

Ciberdelincuencia: principales amenazas y medidas preventivas



DERECHOS DE USO

La presente documentación es propiedad de la Superintendencia de Servicios de Certificación Electrónica SUSCERTE, tiene carácter privado y confidencial y está dirigido exclusivamente a su(s) destinatario(s), no podrá ser objeto de reproducción total o parcial, ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, digital, registro o cualquier otro, no podrá ser distribuido sin el permiso previo y escrito de SUSCERTE, bajo ningún concepto. Si usted ha recibido este mensaje por error, debe evitar realizar cualquier acción descrita anteriormente, asimismo le agradecemos comunicarlo al remitente y borrar el mensaje y cualquier documento adjunto. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será sancionada conforme a la ley.



Ciberdelincuencia: principales amenazas y medidas preventivas

El ciberdelincuencia, neologismo para describir los ataques de delincuentes vinculados al empleo de las nuevas tecnologías e Internet, ha aumentado exponencialmente en el último año, llegando a afectar a más de 400 millones de personas procedentes de más de 20 países distintos¹. El coste en tiempo invertido para solucionar el problema, considerado por el 40% de las víctimas como la mayor molestia, es de 10 días promedio.

La seguridad telemática es, pues, una cuestión que en poco tiempo ha dejado de ser patrimonio exclusivo de un sector profesional concreto, pasando a formar parte de la realidad diaria y transversal no sólo de la Administración Pública Nacional, sino también de organizaciones privadas y usuarios individuales. Principalmente, en un momento en que buena parte de la población accede constantemente a páginas web, utilizan el correo electrónico para todo tipo de comunicaciones, acumulan información personal en redes sociales y en dispositivos móviles.

Todo ello les convierte en un blanco cada vez más fácil para los ciberdelincuentes, cuyo objetivo final puede estar vinculado a una gran variedad de delitos: captación de información confidencial para múltiples fines (estafas, robos, chantajes, acoso, pornografía infantil), sabotaje, ataques terroristas que atenten contra el funcionamiento de las infraestructuras públicas (también las infraestructuras críticas), propaganda, delitos contra el honor, la intimidad y el derecho a la propia imagen, entre otros.

Los ciberdelincuentes utilizan numerosas técnicas para realizar este tipo de delitos, como el phishing, el envío de spam, los ataques de inyección SQL o los ataques distribuidos de denegación de servicio (DDoS). Éstos últimos se organizan a menudo, a partir de botnets, esto es, redes de computadoras parasitadas y controladas remotamente por el ciberdelincuente para que éste pueda, llegado el momento, lanzar un ataque masivo y coordinado para sabotear a un objetivo concreto.

El riesgo creciente de las redes sociales

Las redes sociales son una puerta de acceso relativamente fácil a datos personales. Uno de cada cinco usuarios admite acceder a todos los enlaces que aparecen en sus cuentas de redes sociales², lo que representa un gran riesgo debido a que estos suelen presentarse acortados (ej. <http://bit.ly/n3Vjl1>) y, por tanto, las posibles amenazas son de muy difícil detección, manteniéndose camuflajeadas. Al hacer click en un enlace dañino, la viralidad intrínseca de la propia red social y la confianza depositada en los contenidos recomendados por otros contactos hace el trabajo, consolidando así la propagación eficaz del malware.

A partir de esto, el ciberdelincuente puede utilizar los datos personales de un usuario para distintos objetivos, como por ejemplo la venta de información de perfiles personales en el *mercado negro*, que ofrece miles de direcciones de correo electrónico a los remitentes de

¹ Informe Norton de Ciberdelincuencia (Septiembre de 2011)

² Estudio G Data "¿Cómo perciben los usuarios los peligros de Internet?"
http://hu.gdatasoftware.com/uploads/media/GData_SecuritySurvey_2011_EN_03.pdf



spam. En algunos casos, el estudio minucioso de perfiles públicos de profesionales que ocupan cargos elevados en sus organizaciones permite a los ciberdelincuentes construir una estrategia convincente de *phishing*, cuyo objetivo es obtener información personal sensible de otro usuario para poder acceder a sus cuentas bancarias.

El *phishing* basa su estrategia en la mimetización de páginas web oficiales. De una apariencia asombrosa, la única diferencia apreciable entre las webs oficiales y las imitadas estriba en la url, que suele diferir por una sola letra. El tamaño reducido de la barra del navegador, de ardua lectura, y la capacidad del ojo humano de armonizar o corregir las frases erróneas, asimilándolas a su versión correcta, contribuye a que el usuario no detecte el engaño.

El *phishing* puede servir, en este caso, para acceder también a información sensible de la organización a la que pertenece un alto cargo. Sabotear el funcionamiento de una infraestructura sensible, atentar contra la propiedad intelectual asociada a un producto empresarial o conocer información secreta son algunas de las motivaciones que inducen a los hackers a actuar en esta línea.

Existe un punto, pues, en el que individuo y organización entrelazan su identidad en Internet a través de los perfiles personales en las redes sociales. A título individual, es importante activar los niveles de privacidad más elevados en las cuentas de usuario de los medios sociales, no publicar información sensible y no establecer contacto con personas que no se conocen. A nivel de organización, es recomendable establecer una política de uso de las redes sociales para sus trabajadores, que debe fundamentalmente contemplar dos aspectos: qué tipo de información sobre la organización se permite difundir a los trabajadores en sus perfiles sociales, por un lado, y a qué sitios y redes sociales se permite acceder desde los terminales de la organización o utilizando sus redes inalámbricas.

Los ataques a celulares se duplican en 2011

De hecho, las redes inalámbricas y los celulares, con y sin conexión a Internet, constituyen una de las amenazas actuales más importantes en el campo de la seguridad de la información. La percepción de riesgo del usuario disminuye cuando navega a través del terminal telefónico, una realidad que incrementa aún más las posibilidades de recibir un ciberataque. Conectarse a redes inalámbricas –el 25% de ellas son muy vulnerables a los ataques³– entraña el peligro de que un tercero pueda acceder a toda la información almacenada en un celular, especialmente si se trata de redes abiertas. En este sentido, cada día aumentan los ataques de código dañino que hacen blanco en los teléfonos, acción que se duplicó en 2011⁴. Los desarrolladores de software malicioso han encontrado en los celulares una vía fértil para propagar rápida y eficazmente sus amenazas, que pueden ocultarse por ejemplo, bajo servicios exclusivos de mensajes de texto o en aplicaciones de juegos.

³ Estudio elaborado por Bitdefender (Noviembre 2010-Setiembre 2011) <http://www.malwarecity.com/blog/25-percent-of-wireless-networks-are-highly-vulnerable-to-hacking-attacks-wi-fi-security-survey-reveals-1174.html>

⁴ Informe X-Force de Tendencias y Riesgos de Mitad de Año 2011 <http://public.dhe.ibm.com/common/ssi/ecm/en/wge03015usen/WGE03015USEN.PDF>



Si bien las redes sociales y los celulares son algunos de las amenazas más recientes de la ciberdelincuencia, existen técnicas de ataque tradicionales, conocidas y catalogadas desde hace mucho tiempo, que siguen causando estragos. Es el caso de la inyección SQL, utilizada por grupos “hactivistas”, cuya finalidad es por lo general sabotear los sitios web oficiales de grandes empresas y gobiernos, entre otros. Y la inyección SQL, que está orientada al acceso a bases de datos, utiliza los formularios que los usuarios suelen rellenar en Internet. Al no estar muchos de ellos cifrados, el “hactivista” aprovecha esta puerta de entrada para obtener miles de datos confidenciales almacenados en las bases de datos, donde van a parar las credenciales que el usuario introdujo en el formulario.

La necesidad de cifrar la información

¿Qué opciones existen para que un formulario de datos disfrute de una seguridad informática robusta? El cifrado de la información es la respuesta. Los datos introducidos por el usuario en el formulario deben estar a la ampara de un código cifrado, cuya fuerza estriba en el carácter público del algoritmo que la sustenta, a menudo basado éste en fórmulas matemáticas que la comunidad conoce y acepta como robustas. De este modo, el nivel de seguridad no se mide por el anonimato de las contraseñas utilizadas sino más bien por la complejidad de la fórmula o algoritmo que permite la creación de la contraseña en sí.

Por otro lado, el ataque de aplicaciones web sigue en aumento, atentando contra sitios web que disfrutaban de credibilidad. Los usuarios navegan y acceden a estos sitios con total confianza, desconociendo que estas páginas han dejado de ser seguras. Al contrario, en muchas ocasiones se han convertido en servidores malignos al servicio de los ataques que se ejecutan en el ordenador del cliente al interactuar éste con el sitio web.

Un buen ejemplo de este tipo de amenazas se encuentra en las webs pornográficas, que representan un 12% del total de webs existentes en la actualidad⁵. Para este caso concreto, los hackers están utilizando la técnica del posicionamiento mediante palabras claves de búsqueda en Internet. A partir del estudio de los portales pornográficos más visitados, los ciberdelincuentes intentan diseminar su código dañino a través de las aplicaciones multimedia imprescindibles para visualizar los contenidos de este tipo de páginas.

Algo similar sucede con las aplicaciones más populares, como Acrobat Reader, Microsoft Office y Apple Quick Time, por ejemplo. Los hackers estudian las vulnerabilidades de los programas que gestionan estas aplicaciones e intentan acceder a los terminales a través de archivos concretos. Por esta razón es importante descargar las últimas versiones actualizadas de las aplicaciones. A nivel de organización, es fundamental disponer de una política de actualización de aplicaciones y seguirla escrupulosamente.

Finalmente, también cabe hablar de un aumento de la actividad de los ataques mediante *botnet*, una estrategia por la cual los hackers se adueñan de la computadora de un tercero vía control remoto. Llegado el momento, el ciberdelincuente utilizará la red de computadoras parasitadas para lanzar algún tipo de ataque y conseguir que éste alcance

⁵ Informe Norton de Cibercrimen (septiembre de 2011)
http://es.norton.com/content/es/es/home_homeoffice/html/cybercrimereport/



gran propagación, quedando el ciberdelincuente y su identidad totalmente en el anonimato y comprometiendo, en cambio, la IP de los ordenadores utilizados.

Medidas preventivas y formación

Las vulnerabilidades en los software y los hardware requieren soluciones técnicas específicas, algunas de las cuales se han apuntado tímidamente en este artículo. Sin embargo, muchos de los riesgos de ciberataques, especialmente aquellos que conciernen al uso individual de Internet, están relacionados con la falta de medidas protectoras higiénicas. Y es que el 41% de los usuarios, por ejemplo, admiten no disponer de ningún antivirus⁶. Aunque parezca insólito, los consejos más básicos, a parte de la imperiosa necesidad de disponer de un paquete de software de seguridad actualizado, pueden ayudar a la mayoría de usuarios a evitar las amenazas más comunes. En este sentido, construir contraseñas robustas (más de 8 caracteres, combinación de mayúsculas y minúsculas, alfanuméricas y nunca basadas en palabras del diccionario), cambiarlas periódicamente, no acceder a redes inalámbricas desprotegidas, actualizar periódicamente los programas y mantener una actitud vigilante al navegar por Internet y al interactuar en las redes sociales, son algunas de las recomendaciones que, por simples que puedan parecer, siguen siendo cruciales.

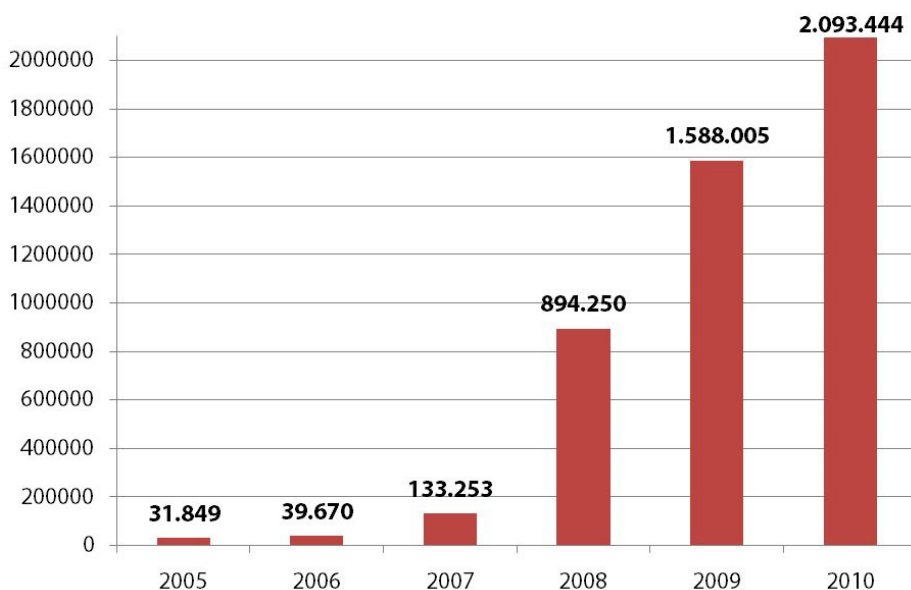
La importancia de la formación

A este respecto, la formación en seguridad de la información debe tener un papel fundamental a la hora de concienciar a la población sobre las buenas prácticas y la navegación segura en Internet. Los usuarios son conscientes de que existen peligros, es cierto, pero todavía prevalecen algunos tópicos sobre estos peligros, que contribuyen a aumentar en gran medida el riesgo de propagación de ciberataques. El código dañino es un buen ejemplo para ilustrar este fenómeno, pues en los últimos años su presencia ha aumentado exponencialmente, tal y como se aprecia en la gráfica. Según los datos⁷, 9 de cada 10 usuarios creen que el comportamiento de su computadora se verá afectado de algún modo u otro si ésta es objeto de un ataque vía código dañino. Esta concepción, totalmente errónea, crea una falsa ilusión de seguridad en muchísimos usuarios cuya computadora, sin saberlo ellos, sí está infectada por un malware.

⁶ Informe Norton de Ciberdelincuencia (septiembre de 2011)
http://es.norton.com/content/es/es/home_homeoffice/html/cybercrimereport/

⁷ Estudio G Data “¿Cómo perciben los usuarios los peligros de Internet?”
http://hu.gdatasoftware.com/uploads/media/GData_SecuritySurvey_2011_EN_03.pdf





Fuente: Estudio G Data

En poco tiempo, la red ha dejado de ser un medio aislado, donde pasan cosas que sólo tienen consecuencias intra muros. Todo lo contrario, actualmente cualquier amenaza en la red tiene un impacto y una repercusión palpable, que atentan contra la seguridad y los derechos de las personas y las organizaciones. Por esta razón, conocer los riesgos y atajarlos es una responsabilidad colectiva.

