ESTEGANOGRAFÍA, EL ARTE DE OCULTAR INFORMACIÓN

Del griego *steganos* (oculto) y *graphos* (escritura), la esteganografía se puede definir como la ocultación de información en un canal encubierto con el propósito de prevenir la detección de un mensaje oculto.

La esteganografía estudia el conjunto de técnicas cuyo fin es insertar información sensible dentro de otro fichero. A este fichero se le denomina fichero contenedor (gráficos, documentos, programas ejecutables, etc.). De esta forma, se consigue que la información pase inadvertida a terceros, de tal forma que sólo sea recuperada por un usuario legítimo que conozca un determinado algoritmo de extracción de la misma.

Ilustración 1: Recortes de periódico: "La esteganografía no es sólo un ingenio teórico"


USA TODAY

Home
News
Money
Sports
Life
Tech
Main Categories
Tech briefs
Web Guide
Tech Investor
Product reviews

CyberSpeak

• E-mail this story • Subscribe to the newspaper • Sign-up for e-mail news

12/19/2001 - Updated 09:30 AM ET

Bin Laden's messages could be hiding in plain sight

Now we have to worry about steganography. That's right: steganography. No not the ancient art of writing on a stegosaurus. It's a way to conceal a coded

Uso extendido

ETA no es la única organización terrorista que acude a programas de encriptación para proteger sus documentos y bases de datos.

Al Qaeda tiene incluso una aplicación propia y de distribución libre, el conocido como **Mujahidin's Secret**, capaz de codificar y enviar de forma segura todo tipo de archivos a través de internet.

También se ha detectado el uso de la esteganografía, una técnica muy antigua pero que ahora aprovecha las nuevas tecnologías y que permite camuflar información relevante en documentos, como fotografías, textos o incluso canciones, en apariencia inofensivos.

Fuente: INTECO

Esta ciencia ha suscitado mucho interés en los últimos años debido a que ha sido utilizada por organizaciones criminales y terroristas. No obstante, no se trata de ningún nuevo ingenio, se lleva empleando desde la más remota antigüedad. Este artículo pretende introducir al lector en el campo de la esteganografía, clarificando sus diferencias con la criptografía y mostrando ejemplos de software para hacer uso de esta técnica.

I Historia y orígenes

Más de 400 años antes de Cristo, Herodoto ya reflejó en su libro *Las Historias* el uso de la esteganografía en la antigua Grecia. En dicho libro describe como un personaje toma un cuadernillo de dos hojas o tablillas; raya bien la cera que las cubre y en la madera misma graba un mensaje y lo vuelve a cubrir con cera.

Otra historia, en el mismo libro, describe como otro personaje rasura a navaja la cabeza de uno de sus esclavos y le tatúa un mensaje en el cuero cabelludo. Así, espera a que le vuelva a crecer el cabello y lo manda al receptor del mensaje con instrucciones de que le rasuren la cabeza.

Ilustración 2: Tablilla para escribir con mensaje oculto grabado en la madera bajo la cera

Fuente: INTECO

Un ejemplo histórico más de uso de la esteganografía es el libro *Hypnerotomachia Poliphili* de Francesco Colonna, que data de 1499. En él, tomando la primera letra de sus 38 capítulos se puede leer "*Poliam frater Franciscus Columna peramavit*", que se traduce por "*El hermano Francesco Colonna ama apasionadamente a Polia*".

De manera similar, durante la Segunda Guerra Mundial se hacen pequeñas perforaciones sobre las letras de interés de un periódico de tal forma que al sostenerlo a la luz se pueden observar todas aquellas letras seleccionadas e interpretarlas en forma de mensaje.

Bastante más familiar para el lector resulta el ejemplo de la tinta invisible. Son muchos los niños que juegan a enviarse mensajes escritos con zumo de limón o substancias similares (con alto contenido en carbono), de tal forma que al calentar la superficie sobre la que se escribe el mensaje, éste aparece en un tono color café. Esta técnica se puede hacer más compleja si se involucran reacciones químicas.

Queda patente que la esteganografía ha estado presente en nuestra civilización desde tiempos inmemoriales y ha sido tradicionalmente empleada por las agencias militares y de inteligencia, los criminales y la policía, así como por civiles que desean saltarse restricciones gubernamentales. Ahora bien, mientras la esteganografía clásica se basaba únicamente en el desconocimiento del canal encubierto bajo uso, en la era moderna se emplean canales digitales (imagen, video, audio, protocolos de comunicaciones, etc.) para alcanzar el objetivo. En muchos casos el objeto contenedor es conocido, lo que se ignora es el algoritmo de inserción de la información en dicho objeto.

II Definiciones y fundamentos teóricos

La esteganografía es una solución al clásico problema del prisionero. En una prisión de alta seguridad dos internos en celdas separadas, Rómulo y Remo, se quieren comunicar para elaborar un plan de fuga. Ahora bien, toda comunicación intercambiada entre ellos es examinada por un guardia que los aísla por completo ante cualquier sospecha de comunicación encubierta. Con la esteganografía el guardia inspecciona mensajes aparentemente inocuos que contienen un canal subliminal muy útil para los prisioneros.

Se pueden observar distintos actores implicados en el campo de la esteganografía:

- **Objeto contenedor:** se trata de la entidad que se emplea para portar el mensaje oculto. Acudiendo al ejemplo de los mensajes sobre el cuero cabelludo, el objeto contenedor es el esclavo en sí.

- **Estego-objeto:** se trata del objeto contenedor más el mensaje encubierto. Siguiendo con el ejemplo, se trata del esclavo una vez se ha escrito en su cuero cabelludo el mensaje y se le ha dejado crecer el pelo.

- **Adversario:** son todos aquellos entes a los que se trata de ocultar la información encubierta. En el ejemplo de la prisión, se trata del guardia que entrega los mensajes a uno y otro prisionero. Este adversario puede ser pasivo o activo. Un adversario pasivo sospecha que se puede estar produciendo una comunicación encubierta y trata de descubrir el algoritmo que se extrae del estego-objeto, pero no trata de modificar dicho objeto. Un adversario activo, además de tratar de hallar el algoritmo de comunicación encubierta, modifica el estego-objeto con el fin de corromper cualquier intento de mensajería subliminal.

- **Estegoanálisis:** ciencia que estudia la detección (ataques pasivos) y/o anulación (ataques activos) de información oculta en distintas tapaderas, así como la posibilidad de localizar la información útil dentro de la misma (existencia y tamaño).

Teniendo en cuenta que pueden existir adversarios activos, una buena técnica esteganográfica debe ser robusta ante distorsiones, ya sean accidentales o fruto de la interacción de un adversario activo.

La robustez ante distorsiones también suele ser un objetivo de la criptografía, ahora bien, la esteganografía y la criptografía son campos distintos. En la criptografía, el objetivo es asegurar la confidencialidad de la información ante los ojos de un interceptor que es capaz de ver el criptograma, aun cuando éste conoce el algoritmo que lo genera. En cambio, la esteganografía busca ocultar la presencia del mensaje en sí; ya que si se llega a identificar la posición del mensaje se conoce directamente la comunicación (conocido el algoritmo de ocultación), lo que no ocurre en el caso del criptograma.

Por tanto, la esteganografía en solitario entra en profunda contradicción con uno de los principios básicos de la seguridad: la seguridad por oscuridad (desconocimiento) no funciona.

A principios del siglo XX, Kerkhoff formula una serie de principios que se han erigido como pilares básicos en el campo de la seguridad, uno de ellos indica: "*asume que el usuario (malicioso) conoce todos los procedimientos de cifrado*". Si se aplica dicho principio a la esteganografía, esto significa asumir que el guardia conoce el algoritmo que oculta el mensaje en el objeto contenedor, lo cual implica el aislamiento inmediato de los presos.

Para que la esteganografía sea de más utilidad se debe combinar con la criptografía. El mensaje a intercambiar se ha de cifrar (de forma robusta) y luego introducir en el objeto contenedor. De esta forma, aunque un interceptor descubra el patrón esteganográfico, jamás puede llegar a conocer el mensaje intercambiado.

La combinación de estas dos técnicas tiene otra ventaja adicional, cuando se emplea la criptografía en solitario se conoce que se están intercambiando mensajes, lo cual puede servir como punto de partida para un ataque con el fin de descubrir dicho mensaje. Al introducir la esteganografía, en una gran mayoría de casos ni siquiera se conoce que existe una comunicación cifrada.

III Funcionamiento y ejemplos

Este artículo se va a centrar en el objeto contenedor más utilizado: las imágenes digitales. Especialmente, en formato BMP por su sencillez (es un formato de fichero sin compresión). Las ideas presentadas se pueden extender a otros formatos (JPG, PNG, etc.) y a otros contenedores (vídeos, documentos, etc.) siempre que se respeten las particularidades de cada formato.

Sustitución de bits del objeto contenedor

Esta técnica consiste en sustituir ciertos bits del fichero contenedor por los de la información a ocultar. La ventaja de este enfoque es que el tamaño del fichero contenedor no se ve alterado y, gracias a la redundancia y/o exceso de detalle en dichos ficheros, en muchas ocasiones tampoco su calidad.

Por ejemplo, en un fichero de sonido se pueden emplear los bits que no son audibles por el oído humano para ser reemplazados por los bits del mensaje.

Si se trabaja con imágenes, el método tradicional consiste en sustituir los bits menos significativos (LSB), en una escala de color de 24 bits (mas de 16 millones de colores). Esto se traduce tan sólo en que un píxel con un tono rojo se ve un 1% más oscuro. En muchos casos son cambios inapreciables a los sentidos humanos que tan sólo pueden ser detectados mediante análisis computacional de la estructura de los ficheros.

Los archivos BMP son un formato estándar de imagen de mapa de bits en sistemas operativos DOS, Windows y válido para MAC y PC. Soporta imágenes de 24 bits (millones de colores) y 8 bits (256 colores), y puede trabajar en escala de grises, RGB y CMYK.

Ilustración 3: Zoom ilustrativo sobre píxel de una imagen

Fuente: INTECO

Cada píxel de un archivo BMP de 24 bits está representado por tres bytes. Cada uno de estos bytes contiene la intensidad de color rojo, verde y azul (*RGB: red, green, blue*). Combinando los valores en esas posiciones podemos obtener los 2^{24}, más de 16 millones, de colores que puede mostrar un píxel.

A su vez, cada byte contiene un valor entre 0 y 255, o lo que es lo mismo, entre 00000000 y 11111111 en binario, siendo el dígito de la izquierda el de mayor peso. Lo que demuestra que se pueden modificar los bits menos significativos de un píxel sin producir mayor alteración.

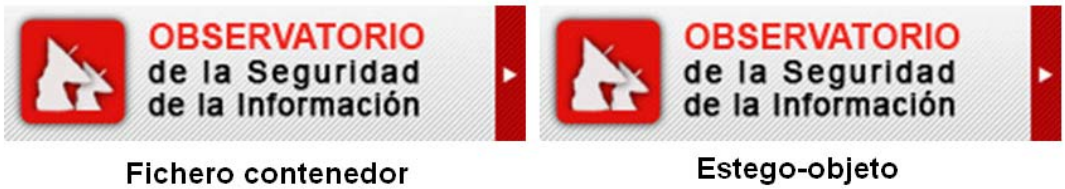
Ilustración 4: Efecto visual de la modificación de los bits menos significativos de las componentes RGB de un píxel

Fuente: INTECO

Se ha aumentado en una unidad cada componente RGB del píxel y el efecto es inapreciable para el ojo humano. De hecho, si se tiene en cuenta que un píxel esta rodeado por otros, el efecto visual si no se modifica su entorno pasa aun más inadvertido.

La implicación es que, utilizando cambios de un bit en cada componente de un píxel, se puede encajar tres bits de información oculta por píxel sin producir cambios notables en la imagen. Esto se puede hacer para cada píxel de una imagen. Se necesitan ocho píxeles para ocultar tres bytes de información, en codificación ASCII esto son 3 letras de información oculta. Así, en una imagen BMP de 502x126 píxeles se puede ocultar un mensaje de 23.719 caracteres ASCII.

Ilustración 5: Imagen en la que se ha ocultado información en los bits menos significativos de sus píxeles



Fichero contenedor

Estego-objeto

Fuente: INTECO

Para el caso de imágenes BMP la esteganografía por sustitución es bastante sencilla, la técnica se complica cuando se trata con otros formatos, pero la idea básica es la misma:

- Modificación de los índices que apuntan a la paleta de colores en un fichero GIF.
- Sustitución de coeficientes cuantificados DCTs en archivos JPG.

Esta técnica tiene un fallo latente de concepto: asume que la información almacenada originalmente en los bits menos significativos es aleatoria, con lo que su modificación para introducir información oculta no devela que la imagen está tratada. Esto no es cierto y puede servir como base para un mecanismo de estegoanálisis que se explica en el epígrafe IV.

Inserción de bits en el objeto contenedor

En este caso se añaden los bits de información a partir de una determinada marca estructural del fichero (fin de fichero o *EOF*, espacios de padding o alineamiento, etc.). Esta opción presenta el inconveniente de que sí se modifica el tamaño del objeto contenedor, con lo cual puede levantar sospechas.

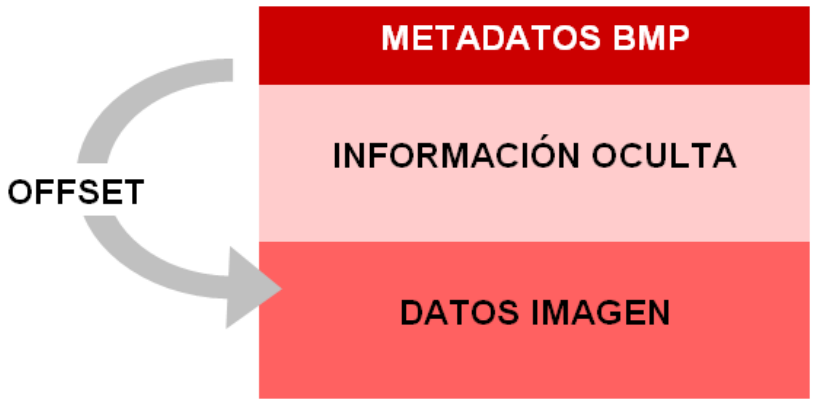
Para extrapolar esta idea al ejemplo de las imágenes BMP hay que comprender primero como se estructura dicho formato. Los primeros 54 bytes contienen los metadatos de la imagen, que se dividen de la siguiente manera:

- 2 bytes → contienen siempre la cadena 'BM', que revela que se trata de un BMP.
- 4 bytes → tamaño del archivo en bytes.
- 4 bytes → reservados (para usos futuros), contienen ceros.
- 4 bytes → offset, distancia entre cabecera y primer píxel de la imagen.
- 4 bytes → tamaño de los metadatos (esta estructura en sí).
- 4 bytes → ancho (número de píxeles horizontales).
- 4 bytes → alto (número de píxeles verticales).
- 2 bytes → número de planos de color.
- 2 bytes → profundidad de color.
- 4 bytes → tipo de compresión (vale cero, ya que BMP es un formato no comprimido).

- 4 bytes → tamaño de la estructura imagen.
- 4 bytes → píxeles por metro horizontal.
- 4 bytes → píxeles por metro vertical.
- 4 bytes → cantidad de colores usados.
- 4 bytes → cantidad de colores importantes.

Dada esta estructura, la forma trivial de ocultar datos consiste en ocultarlos justo después de los metadatos (entre los metadatos y los datos de la imagen en sí) y modificar el campo offset (distancia entre los metadatos y los píxeles de la imagen). De esta forma se puede dejar espacio para todo el contenido adicional que se desee albergar.

Ilustración 6: Esquema del resultado de esteganografía por inserción en imágenes BMP



Fuente: INTECO

La Ilustración 6 pone de manifiesto que esta técnica no es muy sigilosa. Si los datos a ocultar son considerablemente pesados (varios megabytes); es un tanto sospechoso tener un icono de 10x10 píxeles que ocupe 5 megabytes. Así, la persona encargada de ocultar la información debe repartirla sobre diferentes imágenes si desea que el cambio no sea tan notorio.

Creación de un objeto contenedor ad-hoc partiendo de la información a ocultar

Esta alternativa consiste simplemente en generar un fichero contenedor con la propia información a ocultar, en lugar de obtener el fichero contenedor por separado y manipularlo para incluir dicha información.

Por ejemplo, dado un algoritmo específico de reordenamiento de los bytes de los datos a ocultar se puede generar una secuencia de píxeles de un archivo BMP que tengan cierto

significado visual. Si el receptor conoce el algoritmo de reordenamiento, la transmisión de información es posible.

IV Estegoanálisis

Como ya se ha mencionado, el estegoanálisis es la técnica que se usa para recuperar mensajes ocultos o para impedir la comunicación por esteganografía. Existen dos tipos principales de estegoanálisis pasivo, que se explican brevemente a continuación.

Estegoanálisis manual

Consiste en buscar de forma manual diferencias entre el objeto contenedor y el estego-objeto buscando cambios en la estructura para localizar datos ocultos. Los principales inconvenientes de esta técnica son que es necesario tener el objeto contenedor y que en muchas ocasiones se detecta que un objeto contiene información oculta pero es imposible recuperarla.

No obstante, cuando no se dispone del fichero contenedor, se pueden buscar irregularidades en el fichero esteganografiado para tratar de encontrar signos de la existencia de datos ocultos.

Los ataques visuales alertan al ojo humano de la presencia de información oculta gracias a la aplicación de filtros. Considérese el caso del BMP donde el bit menos significativo de las componentes de algunos de sus píxeles ha sido sustituido por información oculta. En tal escenario el estegoanálisis manual consiste en aplicar un filtro tal que sólo se considere el bit menos significativo de cada componente RGB de cada píxel.

Esto es lo que se ha hecho en la Ilustración 7, la primera imagen oculta información y al aplicar el filtro salta a la vista un pequeño patrón uniforme en la parte superior de la imagen, además del cambio de tonalidad global con respecto a la imagen filtrada del fichero original.

Ilustración 7: Estegoanálisis manual de un BMP con información oculta mediante LSB

Fuente: INTECO

Estas diferencias se deben a que la ocultación de información en LSB parte de la premisa de que la información almacenada originalmente en dicho bit es aleatoria. Esto no es cierto y la ocultación de información en él proporciona pistas adicionales a un analista. Precisamente por esto, las imágenes con poca variabilidad de colores y/o regiones uniformes son malas candidatas para una técnica de esteganografía LSB. Una imagen robusta ante un ataque de este tipo es una imagen natural no artificial con mucha variación de tonos y/o colores.

Estegoanálisis estadístico

Consiste en el cotejo de la frecuencia de distribución de colores del estego-objeto. Es una técnica lenta para la que se debe emplear software especializado. Estos programas suelen buscar pautas para ocultar los mensajes que utilizan los programas más habituales de esteganografía, este enfoque los hace muy eficaces cuando se trata de mensajes ocultos con estos programas típicos. Ahora bien, los mensajes ocultados manualmente son casi imposibles de encontrar para estos programas.

Los detalles de las técnicas de estegoanálisis estadístico escapan al alcance de este artículo, se comenta brevemente sólo un mecanismo con el fin de ofrecer al lector una referencia básica.

Una de estas técnicas es el ataque Chi-Square[1] que permite estimar el tamaño de la posible información oculta en un estego-objeto. Es aplicable cuando un conjunto fijo de parejas de valores (PoVs) conmutan de un valor al otro de la pareja cuando se inserta los bits del mensaje oculto.

V Aplicaciones e implicaciones curiosas de la esteganografía

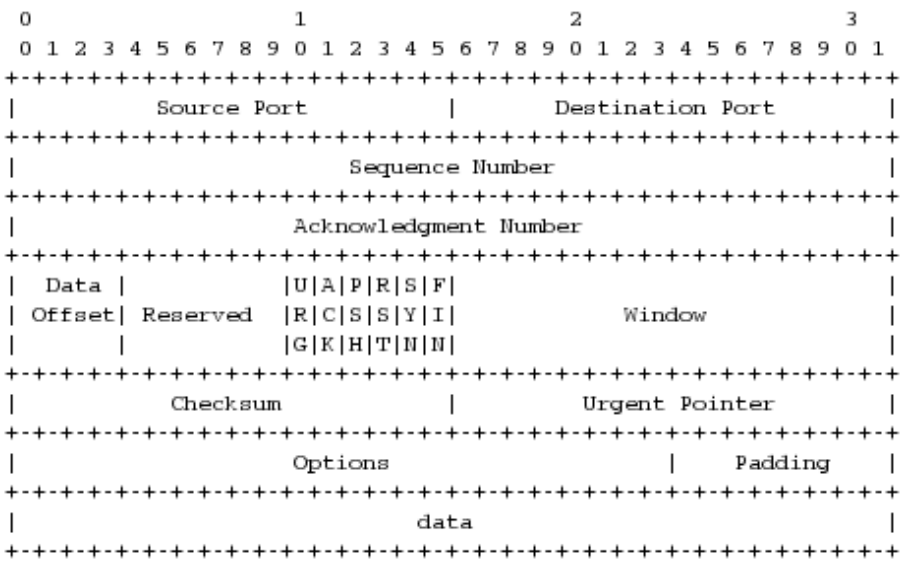
A continuación se señalan situaciones curiosas en las que se ha utilizado o podría utilizarse la esteganografía. No se trata de un listado exhaustivo, tan sólo se pretende ilustrar la aplicación práctica de la teoría ya expuesta.

Esteganografía empleando el protocolo TCP/IP

El protocolo TCP/IP es apropiado para crear canales encubiertos de comunicación ya que a través de las cabeceras se pueden enviar datos relevantes para dos entes que acuerdan un protocolo encubierto. Usando este enfoque es posible empotrar datos en peticiones de conexión iniciales, conexiones establecidas u otros pasos intermedios.

[1] Westfeld, A. Pfitzmann, A. Attacks on Steganographic Systems. http://www.ece.cmu.edu/~adrian/487-s06/westfeld-pfitzmann-ihw99.pdf

Ilustración 8: Cabecera del protocolo TCP



Fuente: RFC793 Transmission Control Protocol

Por ejemplo, considerando únicamente la cabecera TCP, se pueden ocultar datos en el número de secuencia inicial de una conexión. Esto ofrece 32 bits de datos ocultos por paquete de conexión inicial (SYN), es decir, 4 caracteres ASCII. Siguiendo esta filosofía se puede ocultar información en otros campos de las cabeceras de los distintos protocolos que componen TCP/IP, siempre y cuando los cambios no impliquen el rechazo de los paquetes intercambiados.

Control de malware

El malware de hoy día normalmente se comunica con un punto de control en posesión del atacante para recibir órdenes de descarga de módulos adicionales, para enviar datos robados, para indicar que una nueva víctima ha sido infectada, etc.

El protocolo más utilizado para este tipo de comunicación es HTTP ya que normalmente tiene lugar sobre un puerto que no está filtrado por los cortafuegos y porque puede pasar desapercibido en el resto de tráfico de red generado por la navegación legítima.

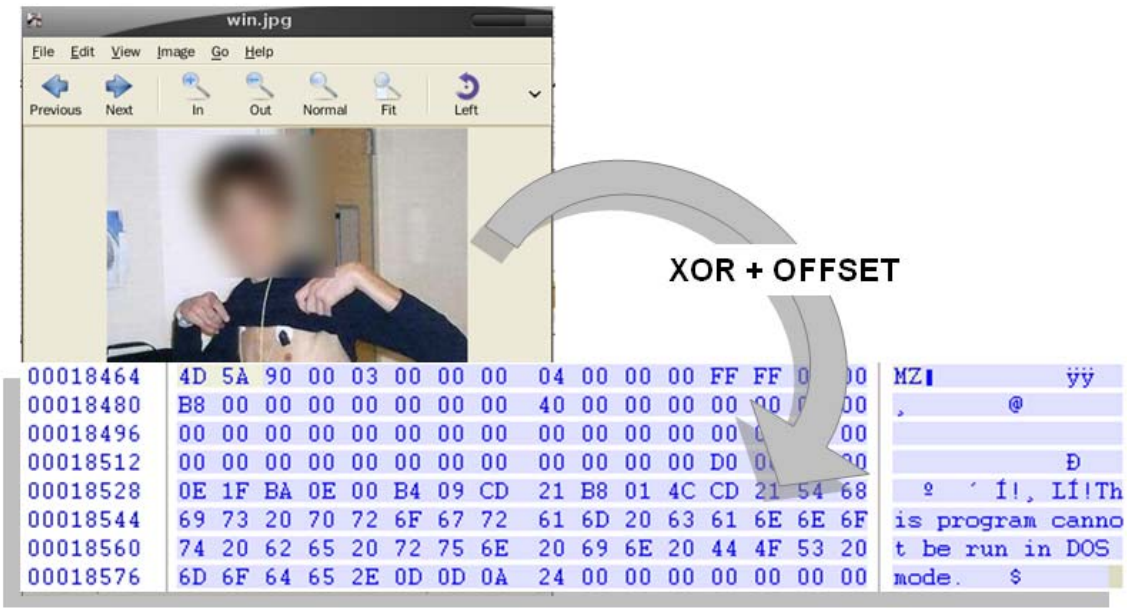
La facilidad de establecer un canal de control con peticiones HTTP GET/POST tradicionales también implica que la comunicación es fácilmente detectable (si no se emplean técnicas de cifrado) por las empresas que gestionan los servidores web/servidores de DNS asociados al enlace de control. Aun más fácil es la identificación e interpretación de dicha comunicación para un analista de malware. Esto significa que ante denuncia de actividad ilegal asociada a un determinado punto de control, las infraestructuras son cerradas más rápidamente por las empresas que las gestionan.

La consecuencia para el atacante es un tiempo de vida medio de su canal de control inferior, y por tanto un menor retorno de inversión.

Para que la identificación y el cierre de las infraestructuras asociadas a un troyano no sea tan trivial, los atacantes han ideado diversas técnicas: desde el simple codificado de las instrucciones para generar cadenas sin significado aparente hasta el uso de P2P.

En este afán por encubrir y fortalecer los canales de comunicación maliciosa, la esteganografía se erige como una baza muy interesante. De hecho, los creadores del gusano Waledac[2] ya han empleado esteganografía por inserción en la descarga e instalación de módulos adicionales que emplea el ejemplar malicioso.

Ilustración 9: Imagen con un ejecutable añadido usada por Waledac



Fuente: INTECO

Una de las funcionalidades de Waledac es la capacidad de descargar e interpretar un archivo de imagen JPEG especialmente manipulado. Dicho archivo es una imagen JPEG normal a la que se le ha añadido un ejecutable tras la imagen en sí, después de un determinado marcador JPEG para ser coherente con el estándar.

El ejecutable se cifra con una operación XOR simple de un byte. El resultado es una imagen que se puede visualizar en la mayoría de navegadores y visores pero que transporta código malicioso adicional para ser instalado por un equipo ya infectado por Waledac. Por ejemplo, se ha visto como Waledac emplea esta técnica para instalar una

[2] Más información en http://alerta-antivirus.inteco.es/virus/detalle_virus.html?cod=8426.

librería de captura de paquetes de red con el fin de registrar todas las claves de servicios FTP, HTTP, etc. que emplea la víctima.

La imagen de la Ilustración 9 estaba publicada en un servidor web. Convencer al administrador de la empresa que gestiona dicho servidor web de que se trata de código malicioso colgado intencionadamente por uno de sus clientes para usar en conjunto con otro malware no es tarea fácil. Esto significa que los tiempos de cierre de infraestructuras como ésta se disparan y los atacantes incrementan sus beneficios.

De forma similar, se pueden crear estego-objetos con órdenes para un troyano: atacar la subred 217.140.16.0/24, hacer clic en la publicidad de una determinada página, etc. y colgarlos en perfiles de redes sociales. Este troyano hipotético consultaría periódicamente el perfil en cuestión de la red social y procesaría las imágenes recientemente colgadas en busca de nuevas instrucciones. Si el perfil de la red social es creíble y las fotos parecen apuntar a que se trata de un individuo real, muy probablemente el departamento de abuso de la red social ignora cualquier petición de borrado del perfil. Es más razonable pensar que se trata de una denuncia por parte de algún conocido que quiere molestar al dueño del perfil causando su cierre, que creer que efectivamente forma parte de la infraestructura de un troyano.

Marcas de agua digitales

Una marca de agua digital es un código de identificación que se introduce directamente en el contenido de un archivo multimedia, normalmente para incluir información relativa a los derechos de autor o de propiedad del contenido digital en cuestión.

La presencia de esta marca de agua debe ser inapreciable para el sistema de percepción humano a la vez que fácilmente extraíble por una aplicación telemática que conozca el algoritmo para recuperarla.

Como consecuencia, en la actualidad se están empleando técnicas que en algunos casos pueden ser consideradas esteganografía para conseguir dicho propósito.

Las aplicaciones más comunes de las marcas de agua son:

- **Prueba de propiedad:** identificación de la fuente, el autor, el propietario, el distribuidor y/o el consumidor de un fichero digital.

- ***Fingerprinting*:** incluye los datos asociados a una transacción, datos del propietario de un fichero y de su comprador. Permite identificar al responsable de copias ilegales de contenido protegido por derechos de autor.

- **Clasificación de contenidos:** las marcas de agua se pueden emplear apara indicar el tipo de contenido de un fichero. Por ejemplo, en un mundo ideal las

páginas con contenido para adultos incluirían marcas de agua específicas en todas sus imágenes, vídeos y demás. Los programas de filtrado de contenidos las detectarían automáticamente de forma sencilla e impedirían su visualización a determinados públicos.

- **Restricción en el uso de contenidos:** empleadas en conjunción con aplicaciones o sistemas empotrados programados para tal fin, las marcas de agua pueden emplearse para impedir la visualización de ciertos contenidos cuando son copiados más de un determinado número de veces, a partir de una determinada fecha, etc.

En cualquier caso, una buena marca de agua debe resistir a cambios producidos en el fichero original, debe ser resistente a manipulaciones de la propia marca de agua, no debe ser humanamente perceptible, y debe tener un impacto mínimo sobre las propiedades estadísticas de su objeto contenedor. Dependiendo del uso que se vaya a hacer de la marca de agua también se puede señalar como propiedad deseada la facilidad para modificarla, por ejemplo para llevar la cuenta de cuántas veces se ha reproducido un determinado contenido.

Otras aplicaciones

De igual forma que el malware puede emplear la esteganografía para crear un canal de comunicación encubierta en redes sociales, también pueden hacerlo personas físicas. De hecho, según el diario USA Today[3] el FBI y la CIA descubrieron en su momento que Bin Laden empleaba imágenes esteganografiadas colgadas en páginas web públicas para comunicarse con sus oficiales.

Otro uso poco ético que se ha hecho de la esteganografía es la fuga de información en entornos corporativos, militares, gubernamentales, etc. En sitios donde se inspecciona el contenido que un empleado extrae del entorno en medios digitales, la esteganografía se puede emplear para portar esquemas, documentos, y demás información delicada sin levantar las sospechas del revisor.

Pero no todas las aplicaciones de la esteganografía tienen que ser maliciosas. Por ejemplo, se puede usar para empotrar información de pacientes en radiografías, TACs y similares. También se puede emplear para clasificación de contenidos multimedia o ser integrada en mecanismos de autenticación.

[3] http://www.usatoday.com/tech/news/2001-02-05-binladen.htm

VI Conclusiones

La esteganografía es una técnica en constante evolución, con una larga historia y con capacidad para adaptarse a nuevas tecnologías. A medida que las herramientas de esteganografía se hacen más avanzadas, las técnicas y las herramientas empleadas en el estegoanálisis también se hacen más complejas.

Los ficheros contenedores no tienen que ser forzosamente imágenes, cualquier medio es válido (audio, video, ejecutables, etc.). Lejos de ser un ingenio exclusivamente teórico, el malware ha demostrado hacer un uso activo de la esteganografía, y se espera que surjan nuevos enfoques de uso para dificultar la labor de los analistas.

Pero las aplicaciones de esta ciencia no sólo se restringen al ámbito de lo poco ético, pudiendo ayudar en campos como la medicina, protección de menores, etc.

En cualquier caso, la eficiencia de las nuevas técnicas de estegoanálisis hace necesario el uso de la esteganografía combinada con criptografía con el fin de alcanzar un nivel de seguridad razonable. La criptografía garantiza la confidencialidad de una conversación pero no esconde el hecho de que dicha conversación se está manteniendo. Por otra parte, la esteganografía en solitario puede ocultar el hecho de que una conversación se mantiene, pero una vez descubierta la interacción, es posible que un atacante conozca el contenido intercambiado. Aun cuando descubrir el contenido original fuera difícil, un atacante puede modificar el estego-objeto para impedir la comunicación (ataque activo). Conjugando ambas técnicas se alcanza una complementariedad que multiplica la seguridad de un intercambio de mensajes.