A raíz de la entrada anterior algunos me habéis preguntado como es posible que aprovechen cualquier antivirus para hacer indetectable una muestra. Evidentemente queda fuera de la temática de este blog, y por descontado de Hispasec, dar ideas en ese sentido, pero si puedo comentar las cosas más extendidas y conocidas por todos, lo que nos puede dar una idea de porque hay tal proliferación de malware en la actualidad y de los problemas de las soluciones basadas exclusivamente en firmas.

Básicamente el uso de los antivirus es como herramienta de ensayo y error, van realizando modificaciones en el malware hasta dar con una versión que no es detectada por el antivirus, de modo que ninguna firma es capaz de identificarlo. Si es una creación nueva o tiene el código fuente del bicho en cuestión las opciones de modificar el binario final son mayores, sino también hay formas bastante sencillas de conseguirlo modificando el binario directamente.

Contrariamente a lo que la mayoría de personas cree, la modificación de un malware, como por ejemplo un troyano, no requiere conocimientos de programación, incluso muchas veces se hace a golpe de ratón dando algunos clicks. El caso más habitual es el uso de empaquetadores o packers, como compresores o cifrados de binarios. Básicamente es una utilidad donde eliges un binario (el troyano) y te devuelve otro binario modificado (compactado, cifrado, incrustado en otro ejecutable, etc). A efectos prácticos el binario resultante tendrá un aspecto "exterior" diferente al original, pero a nivel funcional se comportará igual. Si el motor antivirus no reconoce ese método de empaquetamiento no podrá desenmascarlo y detectarlo en base a las firma con la que reconocía al troyano original.

Otro método también muy extendido es modificar directamente el binario, para lo que es necesario detectar que porción del código es la reconocida por la firma del antivirus. Hay formas de hacerlo manualmente, pero también han desarrollado pequeñas utilidades que van realizando modificaciones de forma automática y comprobando por ensayo y error contra el antivirus hasta que devuelve las posiciones exactas que han de modificar. Dependiendo de lo que haya modificar requerirá desensamblar y modificar algunas instrucciones para evitar "estropear" el troyano o, en algunos casos, directamente se podrá modificar con un editor hexadecimal.

Este tipo de prácticas es una plaga en la actualidad, de hecho una gran parte de las variantes que surgen son modificaciones más o menos burdas de un espécimen original.

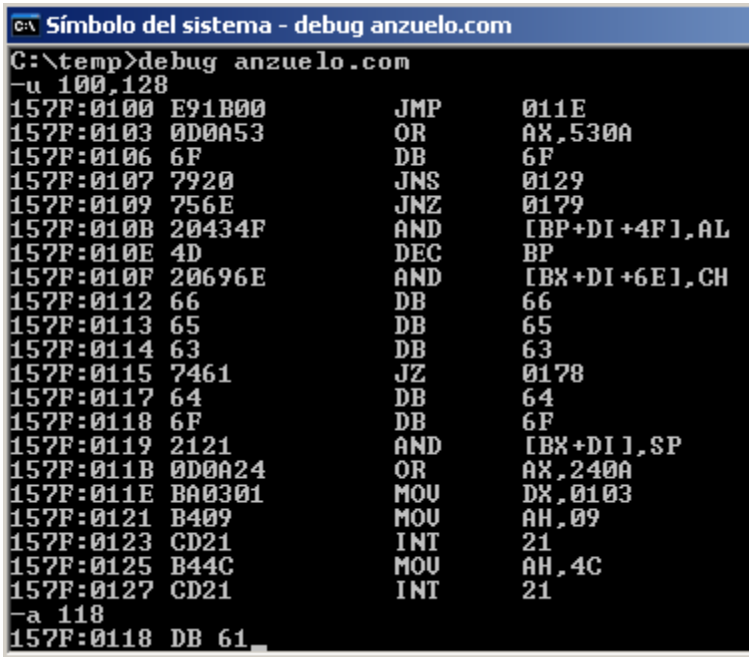
La buena noticia es que este tipo de prácticas masivas no tienen en cuenta la evolución de las soluciones antivirus, y cada vez más los atacantes se llevan sorpresas al ver que su versión recien modificada termina siendo cazada y reconocida por los antivirus de los usuarios que utilizan técnicas más avanzadas o complementarias a las firmas, como por ejemplo el análisis del comportamiento. Estos antivirus a su vez recolectan y envían las muestras sospechosas a los laboratorios para generar firmas específicas.

Este tipo de detecciones no las pueden comprobar con motores antivirus llamados a través de línea de comandos (que es lo que suelen hacer en los tests de ensayo-error), sino que requiere que la solución antivirus esté totalmente instalada en el equipo y ejecutar la variante del troyano en el mismo. Sin duda se les complica el invento, lo que son buenas noticias para el resto de nosotros.

No obstante aun hay mucho antivirus que básicamente depende de las firmas tradicionales, y este tipo de prácticas sigue siendo efectiva contra ellos.

Para terminar vamos con un ejemplo práctico, lo suficientemente simple y absurdo como para ver lo débil que puede resultar una firma y, al mismo tiempo, que NO sirva de pista para que cualquiera pueda imitarlo con un malware auténtico. Para ello vamos a aprovechar el anzuelo.com de la entrada anterior.

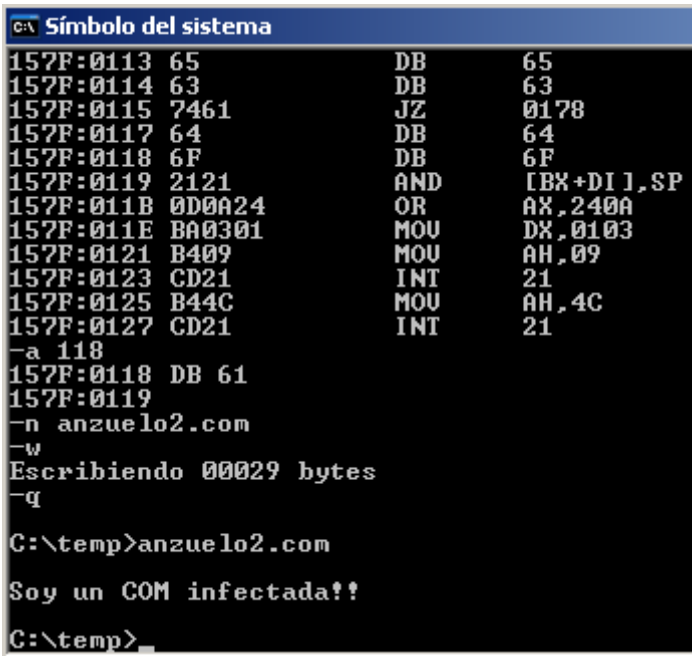
Siguiendo las instrucciones de la entrada anterior llegamos hasta el desensamblado del código, y lo que vamos a hacer es modificar un sólo byte, en concreto el que se encuentra en la dirección 118h que contiene el valor 6F (instrucción DB 6F) que modificaremos por 61 (instrucción DB 61). Para ello ejecutamos el comando -a 118. A continuación introduciremos la instrucción: DB 61, pulsamos intro, aparecerá la línea 119, pulsamos intro de nuevo.



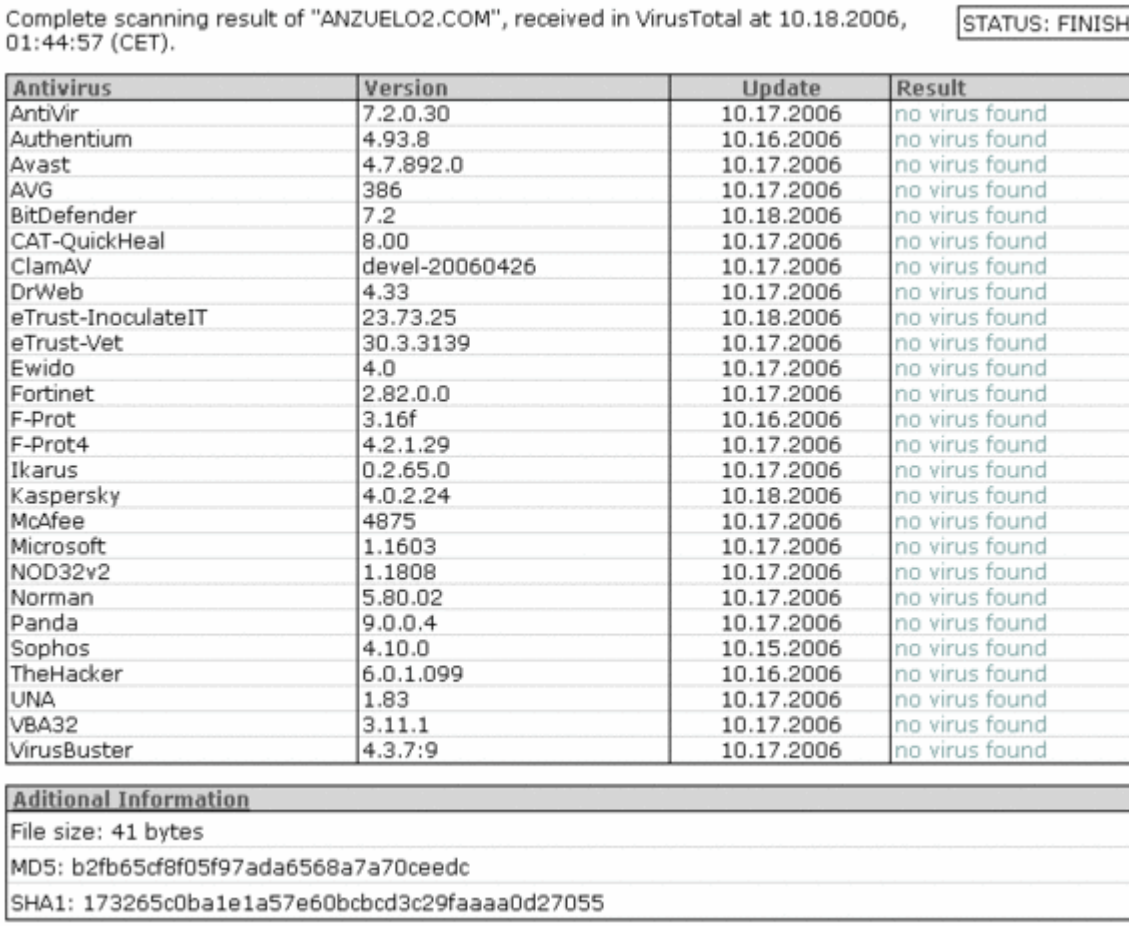
Con ésto lo que hemos hecho es simplemente cambiar una "o" (código ASCII 111, 6F en hexadecimal) por una "a" (código ASCII 97, 61 en hexadecimal). De manera que habremos "cambiado el sexo" (o al menos creado un conflicto de identidad sexual o género) a nuestro ejecutable, en vez de decir "Soy un com infectado!!" ahora dirá "Soy

un com infectada!!".

Para escribir en disco esta modificación vamos a dar unos comandos más a debug. Comando -n anzuelo2.com, comando -w, comando -q. Con esto habremos creado en el mismo directorio un nuevo archivo anzuelo2.com que recoge los cambios realizados. Para hacer la prueba puedes ejecutar anzuelo2.com.



Si pasamos anzuelo2.com por los motores antivirus de McAfee o TrendMicro, y a diferencia del anzuelo.com original, veremos que ya no es detectado. Son más permisivos con el sexo femenino ;)



Complete scanning result of "ANZUELO2.COM", received in VirusTotal at 10.18.2006, 01:44:57 (CET). STATUS: FINISH

Antivirus	Version	Update	Result
AntiVir	7.2.0.30	10.17.2006	no virus found
Authentium	4.93.8	10.16.2006	no virus found
Avast	4.7.892.0	10.17.2006	no virus found
AVG	386	10.17.2006	no virus found
BitDefender	7.2	10.18.2006	no virus found
CAT-QuickHeal	8.00	10.17.2006	no virus found
ClamAV	devel-20060426	10.17.2006	no virus found
DrWeb	4.33	10.17.2006	no virus found
eTrust-InoculateIT	23.73.25	10.18.2006	no virus found
eTrust-Vet	30.3.3139	10.17.2006	no virus found
Ewido	4.0	10.17.2006	no virus found
Fortinet	2.82.0.0	10.17.2006	no virus found
F-Prot	3.16f	10.16.2006	no virus found
F-Prot4	4.2.1.29	10.17.2006	no virus found
Ikarus	0.2.65.0	10.17.2006	no virus found
Kaspersky	4.0.2.24	10.18.2006	no virus found
McAfee	4875	10.17.2006	no virus found
Microsoft	1.1603	10.17.2006	no virus found
NOD32v2	1.1808	10.17.2006	no virus found
Norman	5.80.02	10.17.2006	no virus found
Panda	9.0.0.4	10.17.2006	no virus found
Sophos	4.10.0	10.15.2006	no virus found
TheHacker	6.0.1.099	10.16.2006	no virus found
UNA	1.83	10.17.2006	no virus found
VBA32	3.11.1	10.17.2006	no virus found
VirusBuster	4.3.7:9	10.17.2006	no virus found

Aditional Information
File size: 41 bytes
MD5: b2fb65cf8f05f97ada6568a7a70ceedc
SHA1: 173265c0ba1e1a57e60bcbcd3c29faaaa0d27055

Enviado por **bquintero** a las 02:18 | Enlace permanente | Comentarios (7) | Trackbacks (0)

<< Leyenda urbana sobre VirusTotal | Principal | Antiphishing en Internet Explorer 7 >>

Comentarios

Re: Modificando malware para hacerlo indetectable

"pero también han desarrollado pequeñas utilidades que van realizando modificaciones de forma automática y comprobando por ensayo y error contra el antivirus hasta que devuelve las posiciones exactas que han de modificar"

una consulta, cual es o como se llama ese tipo de herramientas?? nunca habia escuchado de ella...

Posted by: **bkral** at octubre 19,2006 21:16

Re: Modificando malware para hacerlo indetectable

una consulta, cual es o como se llama ese tipo de herramientas?? nunca habia escuchado de ella...

Cada cual le pone el nombre que le parece, normalmente la gente se la programa para uso propio, pero buscando por foros underground puedes encontrar alguna pública que te de una pista de como funcionan.

No puedo poner aquí en el blog referencias directas o URLs a material que se considere malware (por razones obvias), pero te puedo dar la nomenclatura con que algunos antivirus detectan alguna de estas herramientas públicas con cierta solera, es pista más que suficiente si estás interesado en encontrarlas y ver como trabajan (supongo que tu interés e intenciones son legítimas):

AntiVir TR/Virtl.Avpsof.1
Avast Win32:Trojan-gen. {VC}
BitDefender Virtool.Avpsof.A
Ewido Not-A-Virus.VirTool.Win32.Avpsof
Fortinet Dial/Avpsof
Kaspersky VirTool.Win32.Avpsof
McAfee potentially unwanted program Tool-AVPOffset
NOD32 Win32/Avpsof.A
Panda VirTool/AvpOffset
TheHacker Trojan/Avpsof
UNA VirTool.Win32.Avpsof.DE29
VBA32 VirTool.Win32.Avpsof