2015-01-24

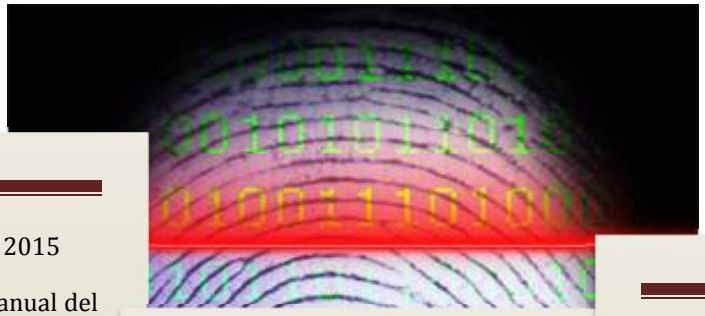
CyberNoticias # 001

SCProgress

www.scprogress.com

ÍNDICE

Noticia # 01: Recrean huellas dactilares a distancia, a partir de fotografías.



Jueves, 01 de enero del 2015

Durante la 31 reunión anual del Chaos Computer Club (CCC) celebrada este pasado fin de semana en Alemania, el experto en biometría Jan Krissler (aka Starbug) ha denunciado la debilidad de muchos sistemas de autenticación basados en parámetros biométricos. Para ello, hizo una demostración en directo de cómo se puede engañar a un lector de huellas. Krissler informó, además, de que ya es posible reproducir las huellas de un individuo tomando fotografías de sus manos.

Durante su presentación, afirmó que había recreado las huellas dactilares de la ministra alemana de defensa Ursula von der Leyen simplemente a partir de fotos de sus manos a distintos ángulos tomadas durante una rueda de prensa. Las distintas fotografías se trataron posteriormente con un software comercial especializado en detectar huellas rotadas o deformadas. La presentación completa de Krissler (en alemán) se puede encontrar en YouTube y en los archivos del CCC. La recreación de la huella de la ministra se trata muy brevemente a partir del minuto 27 del vídeo.

En el pasado, ya se demostró la facilidad para obtener huellas dejadas por una persona al tocar objetos con superficies pulidas como un vaso o la pantalla de un smartphone. Ahora, ya es posible recrear las huellas a distancia, a partir de fotografías.

Fuente: barrapunto.com

Noticia # 02: **Cuenta de Twitter del periódico francés "Le Monde" fue hackeada.**

Miércoles, 21 de enero del 2015

PARÍS.- La cuenta de Twitter del periódico francés "Le Monde" fue hackeada esta noche de martes por el desconocido "Ejército Electrónico de Siria". En la cuenta se publicaron varias imágenes, entre otras, una en la que se leía "Soy un Charlie manipulado" o "No soy Charlie". Estas palabras eran con las que se hacía referencia a "Yo soy Charlie", lema internacional en repudio de los ataques islámicos terroristas perpetrados a principios de enero contra la revista "Charlie Hebdo" en París. Entre las imágenes también podía verse el escudo nacional sirio acompañado de la frase "el Ejército Electrónico de Siria estuvo aquí". En otros mensajes se instaba a respetar la fe de otros. Poco después la cuenta fue suspendida.

Fuente: http://www.emol.com/

Noticia # 03: El Estado Islámico declara la guerra psicológica al Ejército de EE.UU.

Viernes, 16 de enero del 2015

El 12 de enero pasado un grupo de piratas informáticos simpatizantes con el Estado Islámico 'hackeaba' la cuenta oficial de Twitter del Mando Central del Ejército de Estados Unidos y filtraba un documento de 52 páginas con direcciones, correos electrónicos y otra información privada de generales estadounidenses retirados. Bloomberg concluye que las filtraciones son una nueva arma psicológica de los terroristas contra el Ejército estadounidense.

Esa semana funcionarios del Pentágono han comenzado a llamar a los generales retirados para hacerles saber que sus direcciones, correos electrónicos privados y otra información personal habían aparecido en un documento que fue difundido a nivel mundial por un grupo que afirma apoyar al Estado Islámico. Las llamadas telefónicas se iniciaron después de que las cuentas del Mando Central del Ejército de EE.UU. en Twitter y YouTube fueran 'hackeadas'.

Fuente: http://actualidad.rt.com/

El Pentágono, que califica el ataque de "vandalismo cibernético", subraya que los activistas no tuvieron acceso a ninguna información militar secreta. La publicación de los datos personales de los militares retirados es parte de una estrategia terrorista que tiene como finalidad aterrorizar a los profesionales del Ejército, escribe Bloomberg.

El presidente del Comité de Servicios Armados del Senado, John McCain, reveló que fue informado por el Pentágono que el Ejército estadounidense estaba haciendo esfuerzos para monitorear la red en busca de las filtraciones de Twitter, porque potenciales terroristas que no participaron en la operación de 'hackeo' ahora tienen acceso a información sensible.

Bruce Hoffman, director de estudios de seguridad en la Escuela de Servicio Exterior de la Universidad de Georgetown, aseguró que la filtración de información privada refleja el uso de "un arma de guerra psicológica". Hoffman advirtió de que los terroristas "son bastante inteligentes" y conocen perfectamente el impacto que pueden tener estas técnicas psicológicas.

Fuente: http://actualidad.rt.com/

Noticia # 04: **Un desertor confiesa cómo funciona la organización de 'hackers' más secreta del mundo.**

Jueves, 25 de diciembre del 2014

"Corea del Norte tiene algunos de los mejores piratas informáticos del mundo", admite 'Business Insider'. Según la web, para el Gobierno de Pionyang la preparación de sus 'guerreros cibernéticos' es una prioridad desde hace décadas, y menciona el Buró 121, supuestamente una unidad especial de ciberguerra.

Jang Se-yul, un joven que desertó en 2007 de Corea del Norte, se graduó en su momento de la Universidad Mirim, la más prestigiosa en ingeniería (actualmente llamada Universidad de Automatización). Después de graduarse, trabajó en el Buró General de Reconocimiento, la agencia de inteligencia de la que el misterioso Buró 121 forma parte.

En realidad, el propio Jang, que hoy en día lidera en Corea del Sur un grupo llamado Frente de Liberación del Pueblo Norcoreano, no era 'hacker'. Sin embargo, pudo confesar a 'Business Insider' detalles internos del funcionamiento de la red nacional de piratas informáticos de élite de Corea del Norte.

Fuente: http://actualidad.rt.com/

Entrenamiento

Por el Buró 121 habrán pasado unos 1.800 'guerreros cibernéticos'. Todos ellos son sofisticados piratas informáticos con casi nueve años de intenso entrenamiento a sus espaldas en el momento en que son contratados.

La fuente principal de personal para el Buró 121 es la Universidad Mirim de Pionyang. La piratería informática es un campo muy competitivo, y lo demuestra el hecho de que cada clase acepta solo un centenar de estudiantes de los 5.000 que solicitan ingresar. Los principales conocimientos que deben tener los universitarios es cómo desarrollar sus propios virus y programas de 'hackeo' sin basarse en programas ya creados en el extranjero.

Trabajo

Una vez contratados, los piratas informáticos se dividen por grupos que se centran cada uno en un país en particular. Los dos primeros años en el servicio, los 'hackers' los pasan viajando a su país 'objetivo', estudiando su idioma y su cultura. El propósito final del Buró es asaltar las infraestructuras informáticas, especialmente las gubernamentales, de los Estados que consideran enemigos, y obtener toda la información posible, además de crear confusión social.

Fuente: http://actualidad.rt.com/

Noticia # 05: **La NSA hackeó a Corea del Norte antes de que lograran hackear a Sony**

Martes, 20 de enero del 2015

La guerra cibernética no es ninguna broma: es 100% real y los países la están librando desde hace años. Más que destruir, aquí lo que se busca es robar información y secretos de todo tipo. De seguro recordarán que recientemente Estados Unidos indicó que Corea del Norte se encontraba detrás del hackeo a Sony, como venganza por el lanzamiento de la película The Interview.

¿Pero cómo pudo estar el gobierno estadounidense tan seguro al lanzar esta acusación, cuando incluso se hablaba de que un grupo de hackers se había hecho pasar por el gobierno norcoreano? De acuerdo con "nuevos" documentos de Edward Snowden, que recientemente han salido a la luz, los sistemas informáticos de Corea del Norte están comprometidos desde hace años, y las agencias de inteligencia de Estados Unidos pueden ingresar en sus servidores cuando se les da la gana.

Al parecer, la NSA aprovechó la alianza de Estados Unidos con Corea del Sur para instalar malware en las redes de Corea del Norte, lo cual permitió que años más tarde pudieran reunir información suficiente para acusar al mencionado país de ser los responsables del hackeo a Sony. Esto de todas formas lleva a que nos preguntamos por qué la NSA, al tener información sobre los planes del gobierno norcoreano, no lanzó una advertencia a Sony. Sucede que en realidad la NSA no estaba totalmente enterada de los planes de Corea del Norte, ya que desconocían la magnitud del ataque que sería lanzado y calculaban que no provocaría tantos destrozos en los servidores de Sony como terminó provocando.

La evidencia con la que contaba el gobierno fue la suficiente como para que Obama rápidamente acusara al gobierno de Kim Jong-Un como el responsable del ataque, resultando en la primera ocasión en que Estados Unidos realiza una acusación en forma tan directa contra Corea del Norte.

Fuente: http://noticias24carabobo.com/