NEWSLETTER – INFOSEC MX

BOLETIN No. 33

Octubre 01- 09

Elaboración: Octubre 10, 2016

Uno de cada 120 smartphones se infectan de virus: Nokia

por OCTUBRE 03, 2016 / EL ECONOMISTA

Según Nokia, en la primera mitad del año, a nivel global 1 de cada 120 smartphones estuvo infectado por algún virus, las infecciones de los dispositivos móviles se incrementaron en 96% en la primera mitad del 2016, alcanzando su máximo histórico en abril. Las infecciones en smartphones casi se duplicaron entre enero y julio, comparado con la segunda mitad de 2015. El reporte también señaló la aparición de nuevo y más sofisticado malware que puede ser más difícil de detectar y remover.

Kevin McNamee, jefe del Laboratorio de Inteligencia de Amenazas de Nokia, dijo que actualmente los atacantes tienen como objetivo un rango más amplio de aplicaciones y plataformas, incluyendo los juegos móviles más populares y los nuevos dispositivos IoT, y también están desarrollando formas de malware más sofisticadas y destructivas. Tan solo en abril de este año, las infecciones alcanzaron un máximo histórico, con 1.06% de dispositivos afectados por malware, que incluye ransomware, aplicaciones de espionaje telefónico, troyanos SMS, robo de información personal y adware agresivo.

Fuente: : **http://eleconomista.com.mx/tecnociencia/2016/10/03/cada-120-smartphones-se-infectan-virus-nokia?utm_content=buffer2baae&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

Tres nuevas formas de hackeo que acechan a las empresas

por SEPTIEMBRE 30, 2016 / FORMATO7

Para las empresas, el riesgo es latente al incorporar el internet de las cosas, ya que sus redes no están protegidas y monitoreadas para prevenir un ciberataque si los hackers utilizan gadgets o aplicaciones externas para introducirse en sus redes a través de dispositivos inteligentes. Un Centro de Investigación mostró cómo un drone, equipado con un smartphone con aplicaciones como security patrol, para interceptar señales de WiFi, podía utilizarse para manipular el tráfico hacia impresoras inteligentes dentro de un corporativo y robar material clasificado. En una conferencia, se mostró al drone Danger Drone, equipado con una mini computadora Raspberry Pi, con la que sin utilizar aparatos externos el drone intercepta otras señales.

Se estima que para 2020 existan 50,000 millones de cosas conectadas a la red teniendo un valor de 1.4 billones de dólares; en los dos últimos años, los ataques cibernéticos relacionados al Internet de las Cosas crecieron 458% según AT&T. Otras cosas conectadas como aspiradoras o televisiones pueden ser usadas para esconder computadoras o sensores que intercepten señales, hasta objetos externos a una empresa, como las cámaras de vigilancia en las calles, pueden ser vulneradas para después de ahí infectar otras redes, los switches o routers de internet también pueden ser hackeados y usados para tomar escaneos virtuales de un lugar en los que se puede determinar, por ejemplo, cuántas personas hay en un lugar.

Fuente: **http://formato7.com/2016/09/30/tres-nuevas-formas-hackeo-acechan-las-empresas/**

Tips para evitar ciberataques internos

por OCTUBRE 04, 2016 / COMPUTER WORLD MEXICO

Ante este tipo de ciberamenazas, los directivos son cada vez más conscientes e intentan tomar todas las medidas que sean necesarias para evitar un hackeo externo, ya que cualquier trabajador podría colaborar con un ciberdelincuente para robar documentos confidenciales o legales. Con sólo proveer al empleado de un USB cargado de malware diseñado para extraer información del sistema deseado. Este ataque no debería de ocurrir si una organización está bien estructurada en cuanto a seguridad.

Los departamentos donde haya información delicada deben estar aislados de cualquiera que no forma parte de ellos, tener contraseñas en los equipos de cómputo y archivos encriptados son algunas de las prudencias que una organización debe tener para impedir que sus propios empleados roben documentación sensible. Los departamentos de las compañías deben estar preparadas para poder detectar si alguien está copiando, descargando o eliminando documentación importante. Además de requerir una contraseña cuando se quiera manipular algunos de esos archivos sensibles, nadie debe ser capaz de utilizar el almacenamiento USB ya que se controla fácilmente con una apropiada configuración de Windows. Y si se permite el uso, todos los datos escritos en esa deben estar encriptados para que el acceso a esos archivos sea difícil o imposible.

Fuente: **http://computerworldmexico.com.mx/tips-evitar-ciberataques-internos/**

¿Qué pueden hacer los hackers con una identidad robada?

por SEPTIEMBRE 28, 2016 / EL UNIVERSAL

Según un reporte de Norton, el 60% de los usuarios en Internet asegura que tenía mayor control sobre su información antes de la proliferación de teléfonos inteligentes. De los casi 20 millones de afectados por el cibercrimen en México, el 6% ha sufrido el hackeo de su información realizando compras en un centro comercial y el 12% ha sido víctima de fraudes a través de su tarjeta de crédito. Muchos usuarios lo consideran menos peligroso porque piensan que su historial financiero no es atractivo para los cibercriminales.

Actividades de un ciberdelincuente con una identidad robada: Comprar o solicitar servicios con la tarjeta de crédito de la víctima, robar cuentas o generar deudas para el propietario original, solicitar tarjetas de crédito y cuentas bancarias con los datos de las víctimas con documentos falsos y utilizando a una persona llamada para presentarse físicamente en el banco, obtener un nuevo teléfono con el nombre y datos de otra persona (para continuar con la actividad criminal y no ser rastreado por la policía), utilizar la identidad de otra persona para comprar bienes raíces y solicitar puestos de trabajo. En el peor de los casos, los cibercriminales pueden cometer algún delito ensuciando la reputación de la víctima. Se recomienda comprobar las cuentas bancarias con frecuencia, estar alerta ante cargos bancarios y correspondencia inesperada.

Fuente:
http://eluniversal.com.mx/articulo/techbit/2016/10/4/que-pueden-hacer-los-hackers-con-una-identidad-robada

Banxico insta a perseguir ciberdelitos financieros

por OCTUBRE 03, 2016 / EL UNIVERSAL

Ante el incremento de ataques cibernéticos al sistema financiero del país, el Banco de México reconoció que es necesario que estos delitos se persigan por ley como parte de la estrategia de combate a esta actividad delictiva. Alan Elizondo, director general de Asuntos Financieros del Banco de México, dijo que estos fraudes están creciendo a mayor velocidad. De la mano de la Comisión para la Protección y Defensa de los Servicios Financieros (Condusef) se ha platicado acerca de este riesgo, teniendo al igual que la Comisión Nacional Bancaria y Condusef el reto de que con nuestras facultades irlo mitigando o ponerles a clientes mayores herramientas para evitarlo.

realice sus operaciones cuente con un mecanismo para cubrirse en caso de que ocurra una eventualidad. Las bandas delictivas están incurriendo en esta actividad ante la imposibilidad de que se les acuse de un delito grave. Desde el punto de vista del banco es importante que siempre que el cliente interactúe con la institución a través de canales formales tenga mecanismo de recuperarse en caso de malas prácticas.

Fuente:
http://www.eluniversal.com.mx/articulo/cartera/finanzas/2016/10/3/banxico-insta-perseguir-ciberdelitos-financieros

Hackers atacan a mexicanos: 600 mil ataques cibernéticos registrados en agosto

por OCTUBRE 05, 2016 / WEBADICTOS

PSafe reportó un registro de 327,835 ataques cibernéticos en dispositivos móviles. La cifra podría ser aún más elevada; ya que este número sólo corresponde a ataques reportados. México es el segundo país con mayor penetración de teléfonos móviles en América Latina con un 82%, debajo de Argentina con un 86%. En el país, los internautas que se conectan desde sus dispositivos móviles son alrededor de los 36 millones, mientras que los que se conectan desde equipos de escritorio son 42 millones.

Las 5 entidades que registran mayor número de ataques durante el mes de agosto 2016 en México son: CDMX con 327,835 ataques, Estado de México con 86,934 ataques, Jalisco con 74,888 ataques, Nuevo León con 67,135 ataques y Puebla con 65,734 ataques. Y los tres ataques por malwares más comunes durante agosto 2016 fueron por Troyanos con 756,725 ataques, Adware con 248,888 y Riskware con 51,840.

Fuente: **https://webadictos.com/2016/10/05/hackers-atacan-mexicanos-600-mil-ataques-ciberneticos-registrados-agosto/**

Se filtra la base de datos con los 68 millones de cuentas robadas de Dropbox

por OCTUBRE 04, 2016 / REDES ZONE

En el 2012, Dropbox sufrió un incidente de seguridad que se ha saldado con 68 millones de cuentas robadas, ahora el "dump" de dicha base de datos robada de Dropbox ya se encuentra disponible en Internet y cualquiera la puede descargar. En agosto, Dropbox estaba reseteando las contraseñas de una gran cantidad de usuarios, y cuando un servicio de Internet resetea las contraseñas de sus usuarios es porque han sufrido un incidente grave de seguridad, aunque lo nieguen.

El mes pasado un ciberdelincuente vendía la base de datos de cuentas robadas en la web profunda por un precio de 1200 dólares (24 mil pesos aprox.), pero, un investigador de seguridad ha subido esta base de datos gratuitamente. El portal Have I Been Pwned obtuvo esta base de datos para actualizar su servicio, y que cualquier pudiera comprobar si su correo electrónico estaba afectado por el incidente de seguridad. Aunque Dropbox utiliza una gran cantidad de medidas de seguridad para proteger las contraseñas de sus usuarios, no ha impedido que se filtre la base de datos.

Fuente **http://www.redeszone.net/2016/10/04/se-filtra-la-base-datos-las-68-millones-cuentas-robadas-dropbox/?utm_content=bufferefb76&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

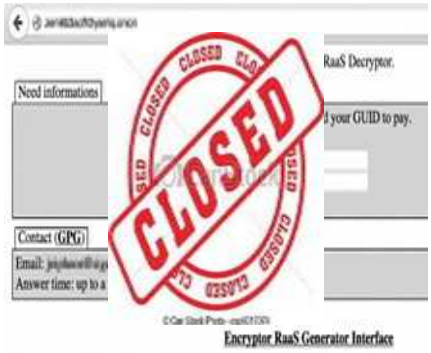
El propietario del ransomware Bitter cierra el negocio y borra las claves de decifrado

por OCTUBRE 01, 2016 / REDES ZONE

El propietario de Bitter ha tomado la decisión de realizar un borrado de todos los contenidos del servidor, incluidas las claves generadas de los equipos que la amenaza había infectado. El problema es que este software ya se había puesto a la venta, en la actualidad el servidor de distribución ha sido desmantelado, pero el problema, es que ya que existe otro que afecta de forma directa a los usuarios. Expertos indican que el propietario de la amenaza cometió un error bastante grave, dejando al descubierto a pesar de estar en la red Tor el servidor que poseía la herramienta para llevar a cabo el descifrado de la información, por lo puede ser este otro de los motivos de esa decisión.

Su distribución continuará en el mercado negro, al igual que sucede con otras amenazas. Y es que son muchas las que han adquirido este modelo de negocio, quitándose los propietarios presión de las autoridades que ahora recae sobre los compradores y los mercados improvisados en el lado oscuro de Internet. Los propietarios de la amenaza además de desactivar el servidor han procedido al borrado de las claves que se habían generado hasta el momento significando que los usuarios que se hayan visto afectados por la amenaza van a tener muy complicado recuperar el acceso a los archivos, sobre todo si no poseen una copia de seguridad o un punto de restauración del sistema operativo Windows.

Fuente: **http://www.redeszone.net/2016/10/01/propietario-del-ransomware-bitter-cierra-negocio-borra-las-claves-descifrado/?utm_content=buffer39c39&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**



Los criminales detrás del ransomware CryptoWall han disminuido sus beneficios

por SEPTIEMBRE 30, 2016 / SILICON

Durante los 10 primeros meses de 2015, la versión CryptoWall 3 había infectado a cientos de miles de víctimas, consiguiendo unos ingresos estimados de 325 millones de dólares (6 mil millones de pesos aprox.). Sin embargo, de noviembre de 2015 a junio de 2016, la última versión, CryptoWall 4, ha cosechado en torno a 18 millones de dólares (350 millones de pesos aprox.).

Los autores de CryptoWall han mostrado su perseverancia creando la cuarta versión del ransomware con características avanzadas, pero CW4 ha sido menos perjudicial. Los grupos que utilizan CryptoWall han multiplicado sus intentos de infectar a los usuarios, pero ha habido una disminución de los daños. La Cyber Threat Alliance (CTA), ha detectado 7,2 millones de intentos de ataques con solo 36.114 víctimas confirmadas, lo que ha supuesto un 0,5% de tasa de éxito, mucho más baja que la tasa de dos dígitos del año pasado.

Fuente: **http://www.silicon.es/los-criminales-detras-del-ransomware-cryptowall-ven-caer-ganancias-2319427?utm_content=bufferf3f8e&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

Redes: 73% de las empresas utilizan dispositivos vulnerables

por SEPTIEMBRE 29, 2016 / CIO LATINOAMERICA

El 73% (más de 250) de las empresas consultadas están utilizando equipos de red al final de su vida útil, haciéndolos completamente vulnerables a los ataques de cualquier código malicioso reciente. El director de prácticas de Cisco, David Vigna, destacó que la revisión realizada por Softchoice a 212.000 dispositivos de redes Cisco, debe ser vista como una señal de alarma. Los dispositivos que se encuentran al final de su vida aumentaron del 4 al 6% en 2015, y 23% de estos dispositivos de redes ya están obsoletos. Si bien la cifra anterior está por debajo del 51% registrado un año antes, los proveedores de estos equipos normalmente dejan de brindar soporte a los dispositivos de dos a cinco años después de dejar de venderlos.

Destacó que las empresas podrían no estar conscientes de que algunos de sus equipos ya han pasado su fecha de vencimiento. Los dispositivos ubicados en el perímetro de una red corporativa (firewalls y sistemas de detección de intrusos representan un peligro particular) incluso si son relativamente nuevos. Con la velocidad a la cual las cosas cambian en tecnología, es recomendable estar atentos mirando su sustitución un poco más a menudo.

Fuente: **http://www.cioal.com/2016/09/29/redes-73-de-las-empresas-utilizan-dispositivos-vulnerables/?utm_content=buffere6c96&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

TOTALSEC NEWSLETTER – INFOSEC

BOLETÍN No. 33

Octubre 01- 09, 2016

Elaboración: Octubre 10, 2016

totalsec