



El Semanario / Fernando Luna

En el Centro de la Ciudad de México se registra el mercado negro de bases de datos que sirven para sustraer dinero de las cuentas bancarias.

FINANZAS

Ladrones en línea

◆ Los tiempos de crisis alimentan las trampas. Por eso, la comercialización fraudulenta de datos personales y de operaciones financieras a través de Internet se ha convertido en un jugoso negocio en todo el mundo, y México no es la excepción.

Frente a la Plaza de la Computación, en pleno centro de la Ciudad de México, entre el bullicio de jóvenes que ofrecen programas de cómputo y videojuegos piratas, y de manera muy discreta, hay alguien que ofrece por 300 pesos una trampa: obtener el password de cualquier correo electrónico. “Anótame en un papelito el correo y en diez minutos te traigo la clave, vamos a probarla y me pagas. ¿Cómo ves?”, dice a manera de reto.

Seguro de lo que dice, este malhechor no acepta preguntas que lo orillen a desvelar su modus operandi y, con una sonrisa cínica, sólo se limita a comentar que sus mejores clientes son aquellos que gustan del espionaje en todas sus derivaciones (familiares, amistosas, laborales). Y, para no cargar culpas, rechaza que su oficio sirva para escudriñar en cuentas bancarias. Ése, presume, no es su negocio, aunque suelta: “Conozco a otros colegas que sí le entran a eso”.

Sí, la compra y venta de datos se está convirtiendo rápidamente en un atractivo negocio, y quienes se dedican a esta actividad no dudan incluso en publicitar y ofrecer abiertamente sus servicios: bases de datos con información que son utilizadas para sustraer dinero de las cuentas o realizar operaciones en línea con tarjetas de crédito. El mercado negro de este tipo de información, que se rige también por la oferta y la demanda, es tal que, incluso, ya existen referencias internacionales para saber

si la información se ofrece a un precio justo o es demasiado cara.

Los datos disponibles encienden la alerta. Según un informe elaborado por la empresa Symantec, que aborda el fenómeno de la “Economía Clandestina”, se estima que entre el primero de julio de 2007 y el 30 de junio de 2008, el valor potencial de todos los bienes anunciados fue superior a 276 mdd, y que la información de tarjetas de crédito es lo que más se ofrece en la economía clandestina con un porcentaje de 31%, seguida de la información de cuentas bancarias con 20%.

Lo más interesante es que Symantec logró detectar el rango de precios a los que se comercializa esta información; por ejemplo, los datos de tarjetas de crédito —que incluyen el número del plástico, fechas de vencimiento y dígitos de seguridad— se ofrecen desde medio dólar hasta 12 dólares por tarjeta, mientras que los datos de las cuentas son el producto más caro ya que fluctúan entre 10 y 1,000 dólares. Por su parte, las contraseñas de cuentas de correo se comercializan entre 4 y 30 dólares, lo que significa que los piratas cibernéticos nacionales están “en línea” con las cotizaciones internacionales.

Además, el estudio de la firma encargada de servicios de seguridad en la red deja claro el crecimiento de la economía clandestina; en el periodo que comprendió su informe, detectó 69,130 anunciantes activos distintos y más de 44 millones de mensajes publicados en diferentes servidores.

Y la tendencia va al alza.

EL MARCO LEGAL

Jorge Díaz, director de Desarrollo y Mercado-tecnia de Servicios de Mexis, empresa mexicana experta en seguridad de redes, considera que la

falta de una cultura de seguridad es la mayor amenaza porque deja abierta la puerta al robo de información confidencial.

Según la encuesta más reciente de la Asociación Mexicana de Internet (Amipci) más de 80% de los usuarios de servicios financieros en línea culpan directamente a las instituciones cuando son víctimas de un fraude o desfalco de sus cuentas, aunque en muchos casos los propios clientes son los que no cumplen con las recomendaciones que hacen los bancos. “Uno de los riesgos somos nosotros mismos”, reconoce Díaz.

El experto opina que si bien las autoridades han empujado regulaciones para elevar los estándares de seguridad de la información y recursos de los clientes, debe existir un equilibrio entre bancos y los usuarios para mantener bajo resguardo la información. “Por ejemplo, el *phishing* (la identidad falsa de una página) se da en el momento en el que el usuario abre un correo que sabe que no debería de abrir, y el reto es crear la conciencia en el usuario para que no lo haga”, explica Díaz.

En México, hace dos años la Comisión Nacional Bancaria y de Valores (CNBV) emitió una circular única para reforzar la seguridad de todas las operaciones bancarias electrónicas, que no sólo aplican para Internet, sino que además incluyen nuevos lineamientos para las transacciones telefónicas e, incluso, los cajeros automáticos. De hecho, la Asociación de Bancos de México (ABM) está a punto de dar a conocer una serie de actualizaciones de la norma que fueron resultado del trabajo coordinado con las autoridades, que iniciaron en diciembre de 2008.

Más de 80% de los usuarios de servicios financieros en línea culpan directamente a las instituciones financieras cuando son víctimas de un fraude, consigna un estudio.



Pero, además, el gremio bancario implementó desde hace varios años prácticas internas para evitar la fuga de información confidencial o la comercialización de las bases de datos de sus clientes. De acuerdo con fuentes de la ABM, periódicamente y de manera aleatoria, acuden a los domicilios del personal que atiende las cajas en los bancos para “constatar que su patrimonio no se ha incrementado fuera de lo normal”. El último reporte de la CNBV detalla que hasta septiembre del año pasado operaban en el país 10,672 sucursales y 151,439 empleados, de los que 60% cubren puestos relacionados con el manejo de información, según estimaciones de expertos.

Así, en caso de que se detecte que algún empleado comercializó o sustrajo de manera indebida información, se denuncia a las autoridades argumentando la violación del Artículo 115 de la Ley de Instituciones de Crédito, que hace referencia al secreto bancario.

ENEMIGO AL ACECHO

Jorge Díaz, de Mexis, dice que pese a las medidas de protección todavía seguirán reportándose ataques, y esto no es una situación exclusiva de México, sino más bien una tendencia mundial. “Primero, los atacantes lo hacían como *hobby* o una especie de reto. Ahora, son todos unos profesionales que lucran con lo que hacen.”

De esta manera, el experto advierte que no existe una cultura de prevención en términos de los permisos de acceso que las empresas entregan a su personal. “El hecho es que 70% de los ataques son internos, es decir, se generan por usuarios con desconocimientos de aplicaciones que bajan y abren las puertas, y que está coludido con gente de fuera para vender información”, enfatiza.

En el caso de los bancos, hay mucho desarrollo de personal y es común que se “hereden” permisos y, dado que no hay una administración correcta de los accesos en función a las aplicaciones, “llega un momento en que eres un usuario que tienes acceso a todo y no hay administración de identidades”.

Mexis ofrece en su cartera de productos una aplicación que se basa en la correlación de eventos, es decir, que cuando un empleado de una institución financiera intenta acceder a una base de datos o aplicación, tiene que hacer “varios brincos”, y este servicio permite monitorear cada salto e identificar un movimiento inusual.

El principio de esta aplicación es idéntico al que utilizan los bancos para monitorear el uso y consumos promedio de un cliente, y que al detectar una operación inusual inmediatamente alertan al usuario limitando temporalmente el uso, por ejemplo, de la tarjeta. La ventaja de la aplicación de Mexis es que toda la gestión es fuera de la institución, lo que reduce la posibilidad de que los empleados

accedan al perfil del cliente, o peor aún, a información confidencial, sobre todo ahora que con el recorte de personal, algunos empleados puedan externar su enojo, sustrayendo información para comercializarla posteriormente.

El problema del robo de información para su posterior comercialización es generalizado en el mundo. Symantec detalla en su reporte que el mayor número de servidores de economía clandestina, que tienen un periodo de vida muy corto para evitar que sean detectados por las autoridades, se localizó en América del Norte con 46% del total, seguida por Europa, Medio Oriente y África con 38%; Asia Pacífico y Japón con 10% y AL con apenas 5%.

Por eso es que una de las opciones para mejorar la seguridad de los medios de pago es la que plantea la firma S21sec, especializada en seguridad digital. La empresa trabaja en el desarrollo de un estándar único para tarjetas de crédito para salvaguardar tanto los datos como las operaciones que realizan los titulares del plástico, en cualquier parte del mundo. La propuesta se conoce como Payment Card Industry Data Security Standard, alineado con las normas internacionales que califican e identifican a los usuarios, comercios y proveedores de servicios de primer y segundo nivel, división que parte del nivel de involucramiento que tiene en cada una de las transacciones.

La dificultad de iniciativas como ésta es que todos los participantes deben de invertir para mejorar o reconvertir sus sistemas para homologarlos, pero esto implica inversión que en estos momentos de crisis económica mundial no está disponible, aunque dadas las condiciones, es el mejor momento para reforzar la seguridad de todo el sistema. ●

Por Roberto Aguilar



El Semanario / Fernando Luna

La información de tarjetas de crédito es lo que más se ofrece en la economía clandestina con un porcentaje de demanda de 31%; después, está la información de cuentas bancarias con 20%.

Para tomarlo en cuenta...

Perimeter, una de las empresas líderes en materia de seguridad en Internet, identificó las amenazas en materia de protección que estarán presentes en 2009.

1) La mayor parte de las amenazas maliciosas llegan a las empresas por medio de los empleados, quienes de forma personal o a través de la misma solicitud de sus empresas, no adquieren programas que les permitan evitar daños en sus equipos. Las empresas, al mismo tiempo, no promueven entre sus empleados reportar este tipo de fallas o problemas tecnológicos.

2) Malware es un problema de generación de contenido malicioso (dañino) para los equipos de cómputo, que el usuario adquiere en forma de virus o como gusano malicioso; se prevé que siga creciendo en 2009.

3) Explotar las vulnerabilidades hoy se conoce como *hacker*, y se trata de alguien que utilizando un usuario y contraseñas falsas, ingresa a la información de un tercero para fines desconocidos, eliminando así barreras de protección colocadas por usuarios y empresas como el *firewall* y/o servidores, dejando la información vulnerable, antes estos *hackers*. Por ello, día a día se han actualizado sistemas de control y protección al usuario.

4) Gartner, empresa reconocida en el mundo de la tecnología, prevé que en el futuro cercano estas formas de filtrar sistemas de seguridad sigan siendo vulneradas por los *hackers* mediante mecanismos sofisticados.

5) El error o descuido de parte de los empleados es otra forma de vulnerabilidad bastante común y riesgosa, ya que éstos emplean claves y contraseñas que involucran información privada o personal y, por consecuencia, al mudarse incluso de trabajo y emplear las mismas contraseñas, pueden ser víctimas de la delincuencia.

6) Economía es un punto importante que consideran las empresas, quienes por las circunstancias no se ocupan de invertir en programas y planes que prevengan ataques masivos por su empresa.

7) Los trabajadores remotos son otro factor de inseguridad para la protección de los equipos, ya que al trabajar a distancia, y no dentro de la organización, pierden control sobre puntos importantes como: el *software* que utilizan para trabajar y proteger el equipo y, en consecuencia, la información que contienen y las actualizaciones de estos programas no tienen a una persona especializada en sistemas que les apoye y asesore; gente externa a la empresa puede manejar esa computadora y bajar o descargar programas con información maliciosa (infectada), entre otros.

8) Estar seguro que el proveedor de soluciones y programas de protección para los equipos sea serio, para no adquirir paquetes que sean vulnerables o riesgosos.

9) Descargar sólo software de protección que sea seguro y revisado por el especialista en sistemas de la empresa. ●