NEWSLETTER – INFOSEC MX

BOLETIN No. 34

Octubre 08- 16

Elaboración: Octubre 17, 2016

Servicio de Telegram se cae, pero descarta problemas de seguridad

por OCTUBRE 13, 2016 / EXCELSIOR

El servicio de mensajería instantánea Telegram dejó de funcionar en América Latina aproximadamente por dos horas este jueves. Telegram es uno de los servicios de mensajería con mayores estándares de seguridad, pero en México se usa más WhatsApp y Facebook Messenger. Pero aun no teniendo muchos usuarios en el país, fueron los suficientes para provocar que la falla se convirtiera en Trending Topic.

Se dio a conocer que fueron fallas de hardware estando en riesgo de sobrecalentamiento en un centro de datos, pero a las 13:41 el sistema de mensajería informó que ya estaba restablecido el servicio para el 99% de sus usuarios en América Latina.

Fuente: : **http://www.excelsior.com.mx/hacker/2016/10/13/1122252**

Usuarios de Spotify aseguran ser víctimas de malware

por OCTUBRE 10, 2016 / EL UNIVERSAL

Algunos usuarios de Spotify aseguran haber sido infectados de malware al utilizar la versión gratuita de la aplicación. Un usuario escribió que al tener abierto Spotify Free, su navegador predeterminado de Internet se ponía en marcha y abría diferentes tipos de sitios maliciosos. En algunos de ellos incluso, no se requiere acción del usuario para causar daño. El código malicioso provenía de los anuncios publicitarios que despliega la aplicación sin costo, y afectó a los diferentes tipos de sistema operativo: Windows, Ubuntu y OS X. A través del foro Spotify Community, la compañía dijo haber identificado el problema y haberlo corregido, pero continuará con el monitoreo de la situación.

El problema con este tipo de ataques es que el riesgo del usuario de dar clic en alguno de los anuncios con malware es alto, ya que es normal que aparezcan estos mensajes en aplicaciones gratuitas y es difícil identificar cuál de ellos es malicioso; de este ataque se destaca la entrega de malware de manera autónoma, sin requerir intervención del usuario provocando que el número de víctimas aumente aún más. Se aconseja a los usuarios que crean haber sido infectados realizar un análisis de malware en su computadora. La herramienta gratuita Kaspersky Virus Removal Tool ayudará a remover el malware de su dispositivo.

Fuente:
http://eluniversal.com.mx/articulo/techbit/2016/10/10/usuarios-de-spotify-aseguran-ser-victimas-de-malware

Investigadores revelan que es posible conocer origen de ciberataques

por OCTUBRE 04, 2016 / COMPUTER WORLD MEXICO

Las técnicas utilizadas por los cibercriminales para cometer ilícitos hacen más difícil su localización. Los investigadores Brian Bartholomew y Juan Andrés, revelaron que los creadores de las amenazas avanzadas utilizan operaciones de banderas falsas (False Flags) para engañar, pero es posible dar con el origen del ataque. Con las muestras relacionadas se podrían determinar las horas de trabajo de los desarrolladores, y sugerirían un uso horario general para sus operaciones, aunque estas marcas pueden ser alteradas con facilidad. El idioma es una pista que revela el origen, por medio del dominio del lenguaje al crear un correo electrónico de un phishing.

Los documentos de phishing pueden tener metadatos que guardan información apuntando a la computadora del autor, pero se pueden manipular los marcadores de idioma y confundir a los investigadores. Se puede buscar el domicilio virtual de los malhechores al indagar los verdaderos servidores de comando y control (C&C), es una infraestructura que puede ser costosa y difícil de mantener, por lo que hasta los atacantes que disponen de buenos recursos tienden a reutilizar una infraestructura C&C o dephishing. Las conexiones secundarias o de back-end pueden dar una idea de la identidad de los atacantes, si estas no logran el anonimato adecuado en las conexiones a Internet al acumular datos de un servidor de correo electrónico o de exfiltración, preparar a un servidor intermediario o de phishing o al verificar a un servidor pirateado.

Fuente:
http://www.20minutos.com.mx/noticia/144922/0/investigadores-revelan-que-es-posible-conocer-origen-de-ciberataques/

Bajo reserva líder de San Lázaro, en manos de hackers

por OCTUBRE 10, 2016 / EL UNIVERSAL

El presidente de la mesa directiva de San Lázaro, Javier Bolaños, fue víctima de los hackers, ya que el pasado fin de semana recibió un ataque cibernético en su teléfono inteligente, que lo dejó incomunicado. Comentó que de pronto, apareció en su pantalla la leyenda: "Este teléfono ha sido reportado como extraviado", y enseguida, desaparecieron sus fotos, videos y notas que guardaba desde hace mucho tiempo.

El legislador tenía más de siete años con el mismo número y ahora se dedica a recuperar todos los contactos perdidos. Además, dice haber visto un dron que sobrevoló por varios minutos su casa, antes de que su celular fuera víctima del golpe cibernético.

Fuente: **http://www.eluniversal.com.mx/entrada-de-opinion/columna/bajo-reserva-periodistas-el-universal/nacion/2016/10/13/lider-de-san**

El 35% de los usuarios de redes sociales sufrió un incidente de malware

por OCTUBRE 10, 2016 / NETMEDIA MX

Según los datos arrojados en una reciente investigación de la firma ESET, el 35% de los encuestados sufrió un incidente de malware o spam a través de campañas de ingeniería social para el robo de información, el control del sistema infectado o adquirir las contraseñas de la víctima. El primer lugar de estos incidentes lo tienen casos de malware y spam, en segunda posición campañas maliciosas y en tercer lugar ataques de phishing.

El 30% reconoció que hizo clic en una publicación extraña alguna vez convirtiéndose en víctima de algún engaño. Es habitual que los atacantes utilicen este tipo de campañas maliciosas para atrapar a los usuarios desprevenidos y propagan contenidos falsos o realizan publicaciones de manera involuntaria desde su perfil. De esta manera, sin descargar nada malicioso en el dispositivo del usuario, lo suscriben a servicios de publicidad generándole algún costo económico. El 15% de los usuarios fue víctima de phishing, que es frecuentemente realizado a través de un correo electrónico y sitios web duplicados, aunque puede realizarse por otros medios como las redes sociales.

Fuente: **http://www.netmedia.mx/b-secure/el-35-de-los-usuarios-de-redes-sociales-sufrio-un-incidente-de-malware/?utm_content=buffer078ab&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

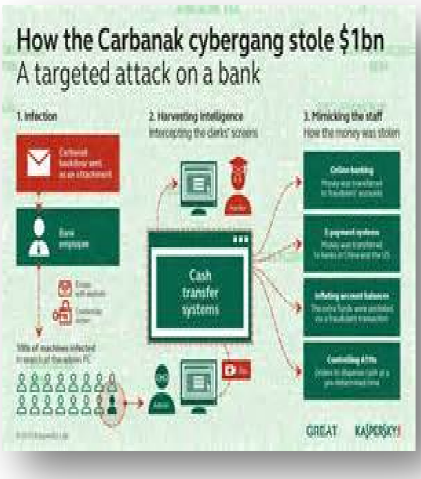
Ordinaff, un nuevo troyano bancario relacionado con Carbanak

por OCTUBRE 12, 2016 / REDES ZONE

Los responsables de Carbanak regresan con el troyano bancario Ordinaff, una nueva amenaza que buscará afectar a entidades bancarias. Antes afectar a los usuarios era algo importante, pero los ciberdelincuentes han visto que no vale la pena centrar sus esfuerzos en ellos, sobre todo porque en el seno de las entidades existen equipos iguales o más vulnerables, y ahora buscan atacar las infraestructuras de las entidades de forma directa.

Se cree que se trata de una primera versión que carece de funcionalidad completa, permitiendo tantear la reacción de las herramientas de seguridad. Estas amenazas permiten cierto control sobre el dispositivo infectado. Se podría decir que nos encontramos ante una puerta trasera, ya que también permite el control sobre el sistema de ficheros del dispositivo afectado, así el ciberdelincuente no pierde ningún detalle y puede optimizar la infección y sacar de esta el máximo partido. Al ser equipos que poseen software bancario instalado, el manejo de información importante es constante. Las entidades bancarias afectadas de momento se cree que la hoja de rutas marcada también sería heredada, probando con bancos asiáticos, en Reino Unido, Australia o Estados Unidos.

Fuente: **http://www.redeszone.net/2016/10/12/ordinaff-nuevo-troyano-bancario-relacionado-carbanak/?utm_content=buffer9739f&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**



Uno de cada 16 smartphones son vulnerables a BadKernel

por SEPTIEMBRE 06, 2016 / REDES ZONE

Es una vulnerabilidad descubierta por una empresa de seguridad china y que fue solucionada hace un año, se encontraba en el motor JavaScript V8 de Google, concretamente entre las versiones 3.20 y 4.2. Es muy sencilla de explotar, y puede llegar a permitir a un atacante acceder sin problemas a toda la información del dispositivo, como a los SMS, a las contraseñas, a la cámara, a los contactos e incluso a la ubicación, y controlarlo de forma remota. Puede afectar a cualquier dispositivo, aunque los fabricantes más afectados son LG, Samsung, Motorola y Huawei.

Según un reciente estudio, aunque la vulnerabilidad en el motor JS v8 de Google ya fue solucionada hace más de un año, a día de hoy uno de cada 16 dispositivos sigue siendo vulnerable. La principal forma de explotar esta vulnerabilidad es a través de páginas web maliciosas o instalando y ejecutando webapps que carguen directamente servidores controlados por cibercriminales con los exploits para tomar el control de los dispositivos vulnerables. Como medida de protección, lo primero que se debe hacer es asegurarse de mantener todas las aplicaciones actualizadas a la versión más reciente, así como actualizar a la última versión de Android disponible.

Fuente **http://www.redeszone.net/2016/10/06/uno-de-cada-16-smartphones-son-vulnerables-a-badkernel/?utm_content=buffer30a01&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

BadKernel

Reciente cumbre del G-20 fue atacada cerca de 133 mil veces

por OCTUBRE 07, 2016 / SEGURIDAD UNAM

La firma contratada por el Ministerio de Seguridad Pública de China para proveer protección del evento, el cuál es siempre un honeypot para la actividad maliciosa de Internet. Se detuvieron 133,254 ataques hacia la red del G-20 y más de 1.9 millones de ataques contra organizaciones que ofrecían servicios para la cumbre. Ataques del tipo stepping stone, una táctica usada contra terceros como una vía fácil para infiltrarse en una organización.

Equipos de contratistas fueron comprometidos para infiltrarse en la Oficina de Administración de Personal y el minorista Target, generando una fuga de más de diez millones de registros. Hubo 169,919 ataques web hacia el G-20 y sus redes afiladas así como 1,984 ataques DDoS, de acuerdo a NSFOCUS. El proveedor encontró 611,356 vulnerabilidades antes de la cumbre, las cuales 190 fueron de alto riesgo

Fuente:
http://www.seguridad.unam.mx/noticia/?noti=3051&utm_content=bufferb96b2&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Mastercard acelera el cambio de contraseñas a selfies

por OCTUBRE 06, 2016 / SEGURIDAD UNAM

Este servicio pronto estará en 12 mercados incluyendo el Reino Unido, España, Suecia, Alemania y los Países Bajos, usa la biométrica facial para verificar la identidad de los usuarios, significando no tener que recordar otra contraseña para completar la transacción. También funcionará usando un escáner de huellas digitales en el dispositivo, mientras el usuario cuente con uno. La idea es que al ofrecer a los clientes una manera más simple de autenticar se obtengan menos compras a medias o que declinen si introducen mal su contraseña. Este servicio será lanzado mundialmente el próximo año.

Paco García, director de tecnología de la firma Yoti, dijo que los vendedores están ahora bajo una gran presión de los nativos digitales, consumidores enfocados en los dispositivos móviles quienes se han acostumbrado a las tarjetas sin contacto y los pagos a distancia. Añadió que el reto clave para cualquiera de estas soluciones de autenticación con selfies es asegurar que la persona frente al teléfono que procesará el pago sea la correcta. Robert Page, pentester de Redscan, advirtió que si la información biométrica se captura y es usada por un atacante, no es posible cambiar las huellas digitales como con una contraseña. La implementación de Mastercard de reconocimiento facial que requiere que el usuario parpadee parece ser una solución para prevenir que otros tomen una foto del usuario. La efectividad de esta implementación aún está por soportar la prueba del tiempo.

Fuente:
http://www.seguridad.unam.mx/noticia/?noti=3049&utm_content=buffereeb73&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

TOTALSEC NEWSLETTER – INFOSEC

BOLETÍN No. 34

Octubre 08- 16, 2016

Elaboración: Octubre 17, 2016

totalsec