2013-06-13

Boletín de Noticias de Seguridad Informática # 5

SCProgress

www.scprogress.com

ÍNDICE

NOTICIA 1: Robo de identidad por 30 Euros a través de tarjetas de crédito Wi-Fi Contact-Less.

30 millones de titulares de tarjetas de débito y de crédito están en riesgo de que sus datos personales sean extraídos por ladrones.

Estos ladrones de identidad que explotan vulnerabilidades en la última tecnología de pago con tarjetas de créditos "sin contacto".

Los números de la tarjeta y los datos personales pueden ser leídos casi al instante por un dispositivo remoto, tal como un teléfono móvil. Las tarjetas Contact-less han estado en uso durante al menos cinco años y son cada vez más populares, ya que ahorran tiempo para los minoristas y los clientes, al agilizar las transacciones.

Los clientes los usan para pagar artículos menos costosos (U$S20 o menos) sin tener que introducir un número PIN o buscar dinero en efectivo. En su lugar, sólo tiene que escanear el plástico sobre un lector electrónico en la caja.

puede ser usada por ladrones y estafadores. Cualquier extraño que haya encontrado o robado una de las tarjetas podría utilizarla para realizar gastos a pequeña escala ya que sól se requiere un PIN después de cinco transacciones en un día.

Y esta semana The Mail on Sunday fue testigo de cómo los detalles de las tarjetas pueden ser copiados sin cables, mediante un teléfono de pantalla táctil ymodificado con partes compradas en Internet por tan sólo 30 EUR.

A través de un teléfono "ajustado" por el experto en seguridad Emms Martin y su equipo de investigadores en el Centro de la Universidad de Newcastle, fueron capaces de acceder a las últimos diez operaciones realizadas en la cuenta de la víctima.

Con sólo sostener el teléfono cerca de una cartera, se pueden descargar los datos en dos segundos, lo que alimenta los temores de que la tecnología podría ser explotada por los ladrones en una multitud. Además, la víctima inocente desconoce que sus datos han sido robados hasta recibir su estado de cuenta bancaria mientras que la información robada puede utilizarse para realizar compras en línea y no requiere un código de seguridad adicional.

Fuente: Segu-Info.com

NOTICIA 2: Obama y Xi Jinping discuten sobre ciberseguridad y Corea Norte.

El presidente de Estados Unidos, Barack Obama, y su homólogo chino, Xi Jinping, acordaron el sábado que Corea del Norte debe renunciar a sus armas nucleares, en medio de una cumbre en la que el líder demócrata expresó directamente la preocupación de su país sobre la seguridad informática.

Obama y Xi abordaron un amplio rango de temas, incluyendo una charla al aire libre de 50 minutos, al final de una visita de acercamiento que incluyó una extensa discusión sobre cómo moderar a Corea del Norte, cuya retórica beligerante en los últimos meses ha alarmado a la región del Asia-Pacífico y también a Estados Unidos.

"Ellos acordaron que Corea del Norte debe desnuclearizarse, que ningún país aceptará a Corea del Norte como un estado con armas nucleares y que trabajarían juntos para mejorar la cooperación y el diálogo a fin de lograr la desnuclearización", dijo a periodistas el asesor de seguridad de la Casa Blanca, Tom Donilon.

El canciller de Estado chino, Yang Jiechi, afirmó en una conferencia de prensa por separado que Xi dijo a Obama que ambos países tenían "las mismas posiciones y objetivos" sobre la disputa nuclear con Corea del Norte.

China es el principal aliado de Pyongyang pero está cada vez más preocupado por las amenazas de Corea del Norte de iniciar una guerra contra Corea del Sur.

En un encuentro que podría haber establecido el tono de las relaciones entre ambos países para los próximos años, los dos líderes pasaron alrededor de ocho horas juntos el viernes y el sábado en un lujoso complejo cerca de Palm Springs, California.

La cumbre informal buscaba inyectar cierta calidez a unas relaciones a menudo distantes, a fin de que ambos mandatarios pudieran hablar de sus diferencias abiertamente.

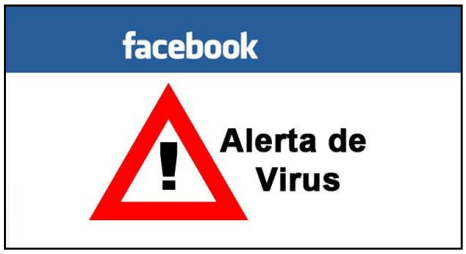
Donilon dijo que Obama expresó directamente con Xi los reclamos de Estados Unidos respecto a los ciberataques chinos que buscaban acceder a secretos industriales estadounidenses.

El presidente estadounidense explicó a su par chino que de no ser solucionados, esta clase de asuntos se convertirían en "un problema muy complejo en la relación económica", agregó Donilon.

Yang, en tanto, dijo a los periodistas que Pekín buscaba cooperación en lugar de fricción con Estados Unidos en torno a la ciberseguridad.

Fuente: http://seguinfo.wordpress.com

NOTICIA 3: Sanción de 40.000 euros por difundir un troyano en Facebook.



"FACUA denunció ante la Agencia Española de Protección de Datos que algunos usuarios de la popular red social estaban recibiendo mensajes"

Estaban recibiendo mensajes que les invitaban a ver fotos o vídeos con el único propósito de expandir un troyano. Los mensajes del tipo "Has visto …?" o "sabes que sales en un vídeo?" intentaban engañar a los receptores con su tono coloquial. Finalmente, el asunto se ha saldado con una sanción de 40.000 euros por difundir un troyano a través de la red social Facebook. El portal especializado en el anonimato en la red www.salirdeinternet.com, nos da más detalles sobre la sanción recibida por una empresa por la difusión de un troyano en Facebook. La denuncia promovida por FACUA indica que esas nuevas páginas informaban de que se requería la instalación de un complemento para el navegador que permitiese visualizar el video.

Al pulsar en el enlace lo que en realidad se descargaba era un programa para utilizar el perfil de Facebook del afectado para transmitir el mensaje inicial a los amigos del usuario afectado.

El programa descargado, además de propagar el mensaje inicial, solicitaba un número de línea de telefonía móvil que era utilizado para suscribir a los afectados a un servicio de tarificación adicional (SMS Premium).

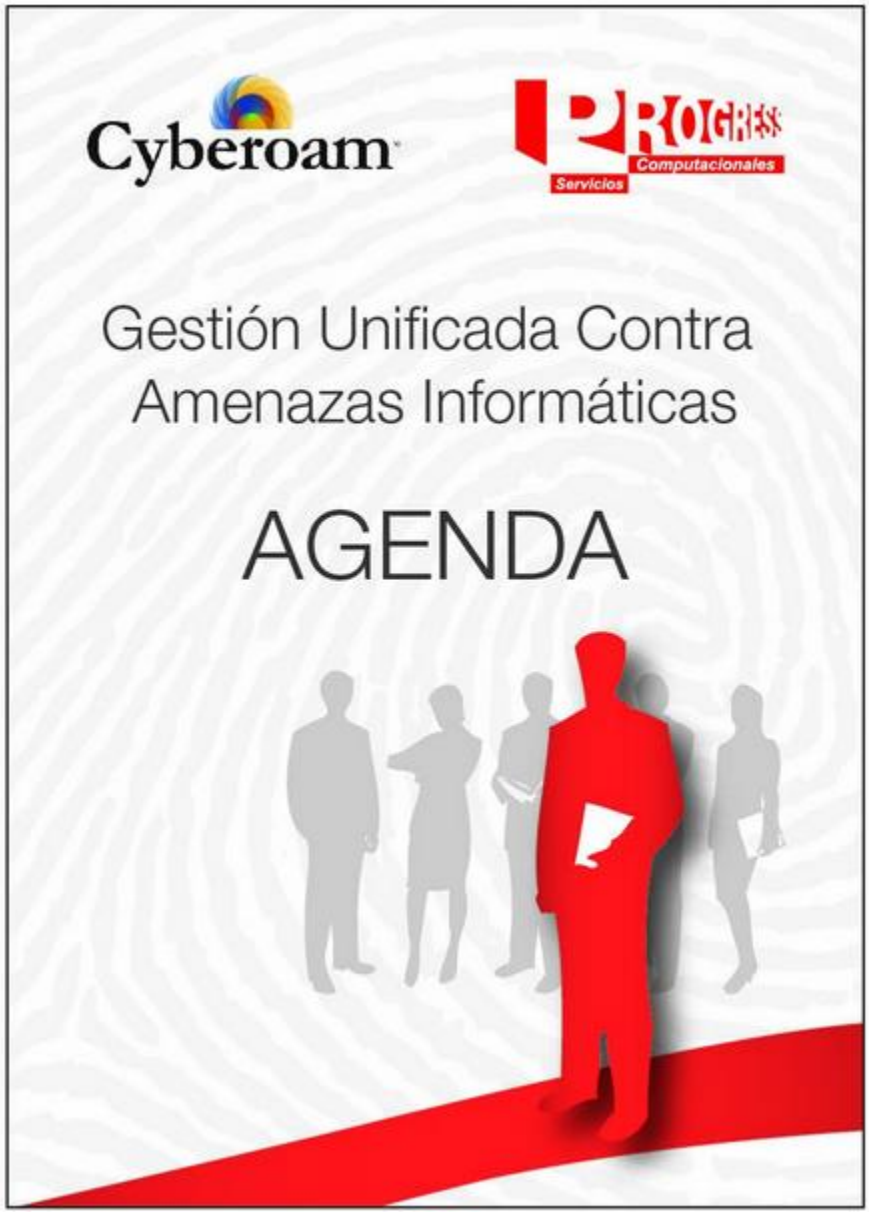
Los usuarios solían ser redirigidos a web alojadas en blogspot que imitaban la apariencia de Facebook. Como sabemos, Google es propietaria de esta plataforma de blogs y se negó a identificar a las personas que estaban detrás del engaño.

La AEPD tuvo que pedir explicaciones a la web responsable de las suscripciones Premium, quien afirmo que todo provenía de las agencias que habían contratado e intentó hacer todo lo posible por poner fin al engaño.

Incluso se publicó una nota de prensa en Europa Press para intentar explicar lo sucedido y se denunciaron los hechos ante la Brigada de Investigación Tecnológica, que intentó sin éxito ponerse en contacto con una de las agencias señalada como responsable. Finalmente, la AEPD ha decidido imponer varias sanciones. En primer lugar, una de las agencias publicitarias ha sido condenada a pagar 40.000 euros mientras que la propietaria de los servicios de SMS Premium ha sido multada con 6.000 euros, después de valorar su buena fe en todo el proceso. Cada cierto tiempo conviene revisar que aplicaciones tiene acceso a nuestros perfiles de redes sociales, con el fin de deshabilitar aquellas sospechosas.

Fuente: elhacker.NET

NOTICIA 4: Agenda del Seminario de Seguridad Informática Perimetral.



SERVICIOS COMPUTACIONALES PROGRESS

SISTEMAS DE SEGURIDAD INFORMATICA INTELIGENTE

08:30 - 09:00	Registro
09:00 - 09:10	Introducción
09:10 - 09:35	Conceptos Básicos de seguridad y networking
09:35 - 10:00	Cyberoam Identity Based UTM
10:00 - 10:20	Información general sobre productos marca Cyberoam
10:20 - 10:30	Preguntas y premios
10:30 - 10:50	Coffe Break
10:50 - 11:10	Cyberoam despliegue en la red
11:10 - 11:35	Firewall
11:35 - 12:00	Formas de autenticación de los usuarios
12:00 - 12:25	Diferentes alternativas para el filtrado de contenidos
12:25 - 12:40	Alternativa para minimizar el riesgo infórmatico, Application filter
12:40 - 12:50	Gateway Anti-Virus / Anti-Spam
12:50 - 13:00	Preguntas, respuestas y premios
13:00 - 13:50	Almuerzo Buffet
13:50 - 14:10	Sistema Detector de Intrusos y Prevención (IDS & IPS)
14:10 - 14:30	Virtual Private Network (VPN)
14:30 - 14:55	Gestión de enlases redundantes (Multilink Manager)
14:55 - 15:20	Routing & Qos
15:20 - 15:45	Administración general y reportes
15:45 - 16:00	Preguntas, respuestas y premios
16:00 - 16:20	Coffe Break
16:20 - 16:40	Preguntas, respuestas
16:40 - 16:55	Sorte del premio mayor entre los participantes del seminario
17:00	Clausura del evento