Seguridad en redes Sociales

(Abstract extendido)

Marc Rivero López
S21Sec
Email: mrivero@s21sec.com

Las redes sociales se han convertido en bases de datos donde se almacena la información de multitud de usuarios. La propia red social insta a que el usuario rellene datos opcionales como, gustos musicales, religión, estado, ciudad de origen etc...

El usuario tiene la sensación de que su actividad se verá aumentada cuando rellena estos datos, de lo que no es consciente es que está proporcionando información que puede ser usada para que se realicen ataques dirigidos.

La seguridad de nuestros datos personales deberían de cobrar mucho mas valor en este tipo de ámbitos.

Las redes sociales además permiten el que se puedan subir fotos, para poder compartir con tus amigos. Estas fotos contienen metadatos que dan información como por ejemplo, sobre cuando se realizó esa foto, las coordenadas GPS, de manera que se podrían estudiar hábitos en los viajes que realiza dicho usuario en concreto.

La seguridad también ha de enfocarse en el acceso, es decir, redes sociales como Twitter por defecto implementan HTTPS. Esto garantiza que los datos que enviemos estarán cifrados.

Por correo electrónico nos llegan los mensajes de notificación de que alguien nos ha agregado, o que alguien nos envió un mensaje, este tipo de mensajes también es común que lo usen en campañas de SPAM. Este tipo de correos enfocados a usuario final tienen como finalidad el robo de credenciales mediante phishing.

El uso de contraseñas robustas dificulta que alguien pueda mediante fuerza bruta obtener nuestra cuenta. La red social LinKedIn sufrió un robo de sus contraseñas. En la fuga se ha realizado un estudio de las contraseñas mas usadas y se ha vuelto a demostrar que los usuarios siguen utilizando contraseñas débiles.

Otro vector de ataque usado es el de los acortadores URL, este servicio en principio legítimo se está usando para la distribución de malware. Al usuario se le presenta un mensaje atractivo en su red social, este enlace apunta en realidad a un Exploit Kit con el que el usuario sin percatarse de nada ser infectado. Los Exploits Kits, mas caros en el mercado underground están actualizados para infectar a usuarios que tengan el navegador actualizado y es que, es posible que contengan 0day que aún no es conocido por el fabricante de software. Cuando consiguen un fallo de este tipo, se suelen realizar campañas que afectan a multitud de usuarios. Se hace así para lograr la máxima infeccción posible antes de que el fabricante solucione el fallo. Una recomendación para este tipo de acortadores es no acceder a ellos si no tenemos confianza en el contenido que pueda albergar.

Los ataques de tipo persistentes o también denominados APT, han sido usados para atacar a grandes compañias como RSA, HBGARY. Los ataques APT se basan en su mayor medida en estudiar al objetivo a atacar. Las redes sociales ya nos proporcionan información para que un atacante pueda reunir la información necesaria para preparar un ataque a medida.

El phishing es otra de las armas usadas contra el usuario final para el robo de credenciales. Un ejemplo de phishing es el caso de fbaction.net. Al usuario final le llegaba un mensaje que hacia al usuario acceder a la URL que había en el correo. Cuando el usuario accedía se le mostraba la página de login de Facebook.

Las fotos que se cuelgan en las redes sociales contienen coordenadas con las que se puede trazar al usuario y saber donde está. Existen ya aplicaciones que introduciendo el nombre dicha red social te dibuja en un mapa donde ha estado dicha persona. Además no solo las fotografías contienen coordenadas, los mensajes también por defecto guardan desde donde el usuario está actualizando la red social.

El malware es uno de los protagonistas mas importantes en la seguridad de las redes sociales. Como curiosidad algunos troyanos bancarios mas importantes como Zeus, debido a todo el tráfico y al gran uso por parte de los usuarios, directamente en la función del troyano que registra las webs donde el usuario introduce credenciales y navega no se guardan de páginas como Facebook.

Las llamadas redes Botnet también tienen cabida en este tipo de redes. Se han realizado pruebas de concepto donde a través de las cookies de los usuarios infectados se podían comunicar a través de la red social Facebook. La herramienta de la prueba de concepto es FaceCat, desarrollada por Jose Selvi de S21Sec.

Otro vector de ataque usado es el clickjacking, en este tipo de ataques, al usuario se le superpone encima de la web real otra página web. Cuando el usuario realiza el click, no se percata que en realidad está aceptando otra cosa.

El malware, la suplantación de identidad, el profiling de usuarios para ataques dirigidos son y seguirán siendo el vector de ataque usado por los atacantes, para conseguir infectar usuarios y robar y vender datos personales.