nos falta indicar la redirección de flujo, es decir indicarle al programa que lea este trozo de código y luego que regrese al punto original. Para eso apuntamos o nos memorizamos la dirección de memoria del primer MOV que en este caso es el 1000701C

```
10007012    00          DB 00
10007013    00          DB 00
10007014    00          DB 00
10007015    00          DB 00
10007016    00          DB 00
10007017    00          DB 00
10007018    00          DB 00
10007019    00          DB 00
1000701A    90          NOP
1000701B    90          NOP
1000701C    BA 10260010 MOV EDX,stub.10002610
10007021    B8 90909090 MOV EAX,90909090
10007026    90          NOP
10007027    90          NOP
10007028    90          NOP
10007029    90          NOP
1000702A    90          NOP
1000702B    90          NOP
1000702C    90          NOP
1000702D    90          NOP
1000702E    90          NOP
```

Ahora regresamos a donde estaban nuestros MOV originales y agregaremos un salto (JMP) a esta sección de código.
Para hacer eso damos doble clic en donde dice MOV y se abrirá la siguiente ventana.



Ahora cambiamos ese valor por nuestra instrucción JMP 1000701C
Con esta instrucción le estamos indicando que de un salto a la parte donde nosotros pegamos las instrucciones MOV en el hueco donde están los NOP.



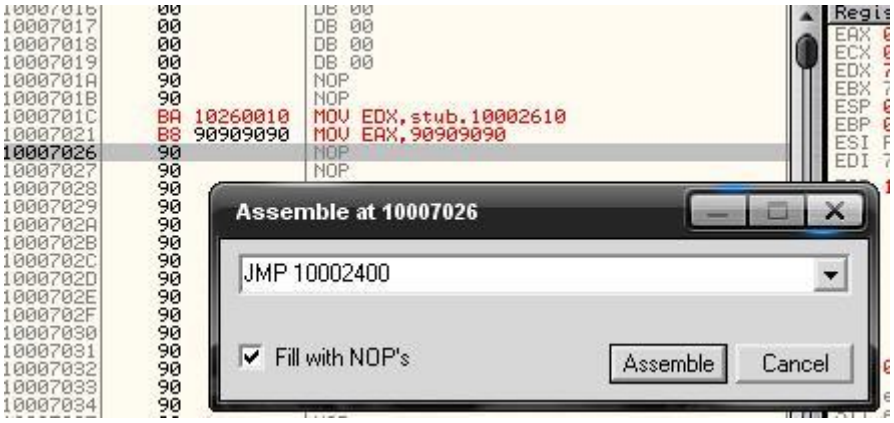
y una ves escrita la instrucción damos clic en Assamble

```
100023F8  .  8D4D E8      LEA ECX,[LOCAL.6]
100023FB  .  E9 1C4C0000  JMP stub.1000701C
10002400  .  B8 3C260010  MOV EAX,stub.1000263C
10002405  .  E8 A2F8FFFF  CALL stub.10001CAC
```

Debió quedar como la imagen de arriba, ahora apuntamos la dirección de memoria que esta abajo del JMP

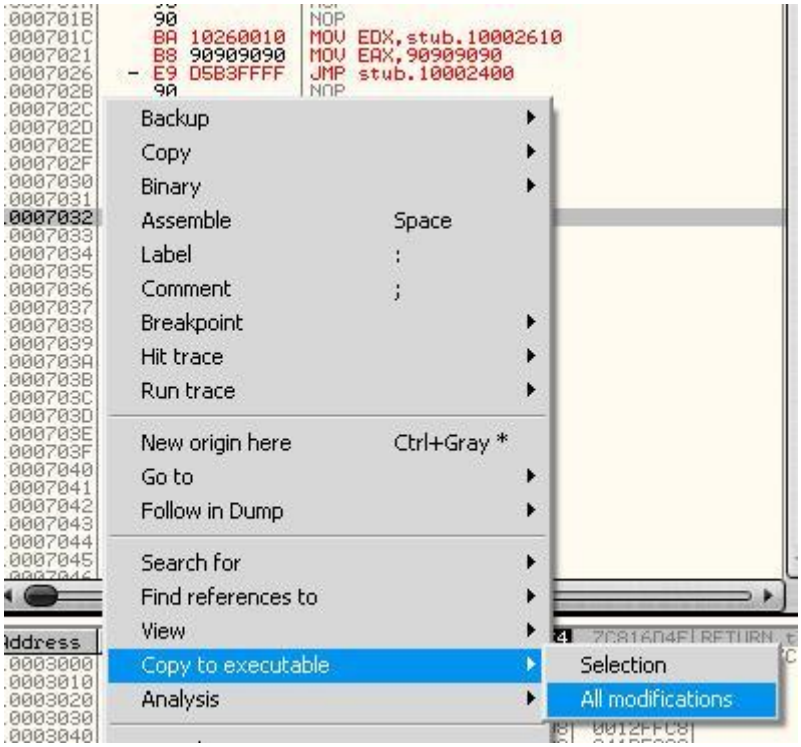
10002400

Regresamos al hueco donde pusimos los MOV y hacemos lo mismo justo después del segundo MOV hacemos otro salto pero esta ves hacia la dirección de memoria 10002400, con esto cerraríamos el flujo y modificamos las firmas.

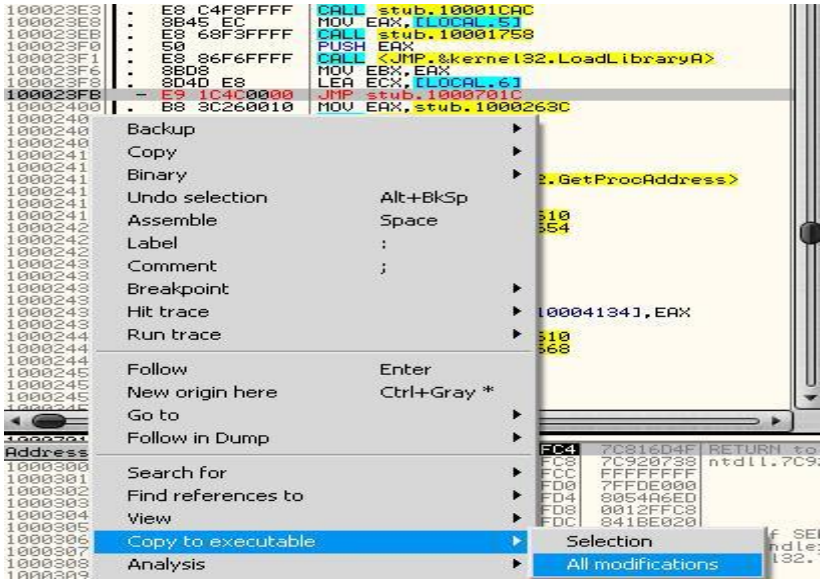


Damos clic en Assamble y nos quedara algo como esto

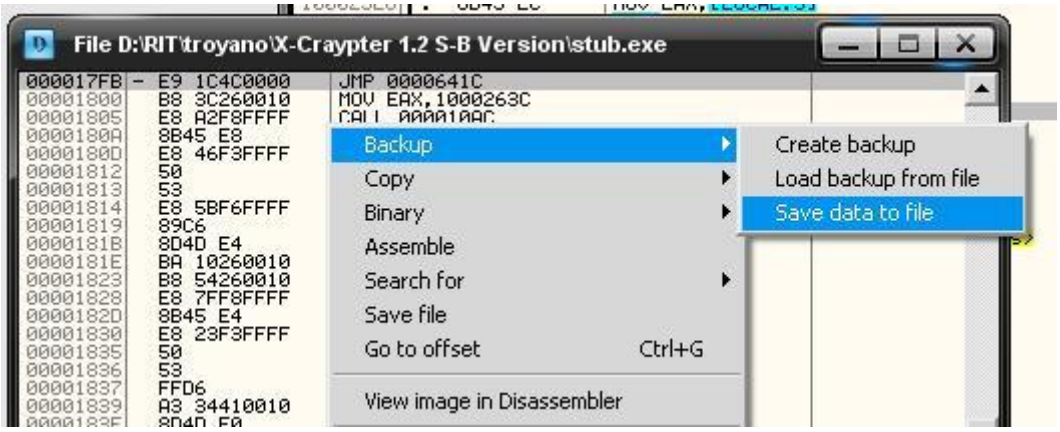
Bien ya hemos terminado de redireccionar el flujo y hemos alterado la firma del antivirus, ahora procederemos a guardar los cambios, para eso damos clic con botón derecho del Mouse y damos clic en copy to executable / all modifications, después le damos en copy all.



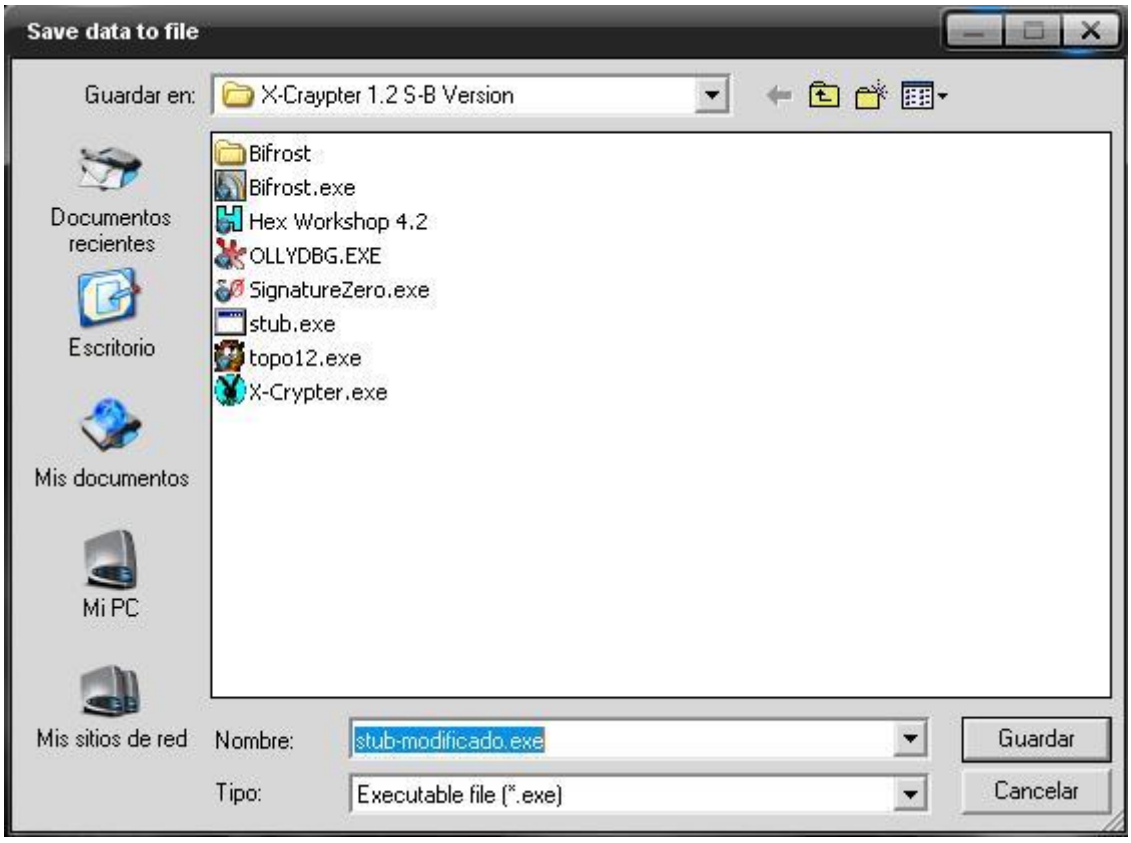
Lo mismo donde hicimos el otro salto



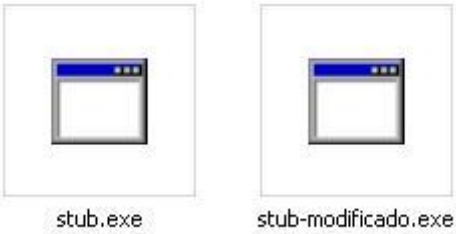
Y en la ventana file damos clic derecho y en backup / save data to file



Y lo guardamos con otro nombre.

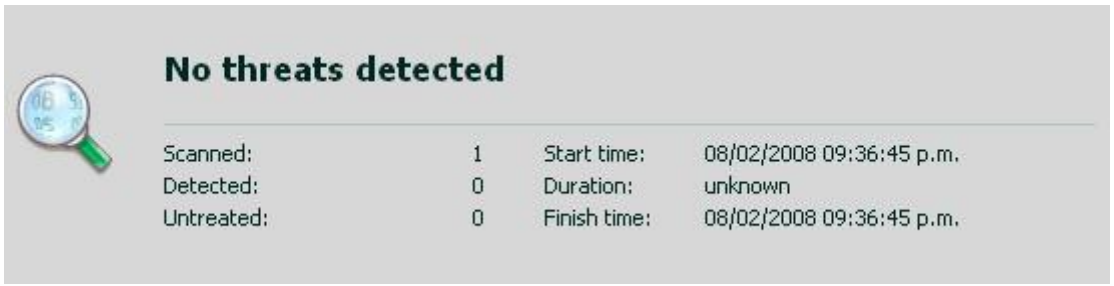


Ahora escaneo ambos stub el original y el modificado y valla!! el antivirus ya no detecta el nuestro.



ANTES:

DESPUES:



Ya tenemos nuestro crypter totalmente indetectable a KASPERSKY antivirus.
Para que veas como se modifico la firma te pongo el antes y el después en HEX.

ANTES:

```
8D4D ECBA 1026 0010 B824 d.Od. .M...&...$
FFFF 8B45 ECE8 68F3 FFFF &.........E..h...
8BD8 8D4D E8BA 1026 0010 P.........M...&..
A2F8 FFFF 8B45 E8E8 46F3 .<&.........E..F.
F6FF FF89 C68D 4DE4 BA10 ..PS.[......M...
```

DESPUES:

```
8D4D ECBA 1026 0010 B824 d.Od. .M...&...$
FFFF 8B45 ECE8 68F3 FFFF &.........E..h...
8BD8 8D4D E8E9 1C4C 0000 P.........M...L..
A2F8 FFFF 8B45 E8E8 46F3 .<&.........E..F.
F6FF FF89 C68D 4DE4 BA10 ..PS.[......M...
```

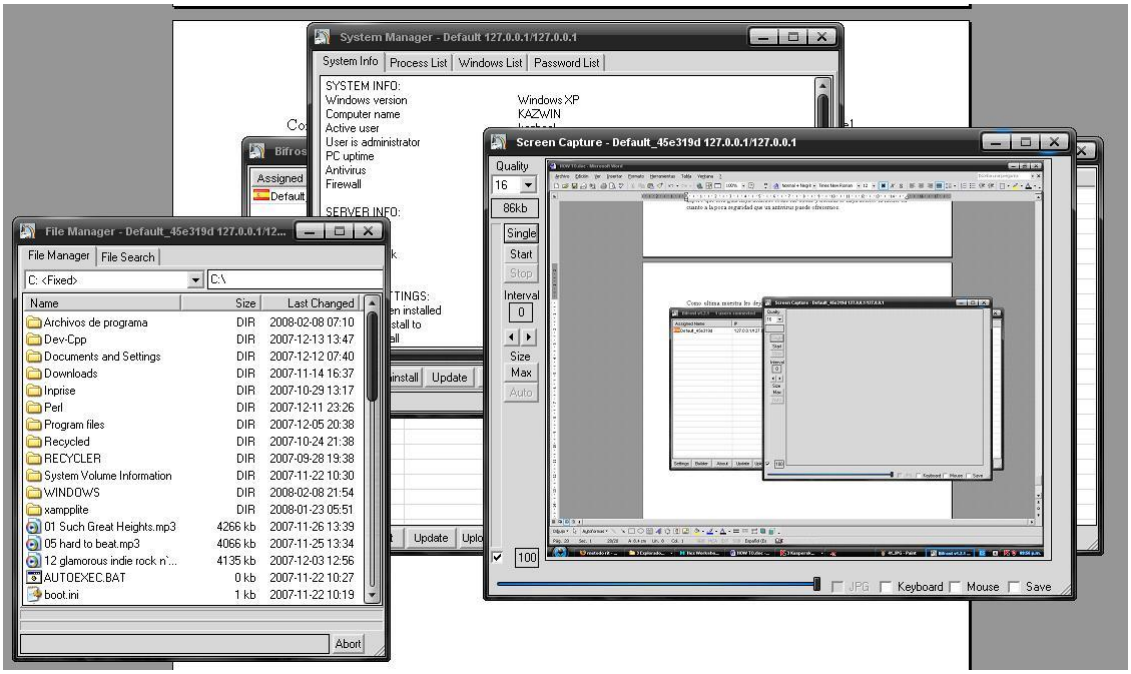
Bien ya has aprendido a hacer tus aplicaciones totalmente INDETECTABLES, solo basta con un poco de practica y harás este proceso en cuestión de minutos. Como dato extra te informo que los antivirus coinciden en firmas, por lo que con unas 3 modificaciones obviamente con diferente antivirus, habrás pasado más de 15 o 20 antivirus, por supuesto lo más populares como son
KASPERSKY NORTON, AVG, AVAST, PANDA, NOD32, MCFEE, AVAST, BITDEFENDER etc…

Ahora solo tienes que utilizar este STUB modificado en el crypter y aplicarlo a cualquier troyano y lo dejaras indetectable en cuestión de segundos.

Espero que esta guía haya aclarado todas tus dudas y además te haya abierto la mente en cuanto a la poca seguridad que un antivirus puede ofrecernos.

Como ultima muestra les dejo una hermosa captura del BIFROST funcionando con el kaspersky activo.

SOLO 36.3 KB Y TOTALMENTE INDETECTABLE



ADEMAS FUNCIONA PERFECTAMENTE

Se supone debería dar alarma no???

Bien con esto me despido por ahora, mucha suerte con sus pruebas y recuerden que por nada del mundo utilicen servicios de escaneo Online o entonces echaran por tierra todo lo que hicieron, si necesitan trabajar con varios antivirus utilicen maquinas virtuales con varias snapshots para cada antivirus.

!!!!NADA DE VIRUSTOTAL
NI PAGINAS COMO ESAS!!!!

octalh@gmail.com