NEWSLETTER – INFOSEC MX

BOLETIN No. 38

Noviembre 05- 13

Elaboración: Noviembre 14, 2016

"El Rostro" del malware que ataca a empresas de energía

por NOVIEMBRE 09, 2016 / EL FINANCIERO

Durante el 2015, el 43% de las empresas de minería, gas y petróleo fueron atacadas por lo menos una vez. Según Fernando Ramírez de Cisco, las ventas de los productos de solución antimalware de Cisco, que están siendo adoptados por el gobierno, empresas de energía, la industria, entre otras, crecen de 300 a 400% trimestre tras trimestre. Algo que caracteriza a estas amenazas cibernéticas, que perder anualmente 445 mil millones de dólares a la economía Mundial, es que son silenciosas, el usuario no percibe que su ordenador o dispositivo está infectado, haciendo establecer una relación prolongada.

El ámbito energético es una infraestructura crítica del país, y está bajo constante amenaza de hackers pero también de otros países. La industria energética es muy competitiva en entidades que están muy conectadas al gobierno central y por eso son targets directos de los hackers que quieren vender la información (para los mayores clientes) de cuáles son los niveles de producción, costos de producción, inventarios, y por eso están constantemente bajo ataque. Empresas de energía como Exxon Mobile, invierten cientos de millones de dólares en ciberseguridad, y en el caso de Pemex, a pesar de que hay inversión, no queda muy claro cuan efectivas han resultado.

Fuente: **http://www.elfinanciero.com.mx/tech/el-rostro-del-malware-que-ataca-a-empresas-de-energia.html**

Malware afecta a Android por vulnerabilidad en el navegador

por NOVIEMBRE 09, 2016 / CIO MEXICO

El Troyano de banca móvil Svpeng, que estaba escondido en la red de publicidad AdSense de Google, está diseñado para robar información de tarjetas bancarias, recopila el historial de llamadas, mensajes de texto y multimedia, favoritos del navegador, así como contactos. Se ejecuta en la versión móvil del navegador Chrome, y ataca principalmente a los países de habla rusa, pero tiene el potencial de propagarse a nivel mundial. La campaña comenzó con un anuncio infectado colocado en Google AdSense que se mostraba habitualmente en páginas web no infectadas, y el troyano se descargaba cuando el usuario accedía a la página mediante el navegador Chrome en un dispositivo Android.

Cuando un archivo APK se descarga en un dispositivo móvil a través de un enlace web externo, el navegador muestra una advertencia de ser un objeto potencialmente peligroso. En este caso, los estafadores encontraron una falla de seguridad que permitía a los archivos APK descargarse sin notificar a los usuarios Se recomienda actualizar el navegador Chrome para Android, instalar una solución de seguridad eficaz y estar al tanto de las herramientas y técnicas usadas por los cibercriminales que intentan engañar a los usuarios para instalar software malicioso y aceptar derechos de dispositivo.

Fuente: **http://cio.com.mx/malware-afecta-a-android-por-vulnerabilidad-en-el-navegador/**

Reconocimiento del iris, el gran reto de la autenticación

por NOVIEMBRE 09, 2016 / CIO MEXICO

La tecnología biométrica basada en el reconocimiento del iris se está consolidando como la alternativa de seguridad que brindará más confianza, pero también se concibe como factor extra de autenticación por el bien de usuarios y empresas. Las contraseñas dada su fragilidad están condenadas a desaparecer, esto por los tiempos que corren, por el aumento de las amenazas, por la sofisticación de su naturaleza y por el deseo de los usuarios de preservar su seguridad lo máximo posible.

Por la complejidad de este escenario en cuanto al uso masivo de aplicaciones personales y profesionales para trabajar o para realizar gestiones, diversificación de la utilización de dispositivos móviles para manejar dichas aplicaciones, un estilo de vida más móvil. Y dos consecuencias contrapuestas: uso de contraseñas cada vez más complejas y difíciles de recordar, o bien otras que cualquier ciberdelicuente podría descifrar en cuestión de segundos.

Fuente: **http://cio.com.mx/reconocimiento-del-iris-el-gran-reto-de-la-autenticacion/**

Internet de las cosas, nueva fuente de acceso para hackers

por NOVIEMBRE 08, 2016 / COMPUTER WORLD

El Internet de las Cosas y los hogares conectados, pueden ser una mina de oro para los atacantes, según Hervé Lambert, retail product manager de Panda Security. Quien agregó que todos los dispositivos que hay conectados a Internet en una casa, son un potencial ejército de zombies cargados de virus esperando a que un ciberdelincuente los despierte, si no se cuenta con un sistema de seguridad que los vigile y los proteja a todos.

Por lo que dio a conocer varios métodos que podrían utilizar los ciberdelincuentes para secuestrar los dispositivos y que podrían ser una fuente de problemas para los usuarios que se conectan a esta nueva ola de innovación. Situaciones que pueden empezar a ser una realidad para los early adopter y parece que en 2020 la mayoría de las casas tendrán muchos de sus objetos conectados a la red, por lo que los hackers podrían encerrarte hasta pagar el dinero que piden, encender las alarmas, cambiar el pedido de la compra, hacer explotar a la aspiradora, abrir el automóvil, o peor aún, conducirlo por ti.

Fuente: **http://computerworldmexico.com.mx/internet-las-cosas-nueva-fuente-acceso-hackers/**

Google pondrá sitios web peligrosos reincidentes en una larga "cuarentena"

por NOVIEMBRE 08, 2016 / CNET

Google se ha dado cuenta de que algunos sitios Web maliciosos que son etiquetados como tales para que los usuarios no entren en ellos están limpiando sus registros solo el tiempo necesario para recibir la aprobación de la empresa y el respaldo de la etiqueta de Navegación Segura. Por lo que, la empresa ha añadido una nueva clasificación a su iniciativa de Navegación Segura, para proteger a los usuarios de estos sitios maliciosos, por lo cual ahora, aunque hayan salido de esa "cuarentena", la empresa continuará recordando que son sitios que han estado expuestos al peligro.

La Navegación Segura empezará a clasificar estos tipos de sitios como Infractores Reincidentes. Por lo que hay que tener en cuenta que los sitios web que son hackeados no serán clasificados como reincidentes; sólo los sitios que publican contenido nocivo a propósito estarán bajo esta política. Y una vez que son clasificados como "Infractores Reincidentes", los sitios webs no podrán solicitar una revisión hasta pasados 30 días, por lo que durante ese tiempo los usuarios seguirán viendo mensajes de advertencia del riesgo que significa visitar este sitio.

Fuente: **https://www.cnet.com/es/noticias/google-sitios-webs-peligrosos-reincidentes/?utm_content=buffer3f7e8&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

La falta de profesionales calificados retrasará el crecimiento de IoT en 2017

por NOVIEMBRE 07, 2016 / COMPUTER WORLD MEXICO

La tecnología IoT utiliza nuevos protocolos de red, hardware y software especializado, y la puesta en marcha de este proyecto se requiere experiencia en transformación de negocios, analítica de datos, ciberseguridad y automatización industrial. La seguridad es compleja dada la doble amenaza que IoT representa: El volumen de dispositivos conectados incrementa los puntos de ataque de una empresa y los hackers pueden explotar vulnerabilidades de dispositivos IoT para lanzar otros ataques. La experiencia en redes también será un desafío, ya que la gama de tecnologías y protocolos inalámbricos necesarios para soportar las implementaciones de IoT se multiplica más allá de las conexiones de Bluetooth, WiFi y móviles.

El tráfico constante de pequeñas ráfagas, el denso conjunto de conexiones o las largas distancias requieren nuevas conexiones inalámbricas, como LoRaWAN, Sigfox o 3GPP de banda estrecha (NB). En 2017, los equipos buscarán más de 20 opciones de conectividad inalámbrica y protocolos para soportar el conjunto de dispositivos de IoT de una compañía. Las condiciones requerirán que el software IoT se distribuya a través de dispositivos de pasarelas y servicios en la nube. Para sacar provecho del valor del negocio, los datos de IoT se acoplarán con los servicios cada vez más poderosos de la IA y del cloud de autoaprendizaje capaces de asimilar estos datos.

Fuente: **http://computerworldmexico.com.mx/la-falta-profesionales-calificados-retrasara-crecimiento-del-iot-en-2017/**

Alertan de nuevo phising contra clientes bancarios

por NOVIEMBRE 05, 2016 / PROCESO

Un nuevo phishing fue detectado por la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) que está dirigido a clientes de Banorte. Con esta alerta, suman 14 los casos detectados de correos falsos. El fraude consiste en el envío de correos electrónicos en el que supuestamente la institución bancaria bloquea la cuenta por motivos de seguridad y solicita al cliente llenar un formulario colocado en un link que manda un sitio falso y de ahí roban los datos.

El correo indica que después de llenar el formato, un empleado de Banorte le realizará una llamada para realizar el proceso de verificación y reactivación de la cuenta. La Condusef recordó que ni los bancos, ni Visa o Mastercard, realizan verificación de datos de sus clientes mediante correo electrónico, ni por teléfono, por lo que se debe desechar de inmediato el correo.

Fuente **http://www.proceso.com.mx/461495/alertan-nuevo-phishing-contra-clientes-bancarios**

Las direcciones IPv4 están agotadas, los estándares de red necesitan soportar completamente IPv6

por NOVIEMBRE 03, 2016 / MI AMBIENTE

En septiembre del año pasado, el Registro Americano de Números de Internet informó de que su grupo de direcciones IPv4 en Norteamérica estaba agotado. Ahora, la Junta de Arquitectura de Internet (IAB) afirmó que todas las direcciones IPv4 han sido asignadas y que los estándares de red necesitan soportar completamente IPv6. La adopción mundial de IPv6 se sitúa en el 14,6% de su base de usuarios, y por países, EEUU alcanza casi el 30%; Reino Unido, el 16% y Alemania, el 27%. Los países de Asia-Pacífico se encuentran a la zaga, con Japón liderando el camino en la región con un 14%.

La transición a IPv6 está siendo muy lenta y ha crecido la tendencia de un soporte dual, tanto IPv4 como IPv6. Para facilitar el uso de IPv6, el organismo proporciona ejemplos de IPv6 con futuros dispositivos establecidos para depender del protocolo actualizado de Internet. El IAB espera que el Grupo de Trabajo de Ingeniería de Internet deje de requerir compatibilidad con IPv4 en protocolos nuevos o extendidos para avanzar en la adopción de IPv6. En mayo, Apple anunció que requeriría aplicaciones iOS para dar soporte a IPv6.

Fuente: **http://www.silicon.es/las-direcciones-ipv4-estan-agotadas-los-estandares-red-necesitan-soportar-completamente-ipv6-2322614?utm_content=buffer2f0b4&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

Una campaña de phising de LinkedIn promete mejorar tu seguridad en Internet

por NOVIEMBRE 08, 2016 / REDES ZONE

Usuarios de LinkedIn se han visto afectados por una campaña de correos electrónicos spam en la que los atacantes les indican que han sido seleccionados para llevar a cabo una mejora de la privacidad de su cuenta, y para ello, necesita una copia de una credencial de identidad o de conducir, después de haber enviado esta información, se recibe una segunda notificación en un email, informando que la configuración de su cuenta se ha evaluado y necesita llevar a cabo mejoras. Incluso Dropbox se utiliza para llevar a cabo esta estafa.

El usuario revira correos como si se tratara de la propia red social, invitando al usuario a realizar un proceso de reseteo de la contraseña, apoyándose en que el teórico test de la configuración de la cuenta ha devuelto que esta sería vulnerable. Aunque la página ofrecida es muy similar, hay aspectos que provocan cierta inseguridad, como por ejemplo datos extraños en la parte inferior de la misma o una cuenta de correo como ejemplo que pertenece a una compañía eléctrica. Es un proceso de restablecimiento de la contraseña bastante atípico, ya que primero el usuario debe introducir su dirección de correo y posteriormente la contraseña actual para fijar la nueva, algo que no corresponde con un proceso de reseteo de la cuenta. Los ciberdelincuentes recopilan los dos primeros datos introducidos por el usuario siendo la nueva contraseña introducida un mero trámite para que el proceso resulte mucho más creíble.

Fuente: **http://www.redeszone.net/2016/11/08/una-campana-phishing-linkedin-promete-mejorar-seguridad-internet/?utm_content=buffer61d87&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

Baddie, otro troyano bancario que afecta Android

por NOVIEMBRE 05, 2016 / REDES ZONE

Es capaz de robar los datos de hasta 96 aplicaciones pertenecientes a entidades bancarias, buscando los datos relacionados con tarjetas de crédito. Accede a la información contenida en los mensajes de texto, empleados por muchos bancos para validar las transacciones de sus clientes, además es capaz de saltarse la verificación en dos pasos que se basa en estos mensajes. Fortinet indica que es el troyano bancario más completo que se ha visto. La función estrella consiste en resetear el dispositivo a valores de fábrica sin previo aviso, por lo que el usuario no podría evitar la pérdida de la información. Cuando llega al dispositivo a través de páginas web de aplicaciones, el usuario realiza la instalación y concede permisos de administrador a la amenaza.

Cuando el usuario usa una de las aplicaciones de Baddie, es capaz de comprobar si el número de la tarjeta de crédito introducido es válido o no. La amenaza muestra pantallas sobre las aplicaciones originales simulando sistemas de verificación de VISA y Mastercard. También cuenta con un módulo que es capaz de emular los formularios de muchas aplicaciones, entre ellas, entidades bancarias y principales redes sociales donde lo que los ciberdelincuentes quieren hacer, es el uso de las cuentas de forma ilegítima para difundir la amenaza de una forma mucho más eficaz entre los usuarios.

Fuente:
http://www.aztecanoticias.com.mx/notas/seguridad/264111/agentes-de-la-ssp-cdmx-recibiran-capacitacion-de-corea-del-sur

Un tercio de los ataques cibernéticos a las empresas propseran

por NOVIEMBRE 02, 2016 / SILICON

Las empresas gastan alrededor de 84.000 millones de dólares para evitar el robo de datos, constándoles cerca de 2.000 millones de dólares anuales. Esta cifra podría elevarse a 90.000 millones para el año 2030 si las tendencias continúan según el pronóstico de Accenture. En su investigación entre 2.000 ejecutivos de seguridad de grandes empresas en todo el mundo, revelando que cerca de un tercio de los intentos de vulnerar la seguridad cibernética de las empresas tienen éxito y, a pesar de esto, tres cuartas partes de los ejecutivos siguen confiando en sus estrategias de seguridad.

La alta tasa de fracaso en la defensa de las organizaciones contra los ciberataques se ve agravada por el volumen. Aunque más de la mitad de los encuestados han asegurado que las infracciones internas causan el mayor daño, dos terceras partes han constatado que carecen de confianza en la capacidad de su organización para monitorear las amenazas internas y la mayoría sigue centrándose en la defensa de atacantes externos. La mayoría ha declarado que se necesitan "meses" para detectar brechas de seguridad exitosas y el 17% manifestó que los ataques se descubrieron transcurrido un año o más. El 98% de las infracciones las reportaron empleados fuera del equipo de seguridad.

Fuente:
http://www.seguridad.unam.mx/noticia/?noti=3076&utm_content=buffer08ac1&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

¿Cuáles son los sectores más atractivos para los ciberdelincuentes?

por OCTUBRE 28, 2016 / MUY SEGURIDAD

Según McAfee, los datos más lucrativos para los ciberdelincuentes son los financieros y de propiedad intelectual de las industrias farmacéuticas y biotecnología, que se venden en el mercado negro. El valor de los datos médicos sigue siendo menor que los de cuentas financieras y a la información de las cuentas en el sector de la distribución. El precio de los datos médicos robados está entre los 3 centavos y 2,42 dólares (.61 a 50 pesos aprox.), mientras que los datos financieros cotizan a un precio que puede variar entre los 14 y 25 dólares (286 y 511 pesos aprox.). Por otro lado, los datos pertenecientes a tarjetas de crédito y débito cotizan entre 4 y 5 dólares (81 y 102 pesos aprox.) por registro.

Los desarrollos de las compañías son muchas veces uno de los elementos más valiosos de estas y los cibercriminales lo saben. Intel Security encontró evidencias de que las fórmulas de los medicamentos de última generación, resultados de ensayos de drogas y otra información confidencial tienen un valor añadido en el mercado negro. Además, ha detectado que los mismos ciberdelincuentes están vendiendo y alquilando kits de exploits permitiendo que hackers de poco nivel puedan llevar a cabo ataques. Así mismo, los ciberdelincuentes están reclutando a infiltrados dentro de la industria de la salud y obtener más fácilmente acceso a información valiosa.

Fuente: **sectores-atractivos-ciberdelincuentes/?utm_content=bufferb2213&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

Seguridad de la red ha aumentado considerablemente en un año

por NOVIEMBRE 08, 2016 / DIARIO TI

Google publicó un informe que refleja un fuerte incremento en el acceso a sitios HTTPS mediante el navegador Chrome, recalcando que no es una tendencia transitoria, sino un cambio radical. Google ha estimulado la implementación de HTTPS sitios web, mejorando su posicionamiento en su buscador. Aparte de reforzar la privacidad y seguridad de los usuarios de Internet se incluye el acceso a funcionalidad web más reciente, que para el caso de varios navegadores requiere la utilización de HTTPS. Esto se aplica, entre otras cosas, a procesos secundarios de optimización y geolocalización. La mayor desventaja al implementar HTTPS es su grado de complejidad y uso de recursos en las empresas.

Las estadísticas presentadas por Google reflejan que sólo el 42% de los dispositivos Android acceden a la web mediante conexiones HTTPS, la empresa atribuye esta situación a que estos usuarios utilizan, mucho más que los usuarios de PC aplicaciones dedicadas al visitar servicios que requieren inicio de sesión. El navegador web es utilizado principalmente para leer noticias; y por ahora son pocos los sitios informativos que presenten sus contenidos mediante HTTPS. Mientras, el sistema operativo de Google, Chrome OS, registra un 68% de conexiones HTTPS, en este caso se trata de usuarios que utilizan el navegador para todo tipo de tareas, incluyendo correo electrónico y aplicaciones ofimáticas. Los Usuarios de PC, utilizan software específico para esas actividades.

Fuente:
http://www.seguridad.unam.mx/noticia/?noti=3076&utm_content=buffer08ac1&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

El Mobile Pwn20wn 2016 revela vulnerabilidades en iPhone 6S y Nexus 6P

por OCTUBRE 29, 2016 / HISPA SEC

La edición del MobilePwn2Own 2016 se ha desarrollado en Tokio en la conferencia PacSec, organizado por Zero Day Initiative (ZDI) y Trend Micro. La competencia comenzó con el equipo de Tencent Keen Security Lab atacando un Google Nexus 6P, al lograr instalar una aplicación falsa en todos sus ataques ganaron 102.500 dólares (2 millones 100 mil pesos aprox.) y 29 puntos para el premio Master of Pwn. Además, instalaron una aplicación falsa en un iPhone 6S pero no se mantenía tras el reinicio del teléfono, a pesar de ello, mostraron fallos interesantes a corregir por lo que ganaron 60.000 dólares (1 millón 300 mil pesos aprox.).

Y sobre ese mismo equipo intentaron robar las fotos, y gracias a una combinación de una vulnerabilidad por uso de memoria después de liberarla al mostrar las fotos y un fallo de corrupción de memoria en la sandbox consiguieron extraer una foto del teléfono, ganando otros 52.500 dólares (1 millón 100 mil pesos aprox.) y 16 puntos para el Master of Pwn. Robert Miller y Georgi Geshev de MWR Labs también intentaron instalar una aplicación falsa en un Google Nexus 6P, parece ser que la última actualización del navegador Chrome hizo que su exploit fuera muy inestable, no logrando así un ataque exitoso en los tiempos requeridos. Sin embargo, mostraron desarrollos innovadores adquiridos a través de los canales ZDI habituales.

Fuente: **http://unaaldia.hispasec.com/2016/10/el-mobile-pwn2own-2016-revela.html?utm_content=buffer86581&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

TOTALSEC NEWSLETTER – INFOSEC

BOLETÍN No. 38

Noviembre 05 - 13, 2016

Elaboración: Noviembre 14, 2016

totalsec