

2013-05-23

**Boletín de Noticias de
Seguridad Informática # 2**



SC Progress

www.scprogress.com

ÍNDICE

1. En Twitter roban una cuenta al día.....	03
2. Cientos de webs de Chile, Australia y Suiza han sido hackeado.....	04
3. El 55% de los usuarios usa la misma contraseña en todos los sitios.....	05



NOTICIA 1: En Twitter roban una cuenta al día



“Comienza a ser algo preocupante la facilidad con la que los hackers se apoderan de las cuentas de los usuarios de la red social basada en microblog”.

En un principio, los responsables de Twitter indicaban que era por culpa de los propios usuarios que las cuentas fuesen robadas. Pero llevamos un mes en el que prácticamente se roba una cuenta al día. ¿Existe un fallo de seguridad en la red social que no se ha descubierto?

Evidentemente, los que no habrían descubierto el fallo serían los responsables de la red social, porque algunos hackers si habrían dado con este. Sin embargo, todo esto se trata de una especulación que algunos usuarios están manejando y que podría ser cierta, aunque también existen otras posibilidades.

La otra posibilidad que se maneja es que el ordenador de los usuarios esté infectado con algún tipo de malware y esto propicie que los cyberdelincuentes puedan hacerse con el control de la cuenta.

En este caso, fue la cuenta de Sky News la que se vio afectada y en la que se publicaron

algunos tweets aprovechando que los atacantes tenían total acceso.

¿Por qué tantos problemas de seguridad?

Debido a la magnitud del problema vamos a empezar descartando (aunque no al 100%) que no se trata de un error de Twitter. Por lo que es muy probable que el problema se encuentre en el lado del usuario.

Existen hoy en día muchos programas malware que se instalan en los ordenadores de los usuarios sin que estos sean conscientes y son capaces de llevar tareas una vez que son residentes en el equipo.

La primera de ellas es la robar datos que se encuentran en el equipo y controlar las acciones del usuario cuando este utiliza el navegador, pudiendo producirse el robo de los datos de acceso. También podemos encontrarnos con que el malware posee scripts que detectan cuando el usuario está utilizando la cuenta de la red social. En este caso, utilizando código es capaz de redactar un mensaje y hacer que este se envíe sin que el usuario lo haya redactado y ni siquiera haya pulsado enviar.

Todo esto tiene un origen: que el usuario haya descargado archivos de origen desconocido que estuviesen infectados, o bien haber abierto correos electrónicos con contenido malware.

Sin tener nada claro cuál es el origen de esta oleada de hackers de cuentas, hay que extremar las precauciones con el contenido que visualizamos y descargamos para evitar posibles infecciones malware.

Fuente: www.redeszone.com

NOTICIA 2: Cientos de webs de Chile, Australia y Suiza han sido hackeado.



“El hacker ‘AnonGhost’ de Anonymous ha atacado y modificado aproximadamente 400 sitios web comerciales de Australia, Suiza, Chile y otros países”.

El pirata informático ha desfigurado 140 sitios web de Australia, 180 sitios de Suiza, 68 sitios de Chile y alrededor de una docena de otros países.

A juzgar por el mensaje publicado en los sitios afectados, los ataques forman parte de una protesta antigubernamental.

“A todos los gobiernos del mundo, podemos ver lo que estáis haciendo, os controlamos, estamos por todas partes”, dijo el hacker.

“Juntos nos unimos contra la injusticia de los gobiernos corruptos. Somos Anonymous. Somos Legión. Unidos como uno. Divididos por cero. Nosotros no perdonamos la injusticia. No olvidamos la opresión”, añadió.

Es interesante observar que muchos grupos hacktivistas desfiguran los sitios web de personas inocentes, o de empresas que no tienen nada que ver con los gobiernos, como una forma de protesta.

Fuente: <http://www.seguridadpc.net/>

NOTICIA 3: El 55% de los usuarios usa la misma contraseña en todos los sitios.



Un estudio realizado por Ofcom, el organismo de control de comunicaciones del Reino Unido, ha descubierto algunas estadísticas terribles que ponen de manifiesto lo malo de las contraseñas para la seguridad y el motivo por el cual PayPal quiere deshacerse de las contraseñas en favor de la biometría.

Según el informe UK adults taking online password security risks [PDF], sobre una encuesta de 1.805 adultos,

el 55% de ellos utiliza la misma contraseña para la mayoría de los sitios que visita y tiene al menos 237 contactos en las redes sociales.

¿Por qué es importante?
Si eres miembro de los sitios web X, Y y Z y utilizas la misma contraseña en cada sitio,

si X sufre una fuga de datos y se accede a su base de datos, entonces los malos tendrán acceso a tu cuenta de X, Y y Z.

Además, algo más de una cuarta parte (26%) dice que tienden a usar contraseñas fáciles de recordar, tales como su cumpleaños o los nombres de personas cercanas.

Si deseas fortalecer tu contraseña te recomiendo la lectura de los artículos ¿Por qué caen nuestras passwords? y el Método de creación de contraseñas.

Fuente: Noticias de Seguridad Informática - Segu-Info