CUADERNOS DE SEGURIDAD
Núm. 317 • DICIEMBRE 2016 • 10 euros
PUNTOSEGURIDAD.com

JOSECHU MIGOYA ELDUAYEN. INNOTEC SYSTEM

Fraude bancario, el juego del ratón y el gato

Una técnica de defensa muy utilizada por nuestros equipos es el uso de códigos trampa avanzados (trapcode) que se ocultan en los sitios web de las entidades bancarias, y que recogen información de todas las peticiones recibidas para que sean correladas y analizadas por los servicios de gestión de incidentes

Suplantación de identidad (corporativa o de usuarios), malware y troyanos, correos fraudulentos, black markets, phishing, pharming, abusos de marca..., son numerosos los vectores de ataque con los que los ciberdelincuentes intentan estafar y obtener un importante botín a los clientes del sector bancario. Ante esta situación, las entidades deben apostar por una detección proactiva, que permita la monitorización de sus redes y equipos, el análisis de sitios web fraudulentos y, sobre todo, una capacidad absoluta para evolucionar al ritmo de los atacantes e, incluso, anticiparse a sus acciones.

La historia del fraude bancario ha sido el juego del ratón y el gato: según se añaden capas de seguridad a los procesos, los atacantes buscan nuevas formas de saltárselos y, según los atacantes encuentran nuevos métodos de ataque, las entidades implementan nuevas estrategias para repelerlos.

El objetivo de estas entidades es doble: por un lado ofrecer al cliente la misma seguridad al operar por Internet (bien sea desde un ordenador, un portátil o un Smartphone), que personándose en una sucursal bancaria; y, por otro, asegurar que las operaciones son realizadas por usuarios legítimos sin interferencias o intervenciones maliciosas.

Medidas tradicionales frente al fraude

Un ejemplo concreto de esta evolución lo encontramos en la identificación de los usuarios. Inicialmente se proporcionaba unas claves de acceso (usuario/contraseña) que tenían que introducir al acceder al sistema.

Al aparecer el malware (programas maliciosos) de tipo keylogger, que registra las pulsaciones de los usuarios, se

empezaron a implementar teclados virtuales que permiten introducir parte de la clave pulsando en la pantalla sin que sea registrada por el teclado. Posteriormente surgieron variantes que capturaban, además del teclado, la pantalla del usuario.

La respuesta de las entidades financieras fue la introducción de un «doble factor» (o «segundo factor») de seguridad en las operaciones más delicadas. Este se basa en la aportación de dos credenciales de diferente naturaleza:

- **Algo que sabes:** credenciales de acceso o pregunta de seguridad.
- **Algo que tienes:** valor de una tarjeta de coordenadas, DNI electrónico o SMS.
- **Algo que eres:** uso de sistema biométrico que permite validar tu persona como la huella dactilar, la voz o el iris del ojo.

Además, muchas de las entidades bancarias han aumentado la seguridad, incluyendo también soluciones de OTP (One-Time Password) en las que se pide un valor aleatorio que el cliente recibe por otra vía, por ejemplo, un mensaje SMS. Este tipo de sistemas son bastante efectivos pero, aún y así, los atacantes han rizado el rizo creando malware que modifica la página del banco al ser visitada, invitando a los usuarios a instalarse en su dispositivo una aplicación móvil para recibir algún supuesto servicio, cuando en realidad roban los OTP que envía el banco.

Este tipo de malware, conocido como troyanos bancarios, lleva entre nosotros mucho tiempo, siendo los más famosos Zeus y sus variantes. Estos programas maliciosos, una vez que infectan a un cliente, se inyectan en el navegador monitorizando las páginas que visitan de forma que, cuando se conecte a ciertos sitios web, modifican su contenido. De esta forma pueden robar las credenciales, mostrar mensajes que engañen al usuario o pedir otros

datos. Las modificaciones para cada entidad se encuentran en un fichero de configuración que se descarga de Internet, lo que permite afectar a varios bancos con una sola infección y mantener actualizado el fraude.

Conociendo a la víctima, ingeniería social

En nuestro servicio de antifraude, se han llegado a detectar incidentes donde un ordenador es infectado con un malware, de tipo spyware, que espía durante mucho tiempo el comportamiento del cliente, accediendo a sus correos electrónicos, historial de navegación , acceso a redes sociales, etc. y, por tanto, llegando a conocer casi al completo su vida.

Incluso, se detectó el caso de una persona que, para agilizar sus trámites, se ponía en contacto con el director de la sucursal por correo electrónico y realizaba transferencias por altos importes. Para tener más seguridad, se ponía en copia al gestor o al departamento financiero de la empresa. Los atacantes espiaron durante meses a esa persona y después enviaron un correo electrónico al director de la sucursal, solicitando una transferencia a una cuenta bancaria controlada por ellos. El correo imitaba perfectamente la forma de escribir utilizada en otros mensajes, incluida la firma y poniendo en copia al gestor para dar mayor veracidad a la petición. ¿Quién podría sospechar? Por suerte, en este caso, al no ser una transferencia nacional, como todas las anteriores, el director de la oficina se puso en contacto por teléfono para ratificar la información y la transferencia nunca llegó a realizarse.

Otro de los casos que hemos investigado de ingeniería social (cada vez más común), es el de una víctima que recibía una llamada desde fuera de España en la que alguien, que se identificaba como trabajador de Microsoft, le informaba de que su ordenador personal estaba comprometido con «un virus». A continuación, se le decía que, dentro del servicio ofrecido al adquirir una licencia de Windows, ellos mismos se encargarían de proceder a la limpie-

za del ordenador. Para ello solicitaban la instalación de una aplicación de control remoto, así como los datos de las cuentas bancarias habituales para validar que no estaban comprometidas. Por si fuese poco, indicaban que para arreglar el equipo necesitaban tres horas durante las cuales se debía ignorar cualquier llamada que recibiese que no fuese de ellos, así como cualquier SMS o acercarse al ordenador. De lo contrario, los «otros delincuentes» podrían llamar fingiendo ser del banco e inventarse que estaban realizando alguna transferencia.

Desgraciadamente, en esta ocasión, los delincuentes sí lograron su objetivo.

Defensa proactiva

Ante esta situación, las entidades bancarias han reaccionado utilizando nuevas técnicas de detección con diferentes tecnologías.

Una de ellas es el uso de la esteganografía; es decir, ocultar información en ficheros legítimos sin que sea visible para un posible intruso. De este modo, cuando un atacante se descarga una web para manipularla y hacer posteriormente phishing (una copia de la imagen del portal para fines fraudulentos), también se descargan ciertos ficheros, por ejemplo, imágenes, que contienen información identificativa de la conexión. Cuando el Phishing es activado, se puede obtener un rastro que localice al atacante a través de esta información.

Otro ejemplo, muy utilizado por nuestro equipo, es el uso de códigos trampa avanzados (trapcode) que se ocultan en los sitios web de las entidades bancarias y que recogen información de todas las peticiones recibidas para que sean correladas y analizadas por los servicios de gestión de incidentes.

La confección de listas blancas de marcas y dominios, el análisis de sitios web fraudulentos o el bloqueo de navegadores web son otras de las técnicas fundamentales a la hora de luchar contra este tipo de fraude.

No obstante, y a pesar de que se van incluyendo nuevas medidas de seguridad que hacen más difícil los fraudes y extorsiones, siempre existen nuevas posibilidades de que los delincuentes lleven a cabo sus actividades. Por lo tanto, es preciso seguir trabajando en actualizar las medidas de protección y concienciar a los usuarios de las amenazas existentes dado que, al final, muchos de los ataques son llevados a cabo abusando de su confianza, ingenuidad y desconocimiento.

Fotos: Innotec System

Contactos de empresas, p. 9.