
# NEWSLETTER – INFOSEC MX

BOLETIN No. 15

MAYO 28 – JUNIO 05

Elaboración: Junio 06, 2016

## GOBIERNO

***En este número encontrarás noticias sobre:***
*- Gobierno*
*- Banca*
*- Tecnología*

## Senado mantiene estancada iniciativa sobre el delito de robo de identidad

por MAYO 29 2016 / REVOLUCION TRES PUNTO CERO

Pese a presiones por sancionar el robo de identidad, que es uno de los delitos que más aquejan a la sociedad mexicana teniendo graves consecuencias para usuarios de servicios financieros, el Senado mantiene congelada una iniciativa para castigar hasta con 15 años de cárcel dicho delito. Desde octubre del 2013, las comisiones de Hacienda y Estudios Legislativos Primera, tienen pendiente la discusión de una reforma a la Ley de Instituciones de Crédito.


También se propuso la sanción a personas que, por cualquier medio, se apoderen, usen o aprovechen datos personales, informaciones o documentos de personas físicas para hacerse pasar por el titular de los datos personales. Incluyendo utilizar de manera ilegal la información para obtener un crédito, realizar un pago, financiamiento, lucro indebido o que implique derechos y obligaciones legales.

**Fuente:** http://revolucionestrespuntocero.com/senado-mantiene-estancada-iniciativa-sobre-el-delito-de-robo-de-identidad/

# BANCA

## Bancos protegen a los clientes del robo de identidad

por MAYO 30, 2016 / DIARIO EN IMAGEN

Ante esta problemática, cada banco evalúa las medidas que habrá de implementar para garantizar la seguridad de sus clientes, pues a la fecha no se han definido estrategias que pudieran adoptarse a nivel sector. De acuerdo con datos de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), del 2011 al 2015 el número de quejas ante el organismo por posible robo de identidad ha pasado de 4 mil a 10 mil, propiciando pérdidas por más de 260 millones de pesos.

Según Luis Niño de Rivera, no hay una cifra conjunta de la banca, ya que cada banco invierte por su cuenta y no comparten esa información, pero son varios millones de dólares invertidos por cada banco para desarrollar estos sistemas. Agregó reconocer una limitante en México, que es el que no existe un documento nacional de identidad, por lo que los bancos tienen que utilizar la credencial de elector o el pasaporte como identificación.

**Fuente:** http://www.dineroenimagen.com/2016-05-30/73609

## Sufren ciberataques 53% de las bolsas del mundo

por JUNIO 01, 2016 / FORBES


Jimena Mora Corredor, directora jurídica de Propiedad Intelectual y Seguridad Digital de Microsoft, advirtió que aproximadamente el 53% de las bolsas de valores del mundo son víctimas de algún ciberataque. El sector financiero mexicano está siendo atacado desde Europa del Este y América Latina, yendo los ciberdelincuentes sobre las cadenas productivas, y las empresas.

3 de cada 5 PyMES han sufrido estos ataques con robo de datos personales y financieros, así como bases de datos de clientes, que se venden en el mercado negro. Ante la pregunta de que, si Microsoft ha detectado ataques cibernéticos para especular en contra del peso, como lo advirtió Banco de México, la respuesta de Mora Corredor fue: "Concretamente no", pero saben que las entidades financieras han tomado todas las medidas necesarias para prevenir y combatir el delito.

**Fuente:** http://www.forbes.com.mx/sufren-ciberataques-53-las-bolsas-valores-del-mundo/

## TECNOLOGÍA

# Ciberataques infectan casas y hasta autos de 11 millones en México

por JUNIO 02, 2016 / PUBLIMETRO

Un estudio hecho por Fortinet, reportó que estos ataques en México se elevaron un 700% entre 2015 y 2016, con un aumento de 100 mil a 800 mil agresiones en 12 meses, y han afectado a más de 11 millones de mexicanos, logrando además penetrar las pantallas, los electrodomésticos y hasta la computadora de los coches que cuentan con conexión web, pasando del séptimo al quinto puesto en generación y ataques cibernéticos a nivel mundial.

Esto puede representar un riesgo grave para la integridad y hasta vida de los dueños de un vehículo, sus familias y los ocupantes. Uno de cada seis dispositivos muestra contenido o rastros de algún virus o código malicioso, la mayor parte de estas afectaciones están en la Ciudad de México, Guadalajara y Monterrey.

**Fuente:** http://www.publimetro.com.mx/economia/ciberataques-infectan-casas-y-autos-de-11-millones-de-mexicanos/mpfb!mj3vxOKfZV8Tg/


# Buscan PROFECO y AMIPCI blindar e-commerce

por MAYO 26, 2016 / EL UNIVERSAL

La Asociación Mexicana de Internet (AMIPCI) y la Procuraduría Federal del Consumidor (PROFECO), firmaron un convenio para trabajar en conjunto y establecer mecanismos de autorregulación del comercio electrónico en el país. La AMIPCI continuará revisando que los sitios web contengan disposiciones que cuiden a los consumidores a través de los esquemas de autorregulación existentes, para brindar certeza jurídica a los internautas en las transacciones mercantiles en línea.

Además, habrá intercambio de información entre ambas instituciones en caso de ser necesario, para que la PROFECO investigue y sancione las irregularidades encontradas. AMIPCI estima que para los siguientes 12 meses las compras en línea serán de un 33%, mientras que las ventas por internet alcanzarán un 25%.

**Fuente:** http://eluniversal.com.mx/articulo/techbit/2016/05/26/buscan-profeco-y-amipci-blindar-e-commerce

# Malware y Phishing, incidentes de Seguridad más frecuentes en Latinoamérica

por MAYO 26, 2016 / PC WORLD EN ESPAÑOL

ESET, presentó el ESET Security Report 2016, un estudio de encuestas realizadas a más de 3,000 profesionales de organizaciones de Argentina, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú y Venezuela. Arrojando que el 40% de las empresas sufrieron un incidente con malware en el último año y el 16% con el phishing.

Siendo los países más afectados: Nicaragua con el 58.3%, seguido de Guatemala con el 55.8% y Ecuador con 51.9%. Mientras que Argentina con el 29.7%, Chile 29.2% y Venezuela 24.1% fueron los menos afectados por casos de malware en las empresas. La mayor preocupación de las empresas son las vulnerabilidades de software y sistemas con el 58%, el malware con el 54% y el acceso indebido a la información con el 46%. La concientización en temas de Seguridad es fundamental, sólo el 49% de las empresas lo aplican.

**Fuente:** http://www.pcworldenespanol.com/2016/05/26/malware-phishing-incidentes-mas-frecuentes/


# Apple contrata a cofundador de Silent Circle para reforzar la Seguridad

por MAYO 26, 2016 / COMPUTER WORLD MEXICO

Jon Callas, cofundador de Silent Circle, empresa que fabrica el Blackphone, ha sido contratado nuevamente por Apple para una función que no ha sido revelada, pero deja entrever que podría colaborar con los de Cupertino. Callas fue también cofundador de PGP Corporation, trabajó en Apple de 1995 a 1997 y después entre 2009 y 2011. Tiene dos patentes a su nombre en esa segunda etapa que se centró en encriptación de disco, que usa Apple en sus smartphones, tablets y computadoras.

Su contratación está enfocada en la encriptación, esto tras la serie de demandas que ha interpuesto el FBI para forzar a la compañía a desbloquear iPhones bajo la ley por la que pueden acceder a sus contenidos.

**Fuente:** http://computerworldmexico.com.mx/apple-contrata-a-cofundador-silen-circle/

## Pueden atacar en minutos un teléfono a través de los puntos de carga móviles

por MAYO 30, 2016 / SEGURIDAD UNAM

Investigadores de la firma de seguridad Kaspersky Lab, encontraron que pueden instalar una aplicación como un virus en un teléfono mediante la conexión USB a una computadora, además vieron que teléfonos Android y iOS probados, filtraron una gran cantidad de datos privados a las computadoras donde se conectaron mientras cargaban, incluyendo el nombre del dispositivo, fabricante, tipo, número de serie e incluso una lista de archivos.

Recomiendan sólo conectar el teléfono en computadoras verificadas, empleando también cables USB verificados, no desbloquearlo mientras carga, usar aplicaciones que usan cifrado como WhatsApp y iMessage para comunicarse, usar antivirus y actualizar el sistema operativo móvil a la versión más reciente.

**Fuente:**
http://www.seguridad.unam.mx/noticia/?noti=2889&utm_content=buffer1693d&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer


## Lo más peligroso de un ataque de DDos no es la pérdida de dinero, sino de reputación

por MAYO 26, 2016 / SILICON

En una encuesta hecha con la ayuda de B2B International, dio como resultado que la pérdida económica no es la más grave, sino que debido a que se trata de una forma tan visible de ataque, la reputación de una empresa y su credibilidad de cara a los clientes es lo que más afecta a las compañías.

La pérdida de clientes por daños en reputación, se repite como el peor de todos los efectos por casi 4 de cada 10 empresas. Un 37 % ha sufrido una pérdida de confianza por parte de sus clientes por esta causa. Y sólo el 28 % nombra el costo de mantener los ataques DDoS controlados o de recuperarse de ellos tras sufrirlos. Y el 26 %, apunta al tiempo de inactividad y a la caída de ingresos derivada de dicho ataque. Estos ataques podrían causar daños desde 53 mil a 417 mil dólares según la empresa.

**Fuente:** http://www.silicon.es/lo-mas-peligroso-de-un-ataque-ddos-no-es-la-perdida-de-dinero-sino-de-reputacion-2309579?utm_content=buffer59c4d&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer#KiBSEx4i37GuHSDv.99

# El ransomware CERBER evoluciona incorporando ataques DDos

por MAYO 23, 2016 / ZONA VIRUS

Además de la función de cifrado de archivos y bloqueo de pantalla, esta amenaza una vez puesta en marcha, envía paquetes de red hacia una subred externa, comportamiento normal de robots DDoS, esto es visto por primera vez en un ransomware. Este malware se difunde a través de documentos en formato .rtf pero no es demasiado sigiloso, ya que es detectado por 37 de los 57 motores de VirusTotal.

Los documentos .rtf activan la función de macros en Office y después ejecutan un VBScript malicioso que descarga y ejecuta el malware. El ransomware en sí, se ejecuta cifrando los datos del usuario y bloqueando la pantalla, para que después un segundo código malicioso binario llamado 3311.tmp también se ponga en marcha y envíe una gran cantidad de datos a través de la Red de la PC infectada. Se teme que se pueda convertir en una nueva tendencia, ya que el alquiler de botnets DDoS en la Deep Web, es un negocio muy lucrativo.

**Fuente:** http://www.zonavirus.com/noticias/2016/el-ransomware-cerber-evoluciona-incorporando-ataques-ddos.asp?utm_content=buffer3e637&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

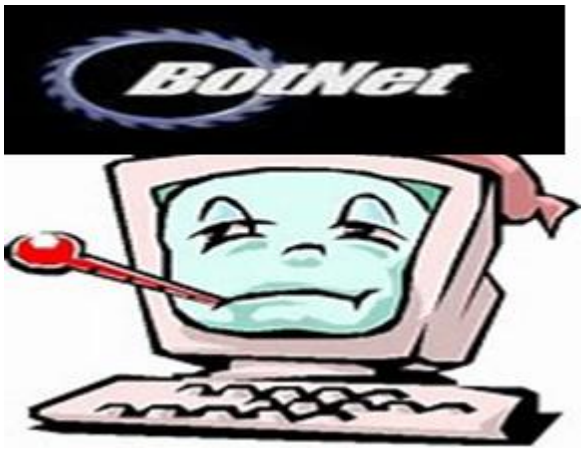

# Botnet infecta a casi un millón de computadoras a través de secuestros de clics

por MAYO 18, 2016 / SEGURIDAD UNAM

Según BitDefender, los responsables de esta botnet ganan dinero a través de Google AdSense para la búsqueda programada. Este programa es para dueños de sitios web que les permite colocar un motor de búsqueda personalizado en sus sitios web, generando ingresos cuando los usuarios hacen clic en los anuncios que aparecen en la búsqueda. Pero en vez de eso, los operadores de la botnet interceptan las búsquedas de Google, Bing y Yahoo hechas por los usuarios, remplazando los resultados por unos generados por su motor de búsqueda personalizada con el programa malicioso que BitDefender detecta como Redirector.Paco.

El malware está incluido en instaladores modificados para programas como WinRAR, Connectify, YouTubem Downloader, Stardock Start8, y KMSPico. Hay dos tipos de este malware, uno en el que el archivo PAC y el proxy están alojados en un servidor remoto y otro donde se almacena en la computadora de forma local.

**Fuente:**
http://www.seguridad.unam.mx/noticia/?noti=2871&utm_content=bufferd3376&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer



# TOTALSEC NEWSLETTER – INFOSEC

BOLETÍN No. 15

MAYO 28 – JUNIO 05, 2016

Elaboración: JUNIO 06, 2016

totalsec
Security Operation Center