2015-02-14

CyberNoticias # 25

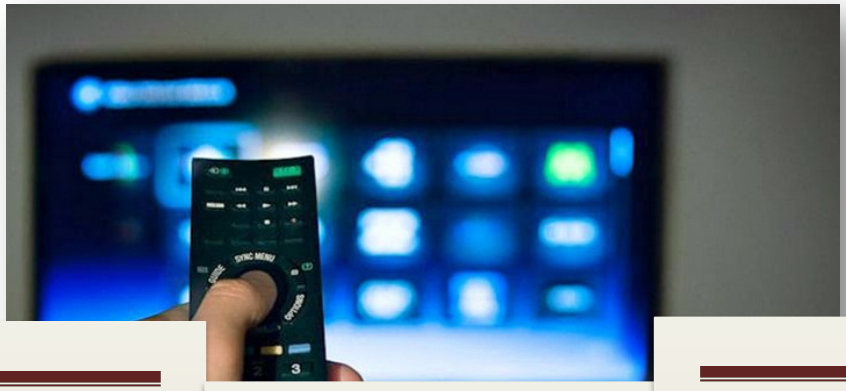
SCProgress

www.scprogress.com

ÍNDICE

1. SAMSUNG SMART TV ESPÍAN LAS CONVERSACIONES DE LOS USUARIOS..... 03
2. UN MENSAJE PUEDE DETENER TU WHATSAPP 04
3. BOLIVIA ANALIZA UN PLAN DE SEGURIDAD INFORMÁTICA TRAS LOS ATAQUES DE HACKERS CHILENOS 05
4. UN ERROR EN IE PERMITE SALTARSE LA POLÍTICA DEL MISMO ORIGEN..... 06
5. TOSHIBA PRESENTA UN USB CON CIFRADO FÍSICO QUE SE AUTODESTRUYE... 07

Noticia # 01: SAMSUNG SMART TV ESPÍAN LAS CONVERSACIONES DE LOS USUARIOS.



Samsung ha confirmado que sus televisores inteligentes con reconocimiento de voz activados, pueden grabar las conversaciones de los usuarios y transmitirlas a terceras partes. Samsung explica que la información recogida está cifrada para "evitar usos no autorizados" aunque no ha aclarado quién son esas "terceras partes" que recogen la información.

Además, aunque la tecnología de reconocimiento de voz se desactive, los televisores siguen recogiendo y transmitiendo información sobre el uso y preferencia de los usuarios.

No es la primera vez que estas Samsung Smart TV, otros televisores inteligentes que también recogen información disparan las alarmas entre los expertos en privacidad.

Garantizarla va a ser todo un reto cuando en unos años haya miles de millones de dispositivos conectados bajo la Internet de las Cosas.

Fuente: http://muyseguridad.net/2015/02/10/samsung-smart-tv

Noticia # 02: UN MENSAJE PUEDE DETENER TU WHATSAPP.

Dos jóvenes investigadores indios Indrajeet Bhuyan y Saurav Kar han encontrado el problema y han publicado un vídeo de demostración del problema. Basta con enviar un mensaje de 2 Kb de tamaño con un conjunto especial de caracteres para provocar la caída del Whatsapp del receptor.

Además el usuario tendrá que eliminar toda la conversación y empezar una nueva, ya que al momento de abrirla el mensaje seguirá provocando el cierre de la aplicación, a menos que se borre completamente. Según los investigadores el problema se puede reproducir en la mayoría de las versiones de Android, incluyendo Jellybean, Kitkat y versiones anteriores de Android. Igualmente se ha reportado que todas las versiones de WhatsApp, incluyendo 2.11.431 y 2.11.432, están afectadas por esta vulnerabilidad.

Fuente: http://unaaldia.hispasec.com/2014/12/un-mensaje-puede-detener-tu-whatsapp.html

Noticia # 03: BOLIVIA ANALIZA UN PLAN DE SEGURIDAD INFORMÁTICA TRAS LOS ATAQUES DE HACKERS CHILENOS

La Paz, 12 feb (EFE).- El Gobierno boliviano organizó hoy el taller "Elementos clave para desarrollar un plan de contingencias informáticas", después de que varias de sus páginas web fueran atacadas por piratas informáticos chilenos, que publicaron en ellas mensajes relativos al contencioso marítimo entre Bolivia y Chile. La actividad fue realizada por la estatal Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transporte (ATT), cuyo director, Luis Felipe Guzmán, confió en que del taller salgan "aportes para que las instituciones del Estado puedan prevenir o reaccionar rápidamente ante estos incidentes". Guzmán, según la agencia oficial ABI, explicó que esta iniciativa fue programada tras los ataques a las páginas de internet de entidades públicas y privadas bolivianas por parte de supuestos "hackers" chilenos.

"La experiencia de las últimas semanas nos ha demostrado que podemos ser vulnerables a los 'hackeos', es un tema de preocupación y política pública que debemos afrontar todas las instituciones del Estado", consideró. El pasado 4 de febrero, piratas informáticos chilenos atacaron el sitio web del Ministerio de Comunicación de Bolivia con mensajes en contra de la centenaria reivindicación marítima de este país hacia Chile por una salida soberana al Pacífico perdida en una guerra del siglo XIX.

Esta acción se la atribuyó a través de la red social Twitter el grupo Chilean Hackers, que también fue responsable en semanas anteriores de ataques similares contra los sitios web de la Armada y la Policía bolivianas. El vicepresidente de Bolivia, Álvaro García Linera, lamentó estos incidentes y recomendó entonces aumentar la seguridad informática del país, si bien precisó que este tipo de actuaciones no pone en riesgo la seguridad del Estado ni su información clasificada.

Fuente: http://www.diariolasamericas.com/5051_america-latina/2950566_bolivia-analiza-un-plan-de-seguridad-informatica-tras-los-ataques-de-hackers-chilenos.html

Noticia # 04: **UN ERROR EN IE PERMITE SALTARSE LA POLÍTICA DEL MISMO ORIGEN.**

Internet Explorer vuelve a estar envuelto en polémica. Desde Microsoft acaban de reconocer que están trabajando para parchear el error que permite a los atacantes eludir la política del mismo origen, una medida de seguridad importante para scripts y que permite inyectar código malicioso en sitios webs, robar cookies y datos de acceso. Un grupo llamado Deuson acaba de publicar una prueba que muestra como el exploit de Internet Explorer permite violar la política del mismo origen en la web de Daily Mail. Este grupo ha podido poner las palabras "Hacked by Deusen" en el sitio web del periódico, lo que prueba que también se puede inyectar otro código HTML o Javascript.

Por su parte Microsoft ha dicho que "no es consciente de que esta vulnerabilidad pueda aprovecharse" y que están "trabajando en una actualización de seguridad". Eso sí, aunque creen que esta vulnerabilidad no puede ser aprovechada sí que han aconsejado a los usuarios que eviten abrir enlace de fuentes que no sean de confianza y que eviten visitar sitios web donde la seguridad brille por su ausencia. También recomiendan cerrar la sesión una vez que dejamos de utilizar alguna cuenta por internet.

Fuente: http://www.softzone.es/2015/02/04/un-error-en-ie-permite-saltarse-la-politica-del-mismo-origen/#more-91859

Noticia # 05: TOSHIBA PRESENTA UN USB CON CIFRADO FÍSICO QUE SE AUTODESTRUYE

La tecnológica japonesa Toshiba lanzó al mercado un pendrive cifrado con un teclado físico en el que se le introduce un código de acceso, para hacerlo más seguro que los comunes.

Denominado por la empresa como Encrypted USB Flash Drive, el pendrive está fabricado en aluminio y para utilizarlo primero hay que introducirle la contraseña -en el teclado incorporado- y luego conectar a la computadora.

Según informó Toshiba, al desconectarlo la memoria se bloquea de forma automática y, tras diez intentos fallidos de introducir la contraseña, la información se borra.

El pendrive USB 2.0 se ofrece con capacidades que van de 4GB a 32GB y funciona con dispositivos Windows, Mac OS X y Linux.

Fuente: http://www.minutouno.com/notas/353017-toshiba-presenta-un-usb-cifrado-fisico-que-se-autodestruye