2013-10-07

Boletín de Noticias de Seguridad Informática #17

SCProgress

www.scprogress.com

ÍNDICE

NOTICIA 1: Avira detecta malware con WhatsApp como gancho

La multinacional experta en seguridad AVIRA detecta malware con WhatsApp como gancho

La multinacional experta en seguridad **AVIRA** ha lanzado una alerta al detectar la distribución masiva de una campaña de malware que se hace pasar por el servicio de buzón de voz de WhatsApp.

El usuario recibe el mensaje como "You have a new voicemail", "1 New Voicemail(s)" (or 4) que ocultan emails que pretenden proceder del popular servicio de mensajes a través de dispositivos móviles.

Se incluye en este email un botón que redirige al usuario a diversas URLS maliciosas con la posibilidad de descargar

Este tipo se técnica de ingeniería social se está empezando a utilizar, afirma Sorin Mustaca, experto en seguridad IT en Avira, empujado por "la atención que está captando el servicio de WhatsApp como modelo de negocio gratuito" (en el caso de la versión para iOS, es gratuito durante el primer año).

Según WhatsApp, el servicio de buzón de voz por email está diseñado de forma estandarizada para poder soportar diferentes dispositivos y "esto es exactamente lo que los cibercriminales están utilizando para esta campaña de spam", añade Mustaca.

Fuente: http://www.noticias2d.com

NOTICIA 2: **Revelaciones de Snowden llevan a advertencia sobre fórmula de seguridad informática**

En las últimas consecuencias de las revelaciones de inteligencia de Edward Snowden, una importante empresa de seguridad informática estadounidense advirtió a miles de clientes el jueves que dejen de usar un software que se basa en una débil fórmula matemática desarrollada por la Agencia de Seguridad Nacional (NSA, por su sigla en inglés).
RSA, la división de seguridad de la empresa de almacenamiento EMC Corp, dijo a sus clientes actuales en un correo electrónico que un conjunto de herramientas para los desarrolladores tenía un generador por defecto de números aleatorios que utiliza la fórmula débil y que los clientes deberían cambiarse a una de varias otras fórmulas en el producto.

La semana pasada, el New York Times reportó que el caché de documentos de Snowden del período en que trabajó para un contratista de la NSA mostraba que la agencia utilizó su participación pública en el proceso para establecer estándares de criptografía voluntarios, a cargo del Instituto Nacional de Estándares y Tecnología del Gobierno, para proponer una fórmula que sabía que podría vulnerar.

El NIST (por su sigla en inglés), que aceptó la propuesta de la NSA en el 2006 como uno de cuatro sistemas aceptables para uso del Gobierno, dijo esta semana que reconsiderará esa inclusión por las dudas sobre su seguridad.

Pero la advertencia de la RSA pone de relieve cómo la lentitud en el lento proceso de actualización de normas y las prácticas de la industria podrían dejar a muchos usuarios expuestos a la piratería por parte de la NSA y otros que podrían explotar el mismo defecto en los próximos años.

RSA no tenía comentarios inmediatos. No estaba claro cómo la empresa podría llegar a todos los antiguos clientes de sus herramientas de desarrollo y mucho menos cómo esos programadores podrían a su vez llegar a todos sus clientes.

Fuente: http://lta.reuters.com

NOTICIA 3: Diez consejos para mantener la seguridad en internet

Miguel Sumer Elías y Joel Gómez Treviño son dos de los pocos abogados que se dedican al derecho informático en la región. A través de América Directo respondieron las dudas de los usuarios.

A continuación, un decálogo de consejos para proteger de virus a tu computadora y evitar así que espíen y roben tu información.

1. No descargar archivos de foros cuya reputación desconoces, sin importar si esos programas se presentan como antivirus.

2. No abrir documentos adjuntos de mails enviados por tus amigos si no estás completamente seguro de que fueron enviados por ellos. Un hacker pudo haberlo mandado luego de intervenir la cuenta de tu conocido.

3. Utilizar el servicio de homebanking sólo si el banco ofrece estrictas medidas de seguridad para operar en la web.

La Policía arrestó a un "súper hacker" de 19 años que robaba hasta u$s50 mil por mes en la web. El caso puso en tela de debate la seguridad informática de los argentinos. Dos especialistas dan consejos para evitar fraudes.

Hay que tener en cuenta que las entidades bancarias están en mejores condiciones que los usuarios para evitar el robo de datos.

4. No hacer operaciones bancarias en computadoras públicas, como las de cibercafés, que suelen estar altamente infectadas.

5. Tener actualizada la computadora, no sólo el antivirus, sino cualquier programa.

6. Usar programas originales. No hacer descargas de sitios no oficiales.

7. No ingresar en páginas web que no consideres del todo confiables.

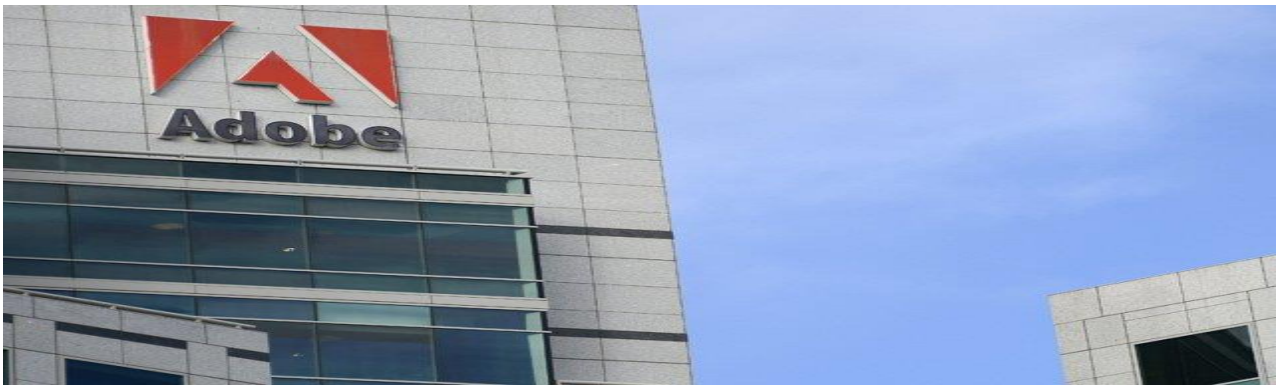
8. Ser muy cauteloso con la información que se decide compartir, porque una vez que algo se sube a internet no se puede borrar nunca más.

9. En caso de sufrir robo de identidad o de información, no denunciarlo inmediatamente a las autoridades porque por la ignorancia que hay sobre estos temas puede terminar empeorando la situación. Acudir primero a un abogado especializado para recibir asesoramiento.

10. No contaminar la evidencia. Conservar intactos los documentos y archivos dañados o robados, así los investigadores estarán en mejores condiciones de descubrir a los delincuentes.

Fuente: http://www.infobae.com

NOTICIA 4: Adobe sufre un ataque informático que compromete datos de clientes



La compañía tecnológica indicó en su blog oficial que se trata de ´ataques sofisticados´ y que los atacantes accedieron a la identificación y contraseñas de los usuarios.

Adobe anunció que sus servidores sufrieron un ataque informático y que los "crackers" tuvieron acceso a información personal de 2,9 millones de clientes y al código fuente de algunos productos.

La compañía tecnológica indicó en su blog oficial que se trata de "ataques sofisticados" y que los atacantes accedieron a la identificación y contraseñas de los usuarios, así como a datos como sus nombres, números encriptados de tarjetas de crédito y débito o fecha de caducidad de las mismas.

"Por el momento, no creemos que los atacantes accedieran en nuestros sistemas a números desencriptados de las tarjetas de crédito y débito", matizó la compañía.

Adobe pidió disculpas y explicó que trabaja con socios externos y con los cuerpos de seguridad para solucionar el "incidente".

Como medida de precaución está borrando contraseñas de algunos clientes, a los que aconseja que cambien sus datos en otros servicios de internet si usaban en ellos los mismos nombres de usuario y claves.

Además, está informando a los usuarios cuya información bancaria se ha visto comprometida sobre cómo tienen que actuar y ha pedido la colaboración de las entidades financieras para que contribuyan a proteger las cuentas de los clientes.

Fuente: . http://www.rpp.com.pe