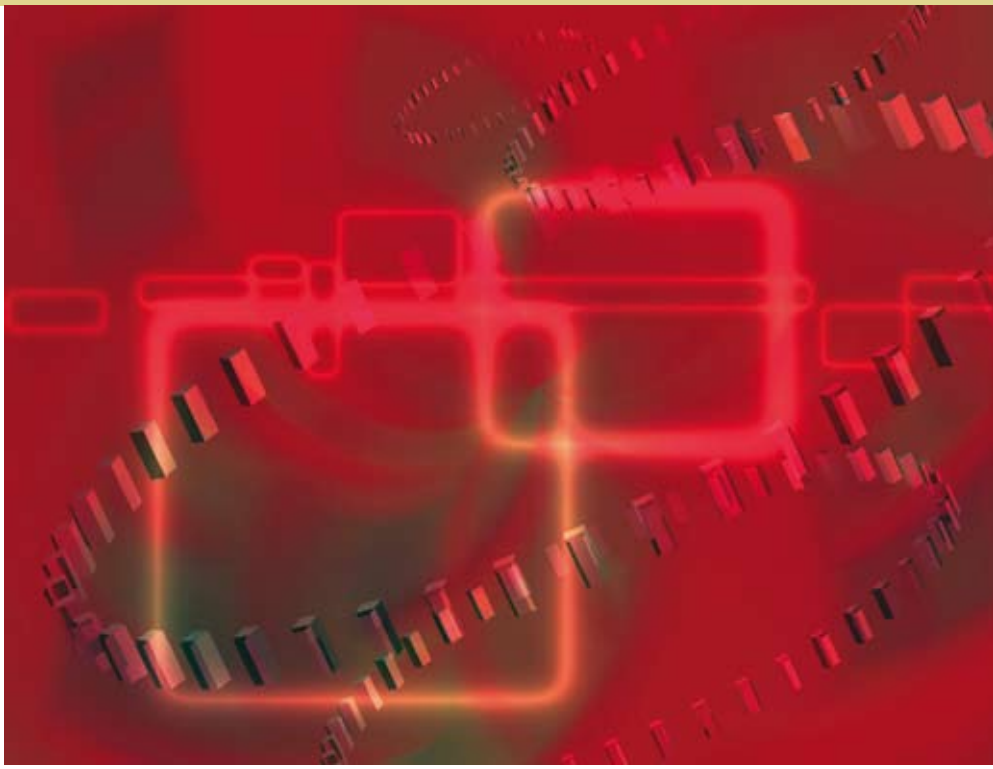
Ciberataques a las redes sociales

Las amenazas también han empezado a introducirse en las redes profesionales

LA POPULARIDAD ADQUIRIDA POR LAS REDES SOCIALES ENTRE CIENTOS DE MILLONES DE USUARIOS DE TODO EL MUNDO LAS HA CONVERTIDO EN UNA HERRAMIENTA EFICAZ UTILIZADA POR LOS 'HACKERS' PARA LANZAR SUS ATAQUES, CON EL OBJETIVO DE CONSEGUIR EL MAYOR NÚMERO DE DATOS PERSONALES Y PERFILES DE LOS MIEMBROS



Tx: Gema Tapia.
Ft: Getty Images.

Las redes sociales pueden servir como herramienta para mantener el contacto con conocidos, intercambiar impresiones e, incluso, establecer nuevas relaciones. Sin embargo, el éxito que estas redes están teniendo entre los usuarios de la Web 2.0 las ha convertido en un objetivo prioritario entre los ciberdelincuentes, especialmente en los casos de Facebook y Twitter, dos de las preferidas de los internautas, debido al elevado número de miembros con los que cuentan en todo el mundo.

Una de las redes más perjudicadas por estos ataques es Twitter, atacada por primera vez a principios de 2009. En esa ocasión, la compañía de seguridad Shopos registró un envío masivo de *phishing* en el que miles de usuarios recibieron mensajes directos de amigos invitándoles a visitar una web. Como señuelo, se ofrecía lo posibilidad de ganar premios, ver fotos divertidas o noticias de actualidad. Si el usuario pinchaba en el *link*, era dirigido a una falsa página de Twitter desde la que se podía robar información del usuario, como el nombre y la contraseña.

Otro de los ataques producidos en este sitio consistió en una avalancha de secuestros de cuentas, mediante los que, según Trend Micro, en sólo dos horas se vieron comprometidas más de 750 cuentas. En esta ocasión, se animaba a los internautas a entablar amistad a través de *webcam* con una mujer de 23 años. Sin embargo, el *link* dirigía a un portal de contenidos pornográficos diseñado con el fin de recoger números de tarjeta de crédito. En caso de "clickear" sobre este enlace, Trend Micro recomendaba cambiar inmediatamente la contraseña.

Además de este ataque, en este sitio web también se registró una suplantación masiva de 33 cuentas de personajes famosos, entre los que se encuentran el mismísimo Barack Obama o la cantante Britney Spears. Gracias a las cuentas pirateadas o suplantadas, los *hackers* utilizan estas identidades comprometidas para enviar mensajes de *spam* a otros miembros de la red.

Mantener la protección del equipo actualizada, desconfiar de mensajes de procedencia desconocida y utilizar contraseñas que combinen números y letras son sencillos consejos que ayudan a evitar la infección

Uno de los ataques más reciente en Twitter ha consisitido en la creación de cientos de cuentas y la publicación en todas ellas de miles de comentarios sobre el tema "*PishTube Broadcast*", relacionado con una banda de rock estadounidense. A través de este sistema, detectado por PandaLabs, los ciberdelincuentes conseguían que ese tema apareciera en la lista de los más comentados (*trending topic*), con lo que lograron una visibilidad y un mayor tráfico de usuarios hacia sus comentarios. Entre los comentarios publicados, se encontraban enlaces que redirigían a una falsa página de contenido pornográfico y si el usuario pinchaba sobre ellos, se infectaba con el falso antivirus PrivacyCenter, que pretendía hacer creer al usuario que su equipo estaba infectado y le ofrecía la posibilidad de eliminar ese *malware* mediante la compra de la versión Premium del falso antivirus. El objetivo de este ataque era, principalmente, obtener dinero.

Ataques similares se han registrado en otros sitios populares, como Digg.com o Youtube.

También Facebook ha sido utilizada por los ciberdelincuentes para hacer negocio. En mayo, se detectó la variante número 56 de la familia de gusanos Boface. Diseñado especialmente para utilizar esta red social, debido a su popularidad a nivel mundial, la misión de esta versión BJ (que se propaga a través de un archivo que se ejecuta en el equipo) era descargar e instalar falsos antivirus y engañar a los usuarios haciéndoles creer que su equipo estaba infectado y que debían adquirir un antivirus falso. Según los cálculos de PandaLabs, dos millones de internautas podrían estar infectados, y, aunque la distribución de las infecciones está muy repartida, el 40 por ciento de ellas se localiza en EEUU.

Suplantación de identidad

Además de intentar obtener beneficios económicos a través de los falsos antivirus, otro de los peligros con los que pueden encontrarse los usuarios de este tipo de redes es la suplantación de identidad. Un hecho del que pueden ser víctima tanto personajes conocidos como personas anónimas, y que prolifera al amparo de la falta de protección de la identidad en estas redes y que hace que las víctimas se encuentren en la Red falsos perfiles con su identidad.

Otra forma de suplantación consiste en apoderarse del perfil de la cuenta de una persona en la red social, e introducir en ella información que la pueda comprometer.

Mientras que crear perfiles con datos falsos para participar en una red social no es constitutivo de delito, sí lo es la usurpación del estado civil (nombre, apellidos, domicilio...). Entrar en una cuenta o perfil de otra persona puede suponer que se esté cometiendo un delito de lesión de privacidad, y si se hace pasar por el verdadero titular se estaría cometiendo un delito de usurpación de estado civil. Estos casos están sancionados con penas de prisión que van de seis meses a tres años.

Para evitar estas situaciones, los expertos en seguridad recomiendan a los usuarios utilizar contraseñas alfanuméricas que contengan letras mayúsculas y minúsculas.

También en redes corporativas

Pero la presencia de los ciberdelincuentes no se limita a las redes sociales utilizadas como forma de ocio y entretenimiento. También las redes empresariales, profesionales y de negocio han sido utilizadas por los cibercriminales para albergar en ellas código malicioso.

Un ejemplo de ello es la red LinkedIn, considerada una de los sitios de redes profesionales más importantes del mundo, con más de 30 millones de usuarios. En ella, Trend Micro detectó, a principios de 2009, la presencia de código malicioso utilizado para realizar ataques a los miembros del propio sitio. La forma de actuar es la misma que en el caso del resto de redes sociales: a través de la lista de contactos de cada usuario se difunden los mensajes con enlaces de *malware*, infectando a los usuarios del propio sitio web. También en este caso, la principal motivación es conseguir atacar equipos en la mayor parte posible de lugares para conseguir datos e información confidencial con los que los delincuentes puedan sacar beneficio económico.

El mecanismo tradicional empleado por los cibercriminales es utilizar diversas funciones dentro del sitio red de negocios, como LinkedIn Answers y el acceso desde dispositivos móviles.

Mejorar la privacidad

En este sentido, la comisaria europea de Sociedad de la Información y Medios de Comunicación, Viviane Reding, ha declarado que los ciuda-

danos de la Unión "tienen derecho a controlar cómo se utiliza su información personal" y ha asegurado que la Comisión "tomará medidas cada vez que los Estados miembros de la Unión Europea (UE) no velen por el respeto de ese derecho".

Asimismo, ha instado a las empresas de redes sociales a reforzar la protección de la intimidad, que considera que debe ser "una de las principales prioridades de los proveedores de redes sociales y de sus usuarios". Además, considera que, en el caso de los menores, los perfiles deben ser privados por defecto, e innacesibles para los motores de búsqueda en Internet.

También se ha mostrado favorable a la especial protección de los menores en Internet la Agencia Española de Protección de Datos (AEPD). Su presidente, Artemi Rallo, ha mantenido una serie de reuniones con representantes de las redes más populares de España, como Facebook y Tuenti, en las que ha transmitido la preocupación de la AEPD por el cumplimiento con la normativa española.

En el caso de Facebook, la edad mínima a partir de la cual permite ser usuario es de 13 años, conforme a la legislación norteamericana. Sin embargo, sus representantes han señalado ante la AEPD su intención de considerar la posibilidad de incrementar el límite de edad en nuestro país, ya que en España la edad mínima para que los menores puedan compartir información mediante este tipo de servicios es de 14 años.

Tuenti, por su parte, se ha comprometido ante la AEPD a implantar sistemas efectivos de verificación de edad y a depurar los perfiles de menores de 14 años.

Buscadores propios

Por otro lado, se ha detectado que los cibercriminales están empezando a crear sus propios buscadores, con el fin, siempre, de engañar a los usuarios y conducirles hasta páginas maliciosas creadas para distribuir *malware*. Hasta ahora, se conformaban con posicionar sus páginas entre los primeros resultados de los buscadores más conocidos, mediante técnicas maliciosas de optimización de búsqueda.

El funcionamiento de estos buscadores, cuya técnica se conoce como ingeniería social, consiste en que, cuando el usuario introduce una palabra en el buscador, éste le muestra varios resultados. Si pincha en alguno de ellos, es redirigido a una página preparada para distribuir contenido malicioso.

Decalógo de riesgos

Para evitar este tipo de infecciones, Panda Security recomienda utilizar sólo buscadores de confianza. También es recomendable extremar las precauciones con las webs que ofrecen vídeos sensacionalistas o noticias curiosas.

Además, conviene mantener actualizados los sistemas de detección de virus en los equipos, teniendo instalada siempre la última versión disponible del *software*.

Por otro lado, Facebook ha anunciado dos medidas para mejorar la privacidad. En primer lugar, ha anunciado que va a implantar un sistema que permitirá a los usuarios seleccionar con quién comparten la información cada vez que la publiquen, eligiendo desde una privacidad parcial hasta una publicidad total. Además, ha afirmado que obligará a los usuarios a revisar y actualizar sus configuraciones de privacidad.

Por otro lado, BitDefender ha elaborado un decálogo de los riesgos sociales y técnicos más habituales en este tipo de redes, e incluye los siguientes: sustracción de datos, fugas involuntarias de información, ataques dirigidos, grado de vulnerabilidad de la red, *spam* y *phishing*, modificación de contenido, propagación de *malware*, reputación profesional, costes de infraestructura y mantenimiento y pérdida de productividad.

Dónde denunciar

Para facilitar la denuncia de este tipo de delitos por medio de Internet, la Brigada de Investigación Tecnológica (BIT) de la Policía Nacional dispone de la página **https://www.policia.es/denuncias/entrada**, o bien para informar específicamente sobre delitos tecnológicos, a través de correo electrónico en **delitos.tecnologicos@policia.es** o **denuncias.pornografia.infantil@policia.es**.

El Grupo de Delitos Telemáticos (GDT) de la Guardia Civil también pone a disposición de los internatuas un servicio que permite realizar denuncias, a través de **https://www.gdt.guardiacivil.es/media/formatodenunciav1.rtf**. Además de denunciar, ofrece la posibilidad de colaborar con ellos, a través del *link* **https://www.gdt.guardiacivil.es/pcolabora.php**, dirigido tanto a expertos como a aficionados que dominen las tecnologías y la Red.