NEWSLETTER – INFOSEC MX

BOLETIN No. 39

Noviembre 12- 20

Elaboración: Noviembre 21, 2016

Cibercrimen aumenta 10% a nivel mundial

por NOVIEMBRE 16, 2016 / EL FINANCIERO

Durante este año, 689 millones de personas fueron víctimas del crimen cibernético a nivel global, representando un incremento de 10% en comparación con el 2015. Esto según el informe Norton sobre Ciberseguridad 2016, el cual se basa en un análisis de seguridad cibernética en 21 países, entre ellos México, el problema lo atribuye a que los usuarios mantienen hábitos en línea poco seguros, aun estando conscientes de los riesgos de seguridad en la red, por lo que los atacantes perfeccionan sus actividades ilegales para obtener mayor ventaja.

El informe destaca que los usuarios mejoraron en la creación de códigos de seguridad para cada una de sus cuentas, no obstante la acción de compartir contraseñas subió 2%, al ubicarse este año en 24%. Cerca del 35% de los encuestados tiene por lo menos un dispositivo desprotegido, que deja a otros vulnerables ante el secuestro virtual, programas maliciosos y fraudes cibernéticos.

Fuente: **http://www.elfinanciero.com.mx/empresas/cibercrimen-aumenta-10-a-nivel-mundial.html**

Difunden datos de 400 millones de usuarios de Adult Friend Finder

por NOVIEMBRE 15, 2016 / EXCELSIOR

AdultFriendFinder acaba de ser hackeada por segunda vez en 18 meses. El número de cuentas implicadas asciende a más de 400 millones según los cálculos de Leakedsource. Estarían expuestos los datos de un total de 412 millones de perfiles, incluso aquellos que hubieran sido eliminados o permanecieran inactivos.

Los delincuentes cibernéticos habrían robado información que representa más de 20 años de datos de los clientes, y Adult FriendFinder no sería la única afectada, sino también otras plataformas del grupo como Penthouse.com, Stripshow.com, iCams.com y Cams.com.

Fuente:
http://www.excelsior.com.mx/hacker/2016/11/15/1128198

Infraestructura en riesgo por ciberataques

por NOVIEMBRE 14, 2016 / EL SIGLO DE TORREON

Mikel Santos de PA Consulting, empresa de consultoría británica, dijo que en México no hay un buen nivel de conciencia acerca de las consecuencias, no se han desarrollado medidas o estrategias de ciberseguridad, no hay una regulación que defina o clasifique lo que es la infraestructura crítica y menos una estrategia para abordar el problema. Y agregó que el país no tiene información respecto a los ataques que se producen. Sin embargo, ya se han registrado casos, como en 2014, cuando Pemex fue blanco de ataques iraníes.

También detalló que cuando se presentan amenazas a la infraestructura crítica, en la mayoría de los casos, detrás están gobiernos o grupos muy bien organizados, ya que para llegar a afectar los sistemas son necesarios muchos recursos y un amplio conocimiento en el tema. Y cuando logran su cometido provocan que la población se quede sin servicios, por ejemplo, sin energía eléctrica, como sucedió el año pasado en Ucrania, ataque que teóricamente provino del gobierno ruso, tuvo una preparación de seis meses para poder entrar a los sistemas de control, porque se necesita tener cierta capacidad y acceso, hace falta replicar la misma arquitectura para desarrollar malware y probar los ataques.

Fuente:
https://www.elsiglodetorreon.com.mx/noticia/1282581.infraestructura-en-riesgo-por-ciberataques.html

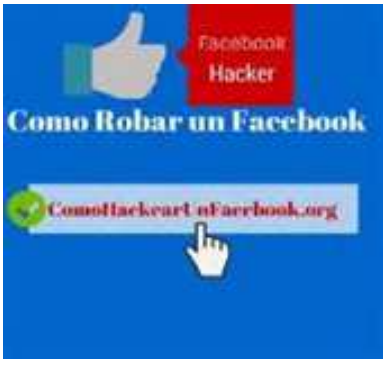
Detectan campaña maliciosa que roba contraseñas en Facebook

por NOVIEMBRE 11, 2016 / NETMEDIA

La campaña está dirigida a Argentina, México, Colombia y Chile. En cinco días más de 18,000 personas accedieron y pudieron haberse convertido en víctimas. Hace días se empezaron a reportar publicaciones en Facebook con una gran cantidad de usuarios etiquetados que eran invitados a ver un supuesto video de contenido pornográfico, y al dar clic sobre la publicación, era llevado a Tumblr, una plataforma para crear micro blogs sociales en la que se publican imágenes, videos y enlaces. En este sitio web, el atacante publicaba distintos enlaces acortados que supuestamente dirigían al video prometido.

Así el usuario no puede observar adónde lo lleva el nuevo enlace que está asociado con smartURL, un acortador de direcciones web gratuito que permite elegir el comportamiento de la redirección, dependiendo del tipo de dispositivo desde el que se esté abriendo el enlace: Si se ingresaba desde un dispositivo móvil, era direccionado a una página de phishing que simulaba ser el login de Facebook y le solicitaba ingresar sus credenciales para poder acceder al video quedando expuesto a publicaciones no autorizadas o al envío de spam. Android fue la más afectada seguida de sistemas operativos de equipos de escritorio. Donde de los más de 18.000 clics hechos, 97.8% se vio expuesto al phishing.

Fuente: **http://www.netmedia.mx/b-secure/detectan-campana-maliciosa-que-roba-contrasenas-en-facebook/?utm_content=buffer1e2d7&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**



Los ciberataques a terminales móviles aumentan más de un 32% con respecto al año pasado

por NOVIEMBRE 11, 2016 / REDES ZONE

Un estudio realizado ha mostrado que en lo que va del año han aumentado el número de infecciones en un 32,6% con respecto al pasado año. Lo cual supone hasta el momento un total de 70 millones de amenazas detectadas, cifra que crecerá cada año, sobre todo por el auge de estos dispositivos entre los usuarios. Los ciberdelincuentes se valen sobre todo para realizar la infección de mensajes SMS spam o bien de tiendas de aplicaciones alternativas, donde las medidas de seguridad no alcanzan las fijadas en las oficiales.

Sin embargo, tampoco es bueno fiarse del contenido de las tienda oficiales, ya que en más de una ocasión han sido capaces de esquivar las medidas de seguridad y publicar virus informáticos. Esto se aplica sobre todo a la Google Play Store, pero también se han dado algunos casos en la App Store de los de Cupertino. El aumento de las conexiones a Internet también permite que los usuarios accedan a este tipo de contenidos y por lo tanto la difusión de los mismos.

Fuente: **http://www.redeszone.net/2016/11/11/los-ciberataques-temrinales-moviles-aumentan-mas-32-respecto-al-pasado-ano/?utm_content=buffer288aa&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

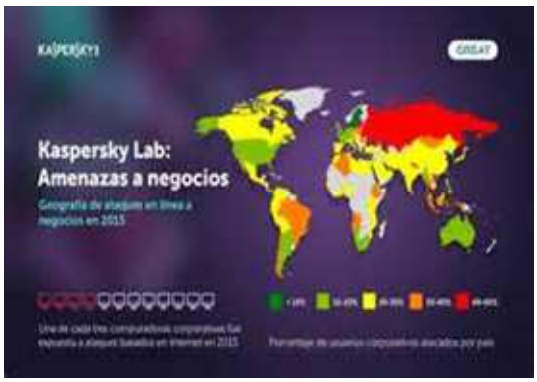
El ransomware para Pymes se multiplica por más de ocho

por NOVIEMBRE 09, 2016 / SILICON

Según Kaspersky Lab, más de la mitad de las pymes que han sufrido un ataque de cifrado tuvo que emplearse durante días para recuperar el acceso a sus datos, siendo el ransomware el problema de seguridad que más ataca a las empresas actualmente. Durante el tercer trimestre de 2016 las empresas de pequeño tamaño han recibido ocho veces más ataques de este malware que en el mismo periodo de 2015.

La solución Kaspersky Small Office Security pasó de bloquear 3.224 ataques hace un año a 27.471 en esta ocasión. Kaspesky Lab habla de tentativas de bloqueo frustradas que pretendían impedir el acceso a información corporativa. Pagar el rescate no garantiza que los datos vayan a ser devueltos sin problemas, dijo Vladimir Zapolyansky, jefe de SBM Marketing en Kaspersky Lab.

Fuente: **http://www.silicon.es/ransomware-pymes-2322591?utm_content=buffercdb64&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**



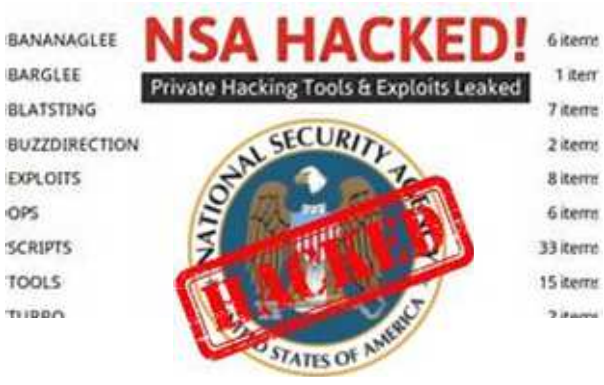
Filtran herramienta de hackeo robada a la NSA – La Jornada

por NOVIEMBRE 14, 2016 / MEDIOS DE MEXICO

El grupo "Shadow Brokers" dio a conocer otra herramienta de intrusión cibernética de alto nivel robada a la Agencia de Seguridad Nacional de Estados Unidos (NSA). La filtración revela nombres clave al estilo de la NSA y porta información de protocolos de internet sobre cientos de organizaciones, muchas de ellas con sede en Japón, China y Corea del Sur. Matthew Hickey, cofundador de Hacker House, dijo que es posible que los servidores hayan sido utilizados como escalas para ayudar a ocultar el origen de las operaciones electrónicas de espionaje.

Lo más preocupante para la NSA es que la filtración respalda las afirmaciones de Shadow Brokers de que robaron una serie de ganzúas electrónicas de la agencia, difíciles de generar además de costosas. La gravedad de la filtración fue confirmada cuando compañías de seguridad se apresuraron a parchar agujeros en su software que salieron a la luz tras la revelación. The Intercept, una publicación de investigación con acceso a material de la NSA filtrado por el ex contratista de inteligencia Edward Snowden, confirmó posteriormente que las herramientas de Shadow Brokers eran de la NSA, al confrontar los datos filtrados con información contenida en un manual ultra secreto que no había sido publicada anteriormente.

Fuente **http://mediosdemexico.com/noticias/filtran-herramienta-de-hackeo-robada-a-la-nsa-la-jornada/**



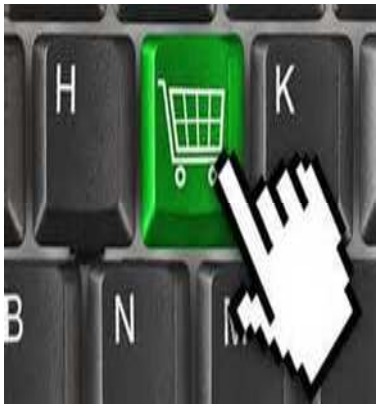
Facebook compra contraseñas en el mercado negro

por NOVIEMBRE 11 29, 2016 / SEGURIDAD UNAM

El CSO de Facebook Alex Stamos, dijo que para mantener seguro a los usuarios es necesario construir un software a prueba de ataques para evitar a los atacantes, pero la reutilización de contraseñas es la principal causa de daño en Internet y el sistema de ingreso de usuario y contraseña que fue introducido en los años 70 es obsoleto. CNET dice que cuando las contraseñas son robadas en masas y se negocian en el mercado negro, se hace evidente cuántos usuarios eligen las contraseñas más débiles para proteger sus cuentas en línea, haciendo su cuenta más vulnerable a un ataque.

Para comprobar que sus usuarios no están haciendo uso de estas contraseñas comunes para sus cuentas de Facebook, la empresa compró contraseñas en el mercado negro para compararlas con contraseñas cifradas utilizadas en su sitio. Y alerta a decenas de millones de usuarios que sus contraseñas necesitan ser cambiadas ya que son muy vulnerables. Facebook proporciona una amplia gama de herramientas para reforzar la seguridad de sus usuarios, incluida la autenticación de dos factores, identificación de rostros de los amigos, así como algoritmos de aprendizaje automático para determinar e informar si la actividad de la cuenta es fraudulenta. Otra nueva medida aborda la cuestión de la recuperación de cuentas, donde si incluso los atacantes logran entrar en su cuenta de correo electrónico, lo que les permitiría aprovecharse de la cuenta de Facebook fácilmente restableciendo la contraseña, la red social permite a sus amigos cercanos verificar la solicitud de recuperación de cuentas en su nombre.

Fuente: **http://digitalcomunicacion.com.mx/facebook-compra-contrasenas-robadas-en-el-mercado-negro/**



TOTALSEC NEWSLETTER – INFOSEC

BOLETÍN No. 39

Noviembre 12 - 20, 2016

Elaboración: Noviembre 21, 2016

totalsec