NEWSLETTER – INFOSEC MX

BOLETIN No. 35

Octubre 15- 23

Elaboración: Octubre 24, 2016

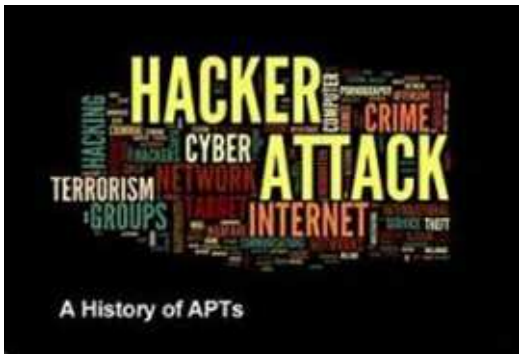
Amazon, Twitter, Netflix y otros populares sitios sufren ciberataques

por OCTUBRE 21, 2016 / EXPANSION

El viernes 21 de octubre cerca de las 6 de la mañana, algunos usuarios carecieron del acceso a varios sitios web a causa de un aparente ataque DDoS masivo. Según Hacker News, la falla es el resultado de un ataque contra el servidor DNS de Dyn, que es la empresa que administra los dominios de los sitios web. Entre los sitios que al parecer se vieron afectados están Twitter, Etsy, Github, Vox, Spotify, Airbnb, Netflix y Reddit. La empresa Dyn en un comunicado señaló haber empezado a vigilar y a mitigar el ataque DDoS contra la infraestructura Dyn Managed DNS. Y agregó que el ataque estaba afectando principalmente a la costa este de Estados Unidos teniendo impacto sobre los clientes de Managed DNS en esa región.

Para las 9:20 de la mañana, Dyn señaló que los servicios regresaron a la normalidad, hay poca información disponible acerca de la causa del ataque, las empresas recurrieron a Twitter para pedirles a los clientes que tuvieran paciencia.

Fuente: **http://expansion.mx/tecnologia/2016/10/21/amazon-twitter-netflix-y-otros-populares-sitios-sufren-ciberataque**



El escenario mundial ante la ciberguerra

por OCTUBRE 13, 2016 / DINERO EN IMAGEN

Las ciberguerras son una realidad y estamos apenas en el inicio de éstas, advirtió el gerente general y vicepresidente de Ventas Internacionales para Fortinet Latinoamérica, Pedro Paixão. Actualmente se está en la fase de espionaje, significando que los gobiernos o grupos terroristas pueden contratar a ciberdelincuentes para robar información. Paixão consideró que las guerras cibernéticas se diferenciarán de las tradicionales sobre todo por las "armas", ya que en una guerra cibernética el arma es un software que, una vez suelto en la red, puede ser ocupada por otras personas o por el enemigo.

Stuxnet es el mejor ejemplo de armas cibernéticas que no desaparecen y se democratizan, ya que dicho gusano ahora puede ser descargado por cualquier persona para estudiarlo, mejorarlo y usarlo. Hay países, tanto avanzados como en desarrollo, cuya infraestructura depende de internet y son más vulnerables. En cambio, atacantes como Corea del Norte o las actuales cunas del terrorismo, tienen la capacidad de desarrollar armas cibernéticas y usarlas, pero es difícil contraatacarlos porque su uso de Internet es muy limitado. Posiblemente faltan años para ver declarada una ciberguerra como tal, mientras que un ataque de ciberterrorismo podría pasar más pronto.

Fuente: **http://www.dineroenimagen.com/2016-10-13/78944**

73% de profesionales de TI desconfían de la nube

por OCTUBRE 18, 2016 / CIO AMERICA LATINA

Una encuesta de la empresa Lieberman Software mostró que el 73% de los profesionales de Ti prefieren mantener los datos corporativos sensibles on-premise más que en la Nube. Las empresas necesitan entender que se enfrentan a los mismos problemas de seguridad en la Nube que en entornos on-premise; "migrar a la Nube no significa que se enfrenten a más o menos riesgos de seguridad que manteniendo sus datos on-premise".

Sobre el cloud y la seguridad, un 90% dice que la nube les está forzando a aprender más, y un 33% afirmó que será el fin de los equipos de seguridad tradicionales. Además, un 43% dice que no cambian sus contraseñas en la Nube con la misma frecuencia como lo hacen en sistemas on-premise. Los atacantes utilizan las mismas técnicas para atacar un entorno físico que uno cloud. Para tener éxito los atacantes necesitan credenciales, para conseguir esas credenciales los cibercriminales utilizan técnicas como el phishing o la ingeniería social para superar las barreras perimetrales como firewalls. Ya dentro de la red, el atacante busca credenciales con privilegios que les permitan moverse entre sistemas y robar datos sensibles.

Fuente: **http://www.cioal.com/2016/10/18/73-profesionales-de-ti-desconfia-nube/**

Kaspersky rastrea cientos de campañas maliciosas

por OCTUBRE 13, 2016 / CIO AMERICA LATINA

Kaspersky Lab rastrea la actividad de más de un centenar de agentes de amenazas y operaciones maliciosas dirigidas contra organizaciones comerciales y gubernamentales en 85 países. Los ataques dirigidos ya no son una actividad de élite, ya que hoy en día se observan campañas de ciberespionaje pequeñas. Estos grupos están a la caza de información confidencial, que puede utilizarse para obtener ventajas geopolíticas o venderla a cualquiera. Incluso cuando las soluciones para el malware son eficaces, no pueden proporcionar una garantía de detección del 100% cuando se trata de ataques dirigidos.

Los que generan estas campañas son profesionales de la ingeniería social, pueden utilizar vulnerabilidades de día cero, y utilizan cada vez más herramientas legítimas para el acceso remoto en lugar de malware real. En una infraestructura de TI empresarial, un software de seguridad debe ir acompañado de medidas de inteligencia, con equipos de seguridad respaldados por la experiencia, de modo que sepan cuándo sea una alarma, y qué pistas buscar si su organización se convierte en el objetivo a atacar. La inteligencia recopilada por Kaspersky Lab está disponible para los clientes empresariales y gubernamentales, a través del acceso por suscripción especial al APT Reporting Portal, donde se detallan los agentes de amenazas, y datos procesables para identificar ataques a una empresa.

Fuente: **http://www.cioal.com/2016/10/13/kaspersky-rastrea-campanas-maliciosas/?utm_content=buffer7234a&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

Detecta BBVA Bancomer más de 2,500 sitios digiales fraudulentos

por OCTUBRE 19, 2016 / CRONICA

BBVA Bancomer reportó que entre 2015 y lo que va del 2016, ha detectado dos mil 500 sitios apócrifos buscando robar la identidad de los usuarios, informó José Juan Ávila Palafox, director de Gestión Multicanal de la entidad, durante la presentación de un nuevo taller de educación financiera que ofrecerá BBVA Bancomer. La forma más frecuente de ciberataque a la banca digital es por phishing, que es la forma en la que los hackers roban la identidad de un usuario a través de un correo electrónico.

Si bien las quejas por ciberataques han crecido 175% en el último año, según datos de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), para Adolfo Albo, director global de educación financiera de BBVA Bancomer, el delito todavía no figura entre los problemas más significativos que tiene el sector financiero. Los delitos en el sistema financiero a través de medios electrónicos han venido incrementándose, pero para el conjunto del sector aún es pequeño, pues ocupa el 0.5% de las operaciones vinculadas con los de la banca digital, y la mayoría se resuelve por medio de los propios bancos.

Fuente: **http://www.cronica.com.mx/notas/2016/990562.html**

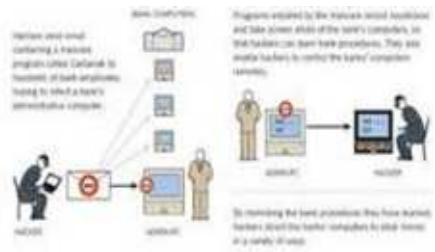
Delincuencia ya no clona tarjetas, ahora hackea chips de bancos

por OCTUBRE 18, 2016 / PERIODICO CENTRAL

Las tecnologías en tarjetas de débito y crédito que los bancos proporcionan a sus cuentahabientes ya no son seguras, y es que los ciberdelincuentes han encontrado la forma de inmiscuirse en páginas web de bancos y hackear los chips de las tarjetas de las instituciones bancarias. Por lo menos el 74% de las 3.6 millones de quejas de bancos recibidas en el primer semestre del año, se relacionaban con asuntos de fraude a través de sitios web de la banca, comercios y aplicaciones para dispositivos móviles.

Incluso en el mismo periodo de tiempo, pero de 2015, el 90% de las quejas se relacionaron con este tema. En este año, de enero a junio, 2 millones de quejas se relacionaron con fraudes de este tipo en tarjetas de crédito, mientras que, en tarjetas de débito, fueron 1.1 millones de quejas. En comparación con las estadísticas de quejas en 2015, este año aumentó por lo menos en 39 y 60% respectivamente. De tal forma que las quejas por fraude en bancas por internet y aplicaciones aumentó de 43 a 51% en tarjetas de crédito en número de quejas por cada 10 mil operaciones y en débito de 5 a 7. Hay quienes se dedican a buscar defraudar por medio de comercios, medios electrónicos y dispositivos móviles. Los ataques continuarán porque ahora no lo hacen las personas, sino máquinas que están todo el tiempo trabajando para identificar una oportunidad o una debilidad.

Fuente: **http://www.periodicocentral.mx/2015/nacional-seccion/delincuencia-ya-no-clona-tarjetas-ahora-hackea-chips-de-bancos**



Baja 8% asalto a sucursales; sube 175% ciberdelitos: Condusef

por OCTUBRE 18, 2016 / CRONICA

Mientras que el asalto a sucursales bancarias disminuyó 8% en el último año, los delincuentes han aprovechado la tecnología para migrar la forma de hacer fraudes y robos a través de los mecanismos digitales, que, según la Condusef, han destacado por haber aumentado hasta 175% las quejas en un año. Entre 2015 y lo que va del año, el banco Santander México detectó 3 mil sitios de internet falsos, informó Omar Herrera, director de Riesgo Tecnológico de la Institución.

En el marco de la presentación de la Suite Digital Santander, la nueva plataforma de servicios financieros digitales, el directivo explicó que los sitios, que ya fueron cerrados, presentaban a los usuarios el logotipo de Santander con alguna oferta crediticia, pero al darle clic a esta imagen, les pedían a los clientes sus datos confidenciales para después cometer un fraude. Agregó que con la adopción de productos y plataformas que ofrecen servicios financieros a través de internet y móviles, se ha visto un incremento en el esfuerzo de los delincuentes por defraudar a los clientes, por lo que las instituciones han tenido que incrementar su vigilancia o intensificar sus sistemas de seguridad en los procesos digitales.

Fuente **http://www.cronica.com.mx/notas/2016/990314.html**

Odín: una nueva versión del ransomware Locky

por OCTUBRE 19, 2016 / SILICON

Odín es el nuevo ransomware activo, es una variante del criptomalware Locky, cuya principal diferencia es que la extensión de los archivos cifrados lleva ".Odín". Se distribuye camuflado en los archivos adjuntos, documentos de Office o archivos comprimidos, de correos electrónicos no deseados que una vez ejecutados descargan el código malicioso e inician el cifrado de directorios locales y unidades de redes compartidas.

La forma más sencilla de minimizar las consecuencias del malware es establecer una política regular de copias de seguridad que, además, deben estar alojadas en un medio físico no conectado a la red principal. Mantener los equipos completamente actualizados, no solo el sistema operativo y el navegador sino todos los programas instalados. Además, usar de forma permanente los equipos con cuentas de administrador facilita la entrada de este ransomware y cualquier otra amenaza por lo que utilizar el control de cuentas y establecer privilegios de uso permite bloquear posibles ataques.

Fuente: **http://www.silicon.es/odin-una-nueva-version-del-ransomware-locky-2320962?utm_content=buffer82de1&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

Descubren dos vulnerabilidades críticas en Apache OpenOffice

por OCTUBRE 18, 2016 / SOFT ZONE

Una de las técnicas más utilizadas por los ciberdelincuentes es la de esconder macros y exploits dentro de documentos aparentemente inofensivos y al ejecutarlos, se pueda llegar a tomar el control del sistema de la víctima. Expertos de seguridad han descubiertos dos vulnerabilidades críticas en esta suite ofimática en la versión 4.1.2 y anteriores de la suite. La primera ha sido registrada como CVE-2016-6803 y se encuentra presente dentro del propio instalador de la suite ofimática, y los ciberdelincuentes podían explotar esta vulnerabilidad para ejecutar otras aplicaciones troyanizadas incluso con permisos de administrador en el sistema.

La segunda es la registrada como CVE-2016-6804, también se encuentra presente en el instalador de la suite, permitiendo a los cibercriminales cargar librerías DLL falsas y maliciosas que les deje ejecutar código arbitrario en la memoria de los sistemas afectados. Para protegernos debemos tener nuestra suite ofimática actualizada, al menos, a la versión 4.1.3. La cuál se puede descargar de forma gratuita desde su página web principal.

Fuente: **http://www.softzone.es/2016/10/18/descubren-dos-vulnerabilidades-criticas-apache-openoffice/?utm_content=bufferedc54&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

Más de la mitad de versiones antiguas de Android están afectadas por el troyano Ghost Push

por OCTUBRE 17, 2016 / SILICON

El troyano conocido como Ghost Push infecta hasta la versión cinco, Android Lollipop, que sigue en uso por alrededor del 57% de los usuarios del sistema operativo móvil. Hasta el momento, esta familia de troyanos representa la mayoría de las infecciones. El malware es capaz de acabar con casi todas las versiones de Android, excepto Android 6.0.

Tanto Android Marshmallow como Android Nougat no se ven afectadas, se recomienda a los usuarios actualizar a las últimas versiones del sistema tan pronto se presenten en el mercado. La mayoría de las infecciones provienen de instalaciones de malware de aplicaciones piratas y de código abierto fuera de la tienda Google Play. 39 aplicaciones originales, incluyendo versiones falsificadas, han facilitado la propagación del troyano, entre las que se encuentran WiFi Enhancer, Amazon, Super Mario, Memory Booster y Wordlock. Más de 20 nuevas variantes del malware instalado en aplicaciones de Android está infectando a unos 600.000 usuarios al día.

Fuente: **http://www.silicon.es/mas-la-mitad-las-versiones-antiguas-android-estan-afectadas-troyano-ghost-push-2320671?utm_content=buffer04c3d&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

CryPy, un ransomware que utiliza una clave para cada archivo cifrado

por OCTUBRE 16, 2016 / REDES ZONE

CryPy, realiza el cifrado de la información en equipos infectados utilizando una clave para cada uno de los archivos, dificultando la recuperación de la información de forma gratuita. Los ciberdelincuentes se han apoyado de una vulnerabilidad existente en una tienda en línea que hace uso de una versión desactualizada de Magento, y así guarda varias copias de este ransomware en la misma y utiliza la misma como servidor de control, permitiendo un ahorro en costo a los ciberdelincuentes. Es más común que se utilicen servidores de otras personas para dar cobijo a la amenaza y el propio servidor de control, ya que es común que los usuarios descuiden la seguridad de estos servicios.

Este servidor además de controlar las copias instaladas en los dispositivos Windows, es capaz de dirigir campañas spam que se realizan para distribuir el ransomware, detectando que se utilizan sobre todo mensajes falsos de PayPal informando sobre problemas que no existen en la cuenta. Existen dos archivos, boot_common.py y encryptor.py que son los únicos que llegan al equipo del usuario, cuando se ejecuta el primero para desactivar el Administrador de tareas o el registro de Windows, y evita que el usuario pueda resolver el problema de forma sencilla.

Fuente: **http://www.redeszone.net/2016/10/16/crypy-ransomware-utiliza-una-clave-archivo-cifrado/?utm_content=buffer1f7da&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

El malware StrongPity se distribuye a través de instaladores falsos de WinRAR y TrueCrypt

por OCTUBRE 13, 2016 / REDES ZONE

Kaspersky ha localizado una amenaza conocida con el nombre de StrongPity que se está distribuyendo utilizando instaladores de dos softwares muy conocidos: WinRAR y TrueCrypt. Se ha encontrado en páginas web falsas y otros de descarga de software donde no se verifica el contenido de los instaladores.

Kaspersky ha detectado sitios web falsos de ambas herramientas que están distribuyendo estos instaladores, confundiendo a los usuarios que solo acceden a las páginas ofrecidas por los buscadores que aparecen entre los primeros resultados. También juegan un papel importante las redes sociales, de hecho, este lugar es el que en realidad se está utilizando para anunciar estas páginas web. Se recomienda recurrir siempre a las páginas oficiales del producto software.

Fuente: **http://www.redeszone.net/2016/10/13/el-malware-strongpity-se-distribuye-a-traves-de-instaladores-falsos-de-winrar-y-truecrypt/?utm_content=buffer2a252&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

PayPal es la principal empresa utilizada por los hackers para los ataques de phising

por OCTUBRE 17, 2016 / PORTALTIC

Check Point Software Technologies, ha detectado un aumento de ataques de 'phishing' o suplantación de identidad lanzados por los hackers haciéndose pasar por la empresa PayPal, con el objetivo de conseguir información sensible o dinero, ya que esta empresa destaca por su popularidad y la gran cantidad de información personal de cada usuario que contiene. Por lo que Check Point aconseja: Fijarse en el emisor. Los e-mails oficiales de Paypal siempre tendrán como remitente una dirección de correo acabada en @paypal.com. Revisar faltas ortográficas, 'Links' falsos. Los hipervínculos enviados mediante ataques de suplantación de identidad no cuentan con el protocolo 'https' (lo que nos indica que la web es segura) ni incluyen la dirección www.paypal.com. Paypal siempre saluda a sus clientes con su nombre y apellidos. Una característica en estos tipos de ataque es que se amenaza a los usuarios con perder su cuenta si no actualiza datos. Las empresas nunca piden información privada por correo electrónico.Paypal no envía archivos adjuntos por correo. No abrir documentos por e-mail si no se conoce la fuente de procedencia.
Un antivirus no es una protección eficaz, es necesario contar con un Sistema de Prevención de Intrusos (ISP) que monitorice el tráfico de red y busque actividades maliciosas para evitar y detener este tipo de ataques.

Fuente: **http://www.europapress.es/portaltic/internet/noticia-paypal-principal-empresa-utilizada-hackers-ataques-phishing-20161017145523.html?utm_content=buffer9d51c&utm_medium=social&utm_source=twitter.com&utm_campaign=buffe**

TOTALSEC NEWSLETTER – INFOSEC

BOLETÍN No. 35

Octubre 15- 23, 2016

Elaboración: Octubre 24, 2016

totalsec