Seguridad en el e-Commerce

Robo de datos en operaciones comerciales por medios electrónicos

Delitos como el phishing y las distintas variantes de malware fueron ampliamente descriptas en ediciones anteriores. En esta oportunidad, damos cuenta de cómo estos delitos informáticos pueden afectar a las transacciones comerciales realizadas por medios electrónicos.

Osvaldo Callegari
Analista de sistemas - *ocalle@ar.inter.net*

El e-Commerce, conocido en español como "comercio electrónico", es la realización de transacciones comerciales de productos o servicios a través de Internet u otros medios electrónicos, tales como un cajero o dispositivo móvil. En los últimos años, el comercio electrónico se popularizó a nivel mundial y Latinoamérica no constituye una excepción, ya que se acrecentó la cantidad de personas de la región que están utilizando estos servicios. Este crecimiento se vio especialmente potenciado por la confianza acentuada de los usuarios para con estas plataformas.

De acuerdo a los resultados arrojados por el Estudio Integral de Comercio Electrónico y Consumo Online en Argentina 2011, durante ese año, por las operaciones comerciales a través de Internet en que participaron consumidores finales, se facturaron 11.593 millones de pesos (excluyendo IVA), lo que representa un crecimiento del 49,5% en comparación con igual parámetro para 2010.

Sin embargo, al utilizar estos servicios, existen una serie de amenazas informáticas relacionadas que los usuarios deben considerar para no exponer en sus compras online su información personal o, peor aún, su dinero.

Malware y phishing son dos amenazas para el eCommerce. De características diferentes, ambas tienen el mismo fin: obtener las claves del usuario

LAS AMENAZAS AL USUARIO

Para empezar, el usuario debe recordar siempre que al utilizar los servicios de comercio electrónico, se están realizando transacciones comerciales aunque, a diferencia de una operación tradicional, se realiza a través de medios virtuales. A pesar de que esta situación puede generar en el usuario una sensación de menor riesgo que en una transacción comercial física, en ambos casos se encuentra involucrado un factor de valor: el dinero.

En este contexto, existen, básicamente, tres amenazas relacionadas con el e-Commerce, todas ellas con finalidades asociadas al lucro por parte de los atacantes. Estas amenazas pueden ser divididas en dos rubros, que explicaremos a continuación.

MALWARE Y PHISHING

En una primera categoría aparecen dos amenazas relacionadas al robo de credenciales de acceso a sitios de e-Commerce: el malware (edición número 61, mayo de 2011 de RNDS) y el phishing (descripto ampliamente en la edición correspondiente a marzo de 2007 de este medio).

Por un lado, los códigos maliciosos enfocaron gran parte de su actividad en el robo de información de los sistemas infectados, especialmente a través de spyware -aplicaciones que recopilan información del usuario, sin el consentimiento de éste- u otras variantes como gusanos o troyanos diseñados para convertir a los equipos en parte de botnets, redes de computadoras zombis que son controladas remotamente por un atacante. En estos casos, el robo de datos también es frecuente, especialmente a través de funcionalidades de keylogger que permiten capturar las pulsaciones del teclado del usuario afectado.

En el caso de los bots, estos suelen tener relación con este tipo de servicios, como el caso reportado por el equipo de Laboratorio de ESET Latinoamérica de Zeus y su relación con los ataques de phishing a sitios bancarios, donde se demostraba la estrecha relación al observar cómo el malware está diseñado junto a la arquitectura de la red para el robo de datos de acceso a sitios de home banking.

En segundo lugar, los ataques de phishing, también diseñados para robar información personal, suelen ser realizados para afectar sitios de e-Commerce. Se conocen como ataques de phishing aquellos que obtienen información sensible del usuario a través de la simulación de una entidad de confianza para la víctima.

El objetivo, en el caso de ambas amenazas, es el mismo: obtener usuario y clave (o las credenciales de acceso necesarias según el servicio) para acceder al sitio. Posteriormente, esos datos pueden ser utilizados con diversos fines económicos fraudulentos, que tienen su máxima aplicación en los casos que hay una relación directa entre la información obtenida y el dinero, ya que muchos usuarios tienen

asociadas las cuentas de estos sitios a sus tarjetas de crédito u otros servicios que habilitan la realización de transacciones en línea.

ESTAFAS POR MEDIOS TECNOLÓGICOS

En una segunda categoría podemos ubicar al scam: la realización de estafas a través de medios tecnológicos. El caso más frecuente, en relación a los sitios de comercio electrónico, es la creación de perfiles falsos para comercializar productos inexistentes y engañar a los usuarios con la reputación de los vendedores, aunque también puede directamente realizarse la estafa sin la necesidad de crear usuarios en la plataforma, sino a través de falsos sitios web.

Tanto el malware y el phishing como el scam son amenazas que tienen como último fin el dinero del usuario y se aprovechan de la popularidad del e-Commerce para tener más víctimas y acrecentar la rentabilidad de los ataques.

"Es importante que, para estar seguro ante este tipo de amenazas, el usuario cuente con una solución con capacidades proactiva de detección de códigos maliciosos, como ESET NOD32 Antivirus, y adopte ciertas buenas prácticas básicas de seguridad", aseguró Sebastián Bortnik, Gerente de Educación & Servicios de ESET Latinoamérica.

LLevar a cabo estafas por medios electrónicos es cada vez más común. Por eso, el usuario debe estar prevenido y comprar a través de sitios y portales seguros

RECOMENDACIONES

Para prevenirse a la hora de realizar transacciones de comercio electrónico se recomienda:

1. ACTUALIZAR SU SISTEMA Y APLICACIONES: Mantener su sistema y sus aplicaciones actualizados le permitirá estar protegido de las amenazas que utilizan vulnerabilidades ya corregidas por los proveedores de los mismos.
2. USAR SERVICIOS E-COMMERCE DE REPUTACIÓN CONOCIDA: Para evitar ser estafado al realizar una compra o ser víctima de un robo de datos bancarios, es recomendable realizar las compras a través de servicios con reputación alta o recomendados.
3. EVITAR ENLACES EN LOS CORREOS ELECTRÓNICOS: Dado que en muchas ocasiones los cibercriminales utilizan técnicas de Ingeniería Social a través de correo para atraer a sus víctimas y así poder hurtar sus datos bancarios, se debe evitar hacer clic en los enlaces que se reciben por esta vía. Para ingresar a los sitios donde se presentan las ofertas, se recomienda escribir la dirección de la página web en el navegador y verificar que esta oferta realmente exista.
4. VERIFICAR LA SEGURIDAD DEL E-COMMERCE: Es indispensable verificar que el sitio en el que se encuentra navegando envíe los datos de manera cifrada, es decir, que opere bajo el protocolo HTTPS en lugar de HTTP. Puede chequear esto en la barra de direcciones, delante de la URL del sitio.
5. NO UTILIZAR CONEXIONES WI-FI DE DUDOSA CONFIABILIDAD: En caso de conectarse desde un dispositivo móvil, recuerde que las redes wi-fi públicas, sean libres o protegidas por contraseña, pueden estar siendo interceptadas, por lo que es recomendable realizar transacciones en línea a través de una red de confianza o utilizar algún mecanismo adicional de seguridad sobre la red como una VPN para asegurarse de establecer un canal seguro entre el servidor y el cliente. ■