ENGAÑOS DE PHISHING Y PHARMING

En una acción también conocida como “ingeniería social” el delincuente informático busca hacerse pasar por el Banco o por una persona o entidad conocida para engañar al usuario.

Con el engaño pretende robar información confidencial a través de manipulación de usuarios legítimos, obtenidos a partir de la instalación o utilización de algún programa malicioso. Algunas de las tácticas más comunes son: phishing, spoofing, pharming, a través de spyware, worms, entre otros.

PHISHING

Una estafa cada vez más frecuente que actualmente está siendo empleada por individuos sin escrúpulos, es el Phishing.

El phishing consiste en el robo de datos bancarios por medio de Internet. El método más habitual es el empleo del correo electrónico enviado a tantas direcciones de correo electrónico de internet como el usuario mal intencionado puede obtener, para contactar con usuarios y convencerles de que visiten páginas que imitan las de la entidad suplantada presumiendo provenir de una organización legítima en la mayoría de los casos de un Banco, un servicio de pagos en línea, un minorista o similar, y en las que, además, deben introducir datos personales (número de cuenta, PIN, número de tarjeta de transacciones bancarias, etc.,), que quedan así registrados. Es habitual que después de la introducción de los datos se muestre una página de error, para que la víctima piense que no se ha podido realizar la conexión y así no sospeche nada.

O bien el correo electrónico solicita que el destinatario ponga al día o verifique su información personal y financiera, incluyendo la fecha de nacimiento, la información de conexión, los detalles de cuentas, los números de la tarjeta de crédito, los números de identificación personal (PIN), etc. Algunos mensajes electrónicos incluyen una amenaza de que si no se actualiza o se valida causará, por ejemplo, que la cuenta sea congelada. El objetivo es inducir a destinatarios confiados, que resultan ser los clientes

de la organización legítima que ha sido imitada, a responder al correo electrónico y proporcionar la información solicitada.

El correo electrónico contendrá una link que le llevará a un sitio web que imita y se aprecia idéntico, o al menos muy similar, al sitio genuino de la organización. En algunos casos, cuando la link en el correo electrónico es pulsado, el sitio genuino es accedido, pero es cubierto con una ventana más pequeña con el sitio falso, haciéndolo más creíble. Pulsar sobre un link también puede descargar en su PC software malicioso, conocido como "spyware", que registrará su uso del Internet y reenviará esta información, y posiblemente un registro de lo que haya tecleado, al usuario mal intencionado.). En la práctica, cuando el troyano detecta que el usuario está visitando la URL de una entidad bancaria, el keylogger se activa y recoge todas las pulsaciones del usuario, que normalmente incluirán logins, passwords, números de cuenta y otros datos bancarios. El usuario malintencionado usará esta información financiera para comprometer cuentas bancarias, tarjetas de crédito, etc.

Para evitar ser víctima del Phishing, nunca responda a mensajes de correo electrónico que requieran información personal o financiera, y nunca pulse un link en ese tipo de correos. Las organizaciones de buena reputación no envían mensajes de correo no solicitado pidiendo a sus clientes actualizar o verificar sus detalle personales y de seguridad. Si tiene duda respecto a la legitimidad del correo, o si cree que ha sido víctima de un engaño de Phishing, debe contactar inmediatamente a la organización de la que se trate. Sin embargo, debe tener cuidado en utilizar el método acostumbrado con el que contactas a esta organización, en lugar de usar cualquiera sugerencia incluida en el correo o respondiendo a éste.

PHARMING

Además de los citados métodos, últimamente se ha reportado un método nuevo, más sofisticado y con el mismo fin, llamado pharming. En este caso, el ataque se realiza al ordenador del usuario o al proveedor de servicio de Internet, de modo que cuando el usuario solicita -como hace normalmente- una página de su entidad bancaria, se le redirecciona a otro sitio web que imita la página original.

En la actualidad, la detección de las citadas amenazas que persiguen el fraude electrónico está supeditada al uso que hacen de las técnicas de malware tradicionales.

En el caso del phishing, tanto si se utilizan técnicas de spam en su difusión, como si se emplean keyloggers conocidos, o si se explota la vulnerabilidad del navegador que permite mostrar una dirección falsa en la barra de direcciones del explorador, la detección es posible. En el pharming, la neutralización es más compleja, máxime si el ataque lo llevan a cabo usuarios malintencionados desde el exterior y no algún tipo de malware introducido previamente.

MULAS DEL PHISHING

Una vez que los defraudadores han recolectado la información financiera de individuos a través del Phishing, están en posición de abusar de esta información y de robar dinero de las cuentas comprometidas. Para cubrir sus pistas reclutan a individuos confiados para actuar como mediadores, que colocan una variedad de ofertas tentadoras de trabajo en el Internet, prometiendo la posibilidad ganar dinero rápidamente y sin mucho esfuerzo. A estos individuos se les conoce como mulas.

Las cuentas bancarias de las mulas son utilizadas para depositar las transferencias del dinero de las cuentas que han sido comprometidas. Entonces, los defraudadores de Phishing dan la instrucción a las mulas de retirar de sus cuentas el dinero en efectivo y reenviarlo, restando la comisión prometida, a través de agencias de transferencia de fondos internacionales. Por lo que los defraudadores pueden conservar su anonimato, aunque hay un rastro hacia las mulas, que puede ser seguido por las autoridades.

Ten mucho cuidado de las ofertas de trabajo que involucran aceptar y liberar fondos a una cuenta bancaria a cambio de una comisión. Las mulas reclutadas por los defraudadores de Phishing, lavan dinero, y es muy probable que tengan que enfrentar un proceso criminal.