TOTALSEC NEWSLETTER – INFOSEC MX

BOLETIN N. 8

ABRIL 09 – 17

Elaboración: Abril 18, 2016

TECNOLOGÍA

En este número encontrarás noticias sobre:
- Tecnología
- Gobierno
- Negocios
- Finanzas

El navegador que usas podría saber todo sobre ti

por ABRIL 06, 2016 / EXCELSIOR

Webkay, es una plataforma que demuestra lo fácil que es tener acceso a la información de cualquier usuario cuando está conectado a Internet.

Su creador dice que se puede acceder a toda esta data sin necesidad de preguntar o pedir permiso, con tan sólo hacer un clic el navegador, despliega todo lo que sabe sobre los usuarios como:

- La localización.
- El software (versión del navegador y extensiones instaladas).
- Hardware.
- La conexión (direcciones IP, proveedor y velocidad de Internet), redes sociales en que se encuentra conectado.
- Click Jacking (identidad del usuario revelada mediante engaños).
- Giroscopio (qué tipo de dispositivo tiene el usuario), Network Scan (busca otros dispositivos) Imágenes (metadatos, información de origen, trayecto y destino de los archivos).

Fuente: http://www.excelsior.com.mx/hacker/2016/04/07/1085110

Ramatien, un malware enfocado a routers y dispositivos de IoT

por MARZO 31, 2016 / GLOBAL CYBERSECERT

Expertos de ESET, han detectado una nueva amenaza que busca infectar routers basados en Linux y dispositivos IoT conectados a la red. Con el nombre de Remaiten, es creado a partir de las amenazas Kaigen y Gafgyt.

Está mejorada y añade nuevas características para ataques más complejos. La versión 2.2 de Remaiten, incluye comandos wget/tftp y tiene binarios para infectar dispositivos de arquitecturas PowerPC y SuperH, pudiendo infectar cualquier dispositivo.

Cuando el malware se ha instalado en el router o dispositivo IoT, permanece ejecutado en primer plano, conectado a su servidor C&C por medio de una interfaz IRC a la espera de órdenes. Todas las conexiones se hacen cifradas, por lo que es difícil detectarlas.

Se centra en buscar nuevas víctimas y realizar ataques de red como ataques de desbordamiento en el router, descargar archivos modificados, hacer barridos de direcciones IP mediante telnet, etc. Se recomienda cambiar la contraseña del telnet por si en caso de ser objetivo de Remaiten, no se pueda conectar a nuestro router.

Fuente: http://www.globalcybersec.com/reader.php?p=1338

Urgen a millores a actualizar Adobe Flash por ciberataque

por ABRIL 08, 2016 / CIOAL

Adobe Systems Inc., lanzó una actualización del software Flash para navegadores de Internet, ya que investigadores descubrieron una brecha de seguridad que estaba siendo utilizada para enviar un virus que afecta con ransomware a computadoras con Windows que visitan sitios web contaminados.

El fabricante de software de seguridad Trend Micro Inc., dijo que ya había advertido a Adobe que había visto explotar las brechas para infectar las computadoras con el ransomware de nombre "Cerber".

Fuente:
http://www.excelsior.com.mx/hacker/2016/04/08/1085427

En México, 8 de cada 10 personas, quieren que se cierre la "Deep Web"

por ABRIL 06,2016 / CODIGO ESPAGUETI

En una encuesta se entrevistaron a 24 mil personas alrededor del mundo, 1000 de ellos mexicanos. En la que el 71% respondió que la deep web debería cerrarse, mientras que en México el 80% responde igual.

Países como la India e Indonesia opinaron lo mismo con un 82% y 85% respectivamente. Kenya, Corea del Sur y Suecia, son los que se colocan con la mayor apertura en torno a la deep web con un 39%.

Este rechazo a la deep web, se debe a que en el sitio se realizan actividades criminales como pornografía infantil, piratería o tráfico de drogas.

Aunque, también es aprovechado para el bien. Softwares como Tor, son utilizados por periodistas y activistas para mover información sensible de manera segura, así como protestar de manera anónima dando da pie a la libertad de expresión.

Fuente:
http://codigoespagueti.com/internet/mexico-contra-deep-web/

Los oscuros términos de Uso de Oculus Rift que la compañía no explica con claridad

por ABRIL 04, 2016 / GIZMODO

Algunos de los Términos de Uso son comunes, como la denegación de servicio por varias razones, terceros pueden recopilar información de tu actividad con el dispositivo.

Ahora Oculus (Facebook), se puede adueñar del contenido creado y puede usarlo cuando quiera.

Siendo una categoría nueva en el mercado, abre todo un abanico de posibilidades y usos diversos.

Un desarrollador creativo podría realizar algún proyecto interactivo y Oculus podría usarlo para un anuncio de la compañía sin su consentimiento.

También la información que Oculus recopile puede ser usada para publicidad dirigida. Así mismo, puede recopilar información como ubicación, registrar tu actividad de manera automática.

Fuente: http://es.gizmodo.com/los-oscuros-terminos-de-uso-de-oculus-rift-que-la-compa-1768863683

Apple no soluciona una vulnerabilidad cuyo exploit cabe en un solo tweet

por ABRIL 04, 2016 / REDES ZONE

Con sus sistemas basados en Unix, y teniendo entre sus características el usuario Root, el cual cuenta con permisos para realizar modificaciones en el sistema o en ficheros, que abre una puerta con la que un atacante toma los permisos de "root" y obtiene acceso total al sistema operativo.

Por lo que Apple desarrolló SIP (System Integrity Protection), una capa de seguridad que impide que cualquier proceso, archivo o carpeta del sistema operativo pueda ser modificado por otros procesos, aun así, se ejecuten como "root".

Apple ha sacado las nuevas versiones de sus sistemas operativos: Mac OS X 10.11.4 y iOS 9.3.1, pero esta vulnerabilidad parece que no ha sido del todo solucionada, por lo que se puede seguir evadiendo la capa de seguridad utilizando un exploit que incluso cabe en un tweet.

Fuente: http://www.redeszone.net/2016/04/04/apple-no-soluciona-una-vulnerabilidad-cuyo-exploit-cabe-solo-tweet/?utm_content=buffer5bf63&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

GOBIERNO

Hacker cuenta con pruebas de espionaje

por ABRIL 07, 2016 / AM GENERAL

Jhon Castelblanco, abogado del hacker Andrés Sepúlveda, aseguró que su cliente tiene pruebas que demuestran que el recluido hizo labores de espionaje informático en la campaña presidencial de Enrique Peña en el 2012.

Algunas de esas pruebas son copias de correos electrónicos, así mismo otras evidencias que fueron entregadas por Sepúlveda a la revista Bloomberg Businessweek. Castelblanco agregó que esta revista entrevistó al hacker en julio del año anterior, pero la publicación salió la semana pasada ya que la revista tardó ocho meses en verificar las afirmaciones y las pruebas ofrecidas por Sepúlveda.

Fuente: http://www.am.com.mx/2016/04/07/mexico/cuenta-con-pruebas-de-espionaje-hacker-274960

Países Latinoamericanos, poco preparados contra el crimen según nuevo informe

por ABRIL 05, 2016 / WE LIVE SECURITY

En el informe: "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), se llegó a la conclusión de que la mayoría de los países de esta región están poco preparados para contrarrestar las amenazas del cibercrimen.

Este informe es resultado de la aplicación del Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM), y desarrollado por el Centro Global de Capacidad sobre Seguridad Cibernética (GCSCC), consta de cinco niveles: Inicial, Formativo, Establecido, Estratégico y Dinámico.

Los datos utilizados fueron recolectados por medio de una encuesta en línea, que analizaron 49 indicadores del CMM categorizados en cinco ejes de evaluación: Política y estrategia, Cultura y sociedad, Educación, Marco jurídico, Tecnologías.

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

Ofrece Pentágono 150 mdd por hackear su página

por ABRIL 04, 2016 / HOY ESTADO

El programa 'Hack the Pentagon' del Departamento de Justicia de Estados Unidos invita a los hackers profesionales a encontrar fallos en su sistema. El programa estará vigente del 18 de abril al 12 de mayo de este año, el ganador se llevará un premio de hasta 150 mil dólares.

Los hackers podrán tener acceso a varios servidores públicos de la instancia de gobierno, pero no podrán acceder a aquellos que pongan en riesgo la seguridad del país.

No podrán inscribirse personas u organizaciones que estén relacionadas con terrorismo, tráfico de drogas, entre otros crímenes, además de que debe ser ciudadano estadunidense.

Fuente: http://www.hoyestado.com/2016/04/ofrece-pentagono-150-mdd-por-hackear-su-pagina/

NEGOCIOS

Smart TV, un nuevo riesgo en empresas

por ABRIL 05, 2016 / EXCELSIOR

Los equipos que se conectan a internet se están convirtiendo en las nuevas puertas para que los cibercriminales cometan diversos delitos, por ejemplo, se dice que a la empresa Target le robaron la información de millones de tarjetas de crédito infectando primero el sistema de calefacción y refrigeración para llegar a las terminales punto de venta.

Brian Kelly, director de Seguridad Global de Rackspace, comentó que la seguridad debe de estar incluida como parte del proceso de diseño viendo los nuevos ángulos de un posible ataque.

André Carreto, estratega de Seguridad de Symantec, destacó que el nuevo vector de ataque a las organizaciones se encuentra en las televisiones inteligentes ya que no tienden a recibir prioridad en las actualizaciones de software y parches correctivos, siendo una amenaza, ya que se puede usar un código malicioso para grabar el audio de reuniones confidenciales, robar propiedad intelectual y hasta sacar fotografías o video cuando están conectadas a una cámara.

Fuente:
http://www.excelsior.com.mx/hacker/2016/04/05/1084612

FINANZAS

Ciberatacantes aumentan esfuerzos para comprometer sistemas PoS

por MARZO 29, 2016 / SEGURIDAD INFORMATICA

Grandes minoristas han sido afectados por las brechas de seguridad en las tarjetas en los últimos años, incluyendo Target, y han actualizado sus sistemas. Pero el costo y las largas demoras en la obtención de nuevos sistemas certificados retrasan la transición y han dejado una ventana abierta a los cibercriminales.

El malware para los sistemas PoS llamado Treasurehunt, roba datos de la tarjeta de pago desde la memoria de una computadora, se implanta en un sistema de punto de venta a través del uso de las credenciales robadas o por medio de ataques de fuerza bruta. Una cadena dentro de su código indica que fue desarrollado por un grupo que se llama a sí mismo Bears Inc.

Este nuevo delito ha demostrado ser rentable para los criminales cibernéticos. Es fácil encontrar foros orientados a tarjetas de pago donde los detalles de estas tienen un precio de acuerdo a cómo fue robada, la fecha del robo, los datos y el límite potencial de la tarjeta.

TOTALSEC NEWSLETTER - INFOSEC

BOLETÍN No. 8

09 ABRIL – 17 ABRIL, 2016

Elaboración: ABRIL 18, 2016.