DAVID MEGÍAS

LOS SECRETOS QUE OCULTA LA RED

Esteganografía y cibercrimen: ¿hay motivos para la alarma?

La digitalización y las herramientas de la Red ponen a disposición de casi cualquier individuo la posibilidad de enviar, gracias a la esteganografía, mensajes ocultos a un destinatario sin que ni siquiera sepamos que se está produciendo dicha comunicación. Por desgracia, delincuentes y terroristas ya están usando estas técnicas para sus fines. ¿Hay motivos para la alarma? ¿Estamos indefensos?

The secrets that Internet hides

STEGANOGRAPHY AND CYBERCRIME: ARE THERE REASONS FOR CONCERN?

The digitization and the tools provided by Internet make available to almost any individual the possibility of sending, thanks to steganography, hidden messages to a recipient without even noticing that this communication is taking place. Unfortunately, criminals and terrorists are already using these techniques for their purposes. Are there reasons for concern? Are we defenseless?

Keywords: *steganography, privacy, cybersecurity, cybercrime, terrorism, virus, malwaree*

Palabras clave:
esteganografía, privacidad, ciberseguridad, ciberdelincuencia, terrorismo, virus, *malware*.

ILUSTRACIÓN: **DAQ**

El envío de mensajes ocultos, que no puedan ser descubiertos aunque se intercepten o espíen las comunicaciones, es una cuestión que ha ocupado a la humanidad desde la antigüedad. Ya en el siglo V a.C., el historiador griego Heródoto[1] relataba cómo el general ateniense Histieo, mientras planeaba la revuelta jónica, afeitó la cabeza de su esclavo más fiel, le tatuó un mensaje y esperó a que le creciese nuevamente el cabello antes de enviarlo a Aristágoras, el tirano de Mileto. A la llegada del esclavo, Aristágoras, conocedor de la existencia del mensaje, le afeitó la cabeza y leyó el tatuaje oculto que le instaba a iniciar la revuelta contra los persas.

Este es uno de los primeros casos conocidos de esteganografía[2, 3], palabra derivada del griego *steganos* (cubierto u oculto) y *graphos* (escritura), que se usa para definir el conjunto de técnicas destinadas al envío de mensajes ocultos, incrustados en elementos aparentemente inocuos, de forma que el mensaje pueda pasar completamente desapercibido para quien no conozca su existencia.

A diferencia de la criptografía, que consiste en el envío de información cifrada para que esta no resulte inteligible a una tercera parte no autorizada, la esteganografía va un paso más allá y pretende ocultar incluso que la propia comunicación se esté produciendo. Estas técnicas se desarrollaron inicialmente para aplicaciones militares o de espionaje, como parece lógico, pero no debemos obviar los usos civiles que han ido apareciendo a lo largo de los años para proteger secretos que queremos mantener a buen recaudo, sin levantar sospechas sobre su existencia.

En las últimas tres décadas, con la llegada de la digitalización asociada a las tecnologías de la información y de la comunicación, las posibilidades de la esteganografía se han multiplicado exponencialmente. Los contenidos multimedia digitales, tales como las imágenes, los vídeos o los archivos de audio, rápidamente se identificaron como portadores ideales para ocultar mensajes secretos que pudiesen pasar inadvertidos a los ojos de curiosos. Y no solo se usan contenidos multimedia como portadores de mensajes ocultos, sino que también los archivos de texto, el código fuente de *software* o los propios protocolos de Internet permiten crear canales esteganográficos encubiertos para establecer comunicaciones privadas sin que nadie repare en ello.

Sin embargo, los contenidos multimedia, por el elevado volumen de información que poseen, por su ubicuidad en toda la Red y por ser un tipo de archivos que pueden intercambiarse libremente entre usuarios sin despertar sospecha alguna, son el medio preferido para este tipo de aplicaciones. ¿Quién podría sospechar que las inocentes fotos de las vacaciones que alguien ha publicado en su cuenta de Instagram ocultan, en realidad, información clasificada que se está haciendo llegar de forma encubierta a un destinatario de un país lejano?

Más allá de las aplicaciones militares o de inteligencia, las técnicas esteganográficas permiten otros usos más o menos obvios. Por un lado, los disidentes en regímenes autoritarios donde se practica la censura o la persecución política, pueden usar la esteganografía para establecer comunicaciones encubiertas, evitando así el escrutinio de las autoridades. Por otro lado, con fines menos loables, la esteganografía se relaciona también con usos criminales o, incluso, terroristas[4]. Comunicarse cuando se está sometido a una estrecha vigilancia es un reto muy complicado. Las autoridades tienen recursos y herramientas legales a su alcance para intervenir las comunicaciones, ya sean telefónicas, postales o telemáticas. Cuando un grupo de delincuentes o de terroristas sabe que los vigilan de cerca, la esteganografía se les presenta como una alternativa muy apetecible para proteger sus comunicaciones más delicadas.

Entonces, ¿hay motivos para la alarma? Es francamente difícil contestar a esta pregunta. Cuando un grupo de individuos –delictivo o no– quiere comunicarse de manera encubierta, si lo hace bien, lo más probable es que dichas comunicaciones nunca se descubran. Por la propia definición de esteganografía, es casi imposible saber hasta qué punto los criminales y los terroristas están utilizando estas herramientas. No obstante, sabemos que esto ya ha ocurrido en varias ocasiones.

Un caso relativamente reciente de este uso se registró en Berlín, en mayo de 2011, cuando un sospechoso de pertenecer a la banda terrorista Al Qaeda fue detenido por las autoridades alemanas[5]. Al presunto terrorista se le incautó una tarjeta de memoria que contenía una carpeta protegida mediante contraseña. La policía científica alemana consiguió acceder a los contenidos de la carpeta y, para su sorpresa, solo hallaron en ella un vídeo con material pornográfico. Que tal archivo estuviese protegido por contraseña despertó las sospechas de las autoridades, que decidieron analizarlo con mayor detalle. De ese vídeo se extrajeron 141 archivos de texto ocultos que contenían información relevante sobre las operaciones de Al Qaeda y sus planes de futuro, bajo títulos tan inequívocos como "Trabajos futuros", "Lecciones aprendidas" e "Informe de operaciones".

La lista de amenazas conocidas no termina ahí. Al margen de los grupos de criminales o terroristas que usan la esteganografía como canal de comunicación encubierto también existen colectivos de ciberdelincuentes para los que estas herramientas son el mecanismo perfecto a través del cual desplegar sus ataques. Entre 2011 y 2017 hay constancia de al menos catorce casos de *malware* (*software* malicioso) que han usado la esteganografía como herramienta infecciosa[6]. En este caso, la esteganografía se utiliza en varios momentos del ataque: en primer lugar, cuando se está examinando al objetivo del ataque, para ocultar el escanea- ➠

La esteganografía va más allá que la criptografía y pretende ocultar que la propia comunicación se está produciendo

1 **Kahn, D.** (1996): "The History of Steganography" en *Proceedings of the First International Workshop on Information Hiding*, de Ross J. Anderson (Ed.). Londres, Springer-Verlag, pág. 1-5.

2 **Cox, I.**, Miller, M., Bloom, J., Fridrich, J., y Kalker, T. (2007): *Digital Watermarking and Steganography* (2 ed.). San Francisco, Morgan Kaufmann Publishers Inc.

3 **Serra, J. y Lerch, D.** (2014). *Esteganografía y estegoanálisis*. 2014. Móstoles (Madrid), 0xWord.

4 **Zielinska, E.; Mazurczyk, W.; y Szczypiorski, K.** (2014): "Trends in steganography" en *Communications of the ACM*, vol. 57, núm. 3, pág. 86-95.

5 **Gallagher, S.** (2012): "Steganography: how al-Qaeda hid secret documents in a porn video", disponible en: https://arstechnica.com/information-technology/2012/05/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video/

6 **Cabaj, K.; Caviglione, L.; Mazurczyk, W.; Wendzel, S.; Woodward, A.; y Zander, S.** (2018): "The New Threats of Information Hiding: The Road Ahead" en *IT Professional*, vol. 20, núm. 3, pág. 31-39.

Los expertos en ciberseguridad y en técnicas forenses trabajamos para combatir las amenazas, para hacer de la Red un lugar algo menos salvaje

contenidos digitales como portadores de la información. La técnica más habitual consiste en usar imágenes digitales para ocultar las configuraciones del *software* malicioso, para proporcionar una dirección de Internet desde la cual descargar componentes adicionales o, incluso, para ocultar directamente el código malicioso. Tampoco el secuestro de datos o *ransomware* ha quedado fuera de esta oleada y ya se han registrado varias infecciones que han utilizado imágenes o canales encubiertos en los protocolos de Internet para transmitir componentes del software de secuestro de datos, facilitando así la infección y dificultando la acción de las aplicaciones *antimalware* que detectan o bloquean este tipo de ataques.

En resumidas cuentas, parece que la tendencia al uso de la esteganografía, tanto para comunicaciones de grupos de delincuentes y terroristas como en el caso de la ciberdelincuencia para la propagación de infecciones de *malware* y *ransomware*, es algo que sí que debe de preocuparnos e instarnos a tomar las contramedidas oportunas.

¿Estamos, pues, indefensos? Por fortuna, no. La comunidad científica lleva décadas investigando las tecnologías de ocultación de la información y, entre ellas, la esteganografía. Quiere decir que ya se han desarrollado herramientas forenses que permiten, tanto a las autoridades como a los expertos en ciberseguridad de organizaciones y empresas, proteger sus sistemas y comunicaciones frente a este tipo de amenazas. Investigadores de todo el mundo centran su actividad en el desarrollo de nuevas técnicas de esteganografía y de sistemas de detección de anomalías que pueden usarse para discriminar si un objeto digital es solo lo que parece o, por el contrario, debe examinarse a fondo para determinar si contiene información oculta. Estas últimas técnicas se denominan estegoanálisis y constituyen la otra cara de la moneda de la esteganografía.

Igual que para la criptografía existe el criptoanálisis, que trata de romper los sistemas criptográficos para descifrar la información secreta, en el ámbito de la esteganografía, el estegonálisis consiste en analizar computacionalmente unos contenidos sospechosos para determinar si presentan algún tipo de desviación estadística respecto a sus análogos inocuos. En caso de hallar alguna anomalía, se analizará si ésta concuerda con alguna técnica esteganográfica concreta. Como es de suponer, el aprendizaje automático es, en estos momentos, uno de los mejores aliados para los estegoanalistas.

Nos hallamos, pues, inmersos en una suerte de "carrera armamentística" entre la esteganografía y el estegonálisis, a la que podemos aplicar una sencilla analogía con los sistemas vivos. Igual que la naturaleza ha dotado a los organismos de un sistema inmunológico para combatir las infecciones biológicas, los expertos en ciberseguridad y en técnicas forenses trabajamos para combatir las amenazas que se valen de la esteganografía, creando nuevas soluciones de estegoanálisis y poniéndolas a disposición de las autoridades y de la sociedad para hacer de la Red un lugar algo menos salvaje.

A causa de la emergencia de estas amenazas, un conjunto de expertos de la comunidad científica, de las fuerzas de seguridad y de diferentes empresas y organizaciones de toda Europa, hemos impulsado la creación del grupo *Criminal Use of Information Hiding*[7] (CUING, Uso Criminal de la Ocultación de la Información) en colaboración con el *European Cybercrime Centre* (EC3) de la Europol.

Las actividades del grupo CUING se centran en crear conciencia sobre los usos maliciosos de estas técnicas, realizar un seguimiento del progreso del uso de estas tecnologías con fines delictivos, compartir inteligencia estratégica sobre las nuevas amenazas, trabajar conjuntamente para combatir estas amenazas, y educar y capacitar a los nuevos profesionales que se van a tener que enfrentar a este tipo de retos, tanto desde las autoridades como desde las organizaciones y empresas. Nuestra labor en este grupo, por lo tanto, sería comparable a la acción del sistema inmunológico de los seres vivos, realizando tareas constantes de vigilancia y supervisión, y ayudando a las autoridades y a los expertos en ciberseguridad a combatir los ataques en que los ciberdelincuentes intentan aprovechar las vulnerabilidades de los sistemas y las nuevas oportunidades que les brindan las técnicas de ocultación de la información.

do; en segundo lugar, para obtener un acceso no autorizado, ocultando el proceso de infección o disfrazando aplicaciones maliciosas como inocentes; finalmente, también se está usando para mantener en el tiempo un acceso no autorizado, ocultando el tráfico de datos y extrayendo, de manera encubierta, información del dispositivo afectado. A diferencia de la criptografía, que no oculta las comunicaciones, la esteganografía sí que lo hace, por lo que puede ser muy difícil, si no imposible, detectar este tipo de intrusiones con las herramientas de seguridad estándar.

En la actualidad, el *malware* que usa esteganografía a menudo se vale de

7 http://cuing.org/

Bibliografía

Cox, I.; Miller, M.; Bloom, J.; Fridrich, J.; y Kalker, T. (2007): *Digital Watermarking and Steganography* (2 ed.). San Francisco, Morgan Kaufmann Publishers Inc.

Kahn, D. (1996): "The History of Steganography" en Proceedings of the First International Workshop on Information Hiding, de Ross J. Anderson (Ed.). Londres, Springer-Verlag, páginas 1-5.

Serra, J. y Lerch, D. (2014). *Esteganografía y estegoanálisis*. 2014. Madrid, 0xWord.

Zielinska, E.; Mazurczyk, W.; y Szczypiorski, K. (2014): "Trends in steganography" en Communications of the ACM, vol. 57, núm. 3, páginas 86-95.