TOTALSEC NEWSLETTER – INFOSEC MX

BOLETIN 7

ABRIL 02 – 10

Elaboración: Abril 11, 2016

TECNOLOGÍA

En este número encontrarás noticias sobre:
- Tecnología
- Finanzas
- Gobierno
- Negocios
- En la opinión de Horacio Azzolin

Mexicanos desarrollan software para detectar rodo de información

por ABRIL 05, 2016 / YUCATAN.COM

Especialistas del Centro de Investigación y de Estudios Avanzados (Cinvestav) del Instituto Politécnico Nacional (IPN) desarrollaron un software especializado de seguridad de documentos para identificar el robo de datos, algo que no existe en el mercado.

Realizado en lenguaje C, con sistema Linux, haciéndolo posible de migrar a otras plataformas para su comercialización.

El sistema se instala en un servidor donde son guardados los documentos, estando disponibles en las terminales o computadoras de los miembros de la organización.

Esto con el fin de que puedan subir archivos y aplicar la encriptación, así como un código de rastreo capaz de identificar si es compartido de forma ilegal.

Los usuarios podrán solicitar la aplicación del software de seguridad al documento; sin embargo, estos no tendrán acceso al código de encriptación ni al de rastreo.

Fuente: http://yucatan.com.mx/tecnologia/computacion/mexicanos-desarrollan-software-para-detectar-robo-de-informacion

USB Thief, un nuevo malware que roba datos desde dispositivos extraíbles

por MARZO 24, 2016 / WE LIVE SECURITY

Este troyano, detectado por ESET como Win32/PSW.Stealer.NAI es conocido como USB Thief, y es utilizado en los dispositivos USB para distribuirse sin dejar rastro en el equipo infectado, empleando mecanismos especiales para protegerlo de una copia o reproducción haciéndolo más difícil de detectar y analizar.

Este malware puede atacar sistemas que se encuentran aislados de Internet.

Lo más probable es que no sea detectado mientras se mantenga en el dispositivo USB y se borre de la máquina tras haber terminado su misión.

En este caso el cifrado también sirve para vincular el malware a un dispositivo en particular y a la vez evita que el código malicioso se filtre fuera del entorno de destino deseado.

Ante esto, por seguridad los puertos USB deben desactivarse siempre que se pueda, y cuando no sea posible, se deben establecer políticas estrictas para su uso seguro.

El personal de la empresa debe de recibir una capacitación en seguridad cibernética, ya que este malware utiliza una forma poco común de engañar al usuario ya que en los dispositivos USB se suelen almacenar versiones portátiles de algunas aplicaciones muy comunes, como Firefox, Notepad ++, TrueCrypt, entre otras.

Por lo que cada vez que se ejecuta la aplicación, el malware también se ejecuta en segundo plano.

Fuente: http://www.welivesecurity.com/la-es/2016/03/24/usb-thief-roba-datos-dispositivos-extraibles/

FINANZAS

Los ATM, vulnerados por los ciberdelincuentes

por ABRIL 04, 2016 / FRONTERA MÉXICO

Pese a tener sistemas de seguridad avanzados, los ATM o cajeros automáticos, contienen importantes vulnerabilidades que los convierten en blancos de los ciberdelincuentes. Un ejemplo son los ataques llamados "jackpotting", los cuáles consiguen que los cajeros dispensen billetes sin control.

El problema surge desde los cajeros que corren sistemas operativos comunes (Windows XP), usen reproductores de flash desactualizados con más de 9.000 "bugs" conectados a herramientas de administración remota, además de estar compuestas por circuitos electrónicos con controladores industriales.

Además, de que en caso de que el cajero cuente con Windows XP, ya no recibirá soporte técnico ni actualizaciones de Microsoft. Haciéndolo más vulnerable ante posibles ataques.

Fuente:
http://www.fronteramexico.com/noticias/tecnologia/9891-los-atm-vulnerados-por-los-ciberdelincuentes.html

Centro biométrico frente a robo de identidad

por MARZO 29, 2016 / IT SITIO

Según cifras del Banco de México, son con 108 millones de pesos los fraudes ligados al robo de identidad, dejando a México en la octava posición a nivel mundial.

Estos casos, se dan en especial con la apertura de cuentas bancarias y tarjetas de crédito y débito no solicitadas, y en créditos diversos no reconocidos.

En una encuesta hecha por Unisys, el 85% de los mexicanos están de acuerdo en que bancos, agencias gubernamentales y comercios minoristas (retail), hagan uso de tecnologías biométricas (como lectores de huellas digitales, escaneo del iris o reconocimiento facial) para la protección de sus datos personales mientras que sólo el 14% no está de acuerdo.

Fuente: http://mexico.itsitio.com/control-biometrico-frente-a-robo-de-identidad/

Necesario garantizar protección de datos de deudores: INAI

por MARZO 27, 2016 / INFORMADOR

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI) consideró que es necesario que los despachos, entidades financieras o comerciales que realicen la cobranza extrajudicial implementen medidas que garanticen la protección de la información personal de los deudores (titulares de datos personales).

Así se podrán corregir malas prácticas mejorando el nivel de cumplimiento, esto de acuerdo con la Guía para ayudar con el correcto tratamiento de datos personales en la cobranza extrajudicial, elaborada por el INAI y la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef).

Fuente:
http://www.informador.mx/mexico/2016/652701/6/necesario-garantizar-proteccion-de-datos-de-deudores-inai.htm

Reclaman 100 mil robos de identidad

por MARZO 31, 2016 / DESPERTAR

En 2015, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), recibió 100 mil 488 reclamaciones por posible robo de identidad, con un monto de reclamaciones por 976 millones de pesos.

De las quejas, 53 mil 922 fueron por uso de productos financieros que el usuario no contrató, esto por 254 millones de pesos y otras 46 mil 566 por retiros en sucursal con 722 millones de pesos.

Por producto no reconocido, el monto promedio fue de 4 mil pesos y por retiro en ventanilla fue de 15 mil pesos.

A esto se suman otras 205 quejas recibidas entre el 22 de febrero y el 29 de marzo de este año, luego de que entró en vigor un protocolo en los bancos para evitar el robo de identidad.

Para que un banco considere que un delito financiero se cometió a través del robo de identidad, el mismo necesita un dictamen de la Condusef u otra acción jurídica, que podría tardar un año para el usuario, Condusef busca habilitar su facultad de arbitraje para que este tiempo reduzca a 60 días, se necesita que se conforme un comité conformado por miembros de Condusef, la Comisión Nacional Bancaria y de Valores (CNBV) y los bancos.

Fuente: http://despertardeoaxaca.com/reclaman-100-mil-robo-de-identidad/

GOBIERNO

En apoyo a Andrea Noel, Anonymous lanza campaña contra decenas de sitios de gobierno #NiUnaMas

por MARZO 31, 2016 / LO QUE SIGUE TV

El grupo de hacktivistas Anonymous en Latinoamérica, lanzó una ofensiva masiva en respuesta al acoso recibido contra la periodista Andrea Noel, que fue atacada sexualmente hace unas semanas en la colonia Condesa, uno de los principales barrios de la Ciudad de México, las autoridades a varias semanas de lo ocurrido no han podido dar con el responsable. Durante los ataques se dejó el mensaje:

"YA NO MAS INSULTOS YA NO MAS MUERTES YA NO MAS IMPUNIDAD #NiUnaMas"

La periodista tuvo que salir del país a causa de estar recibiendo amenazas de muerte y violación por medio de redes sociales.

A través de un comunicado enviado a medios de comunicación, Anonymous informa que son decenas los sitios afectados.

Fuente: http://loquesigue.tv/en-apoyo-a-andrea-noel-anonymous-lanza-campana-masiva-contra-decenas-de-sitios-de-gobierno-niunamas/

Captura policía Cibernética a personas relacionadas en robo de identidad y fraude a servidores públicos

por MARZO 28, 2016 / NSINTESIS

La Policía Cibernética logró identificar y ubicar a Luis V, quien "robó la identidad" del Secretario de Finanzas y Administración de Michoacán y así pretender obtener diferentes cantidades de dinero que solicitó a funcionarios municipales.

Creando un perfil falso a nombre del funcionario estatal Carlos Maldonado Mendoza, estableció contacto con funcionarios municipales de Michoacán a quien les ofreció gestión de recursos para el desarrollo de diversos proyectos, por lo que les solicitó que hicieran el depósito de una garantía en una cuenta personal.

Hasta el momento se tienen ubicados cinco funcionarios municipales que contactó Luis V, además de que el mismo imputado manifestó que ya había creado un perfil de un servidor público de la Ciudad de México para contactar a servidores públicos de la entidad.

Fuente: http://www.nsintesis.com/sucesos/captura-policia-cibernetica-a-persona-relacionada-en-robo-de-identidad-y-fraude-a-servidores-publicos/

NEGOCIOS

Una de cada tres empresas en México, sufre de delitos económicos

por MARZO 29, 2016 / EL FINANCIERO

Según la encuesta realizada por PwC, el 37% de las organizaciones ha sido víctima de delitos económicos en México en los últimos dos años.

Los delitos más cometidos son la malversación de activos con 76%, soborno y corrupción con 21%, y el fraude en adquisiciones y uso indebido de información privilegiada con 19%.

Los sectores más afectados son el de transportación y logística con 70%, la industria de ventas al detalle con 55%.

La industria manufacturera reportó 44% y servicios financieros 42%. El 64% de los fraudes fueron realizados por un defraudador interno con antigüedad de tres a cinco años; mientras que 25% fue hecho por alguien externo a la empresa.

Si bien un menor porcentaje de organizaciones reportaron haber sufrido pérdidas de hasta 100 mil dólares por crímenes cibernéticos respecto a la misma encuesta de 2014, el porcentaje de empresas con pérdidas mayores que llegan hasta los 100 millones de dólares, aumentó entre uno y dos puntos porcentuales.

Este mismo caso se vio en los ataques con un valor de entre un millón y cinco millones, en donde el mismo periodo aumentó un punto porcentual al pasar de 2% a 3%.

Fuente: http://www.elfinanciero.com.mx/economia/una-de-cada-tres-empresas-sufre-delitos-economicos.html

OPINIÓN

Horacio Azzolin, opinión sobre amenazas cibernéticas

por MARZO 31, 2016 / TWITTER

Horacio Azzolin, Fiscal de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), en Buenos Aires, Argentina, publicó en Twitter:

"Las amenazas cibernéticas son hoy casi tan graves como las amenazas terroristas, y en el futuro tal vez las superen"

Esto por la reunión de: "Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?" que estuvo a cargo del Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA).

Fuente:
https://twitter.com/horacioazzolin/status/715534824820355072

TOTALSEC NEWSLETTER - INFOSEC

BOLETÍN No. 7

02 ABRIL – 10 ABRIL, 2016

Elaboración: ABRIL 11, 2016.