# ¿ «Pirateo» de Twitter o vulnerabilidad de las redes sociales?

El masivo pirateo de cuentas en Twitter de políticos, millardarios y compañías el miércoles en Estados Unidos, plantea la pregunta de la seguridad de la red social favorita de Donald Trump y, de manera más amplia, de todas estas plataformas.

Del “modus operandi” hasta las posibles defensas contra los piratas, esto es lo que se sabe de este espectacular ciberataque.

## ¿Qué consecuencias?

Twitter reaccionó rápidamente, desactivando las cuentas concernidas y limitando las posibilidades de compartir mensajes sospechosos.

Financieramente, la estafa parece también de poca envergadura: según el sitio especializado Blockchain.com, que sigue las transacciones efectuadas en criptomonedas, un total de 12,58 bitcoins, es decir cerca de 116.000 dólares, fue enviado a una de las direcciones mencionadas en los falsos tuits.

Por otra parte, fue eso lo que permitió a Twitter limitar el daño: el o los cibercriminales buscaron solo una rápida ganancia, además de llamar la atención con el carácter particulamente espectacular de la operación.

“Twitter fue muy reactivo, tiene visiblemente importantes capacidades de investigación. También jugaron la carta de la transparencia, comunicando de manera regular, algo que le da crédito y es señal de verdadera madurez sobre el tema”, según un portavoz de Clusif (club francés de seguridad de la información).

## Señal de alarma

Las consecuencias pudieron haber sido mucho más graves si los ciberpiratas hubiesen tenidos intenciones políticas, subrayan los expertos.

“Desde un punto de vista político, un tuit falso en un momento crítico podría tener un impacto enorme. Alguien que tuviese acceso a este tipo de cuenta en el buen momento y con el buen

tipo de información falsa podría volcar totalmente una elección", estima en ese sentido Anthony Glees, profesor especializado en seguridad e inteligencia de la Universidad de Buckingham.

"Esta capacidad de controlar un número importante de cuentas certificadas de primer plano en periodo electoral (en Estados Unidos) para tuitear en momentos precisos podría tener un efecto tremendo", confirman en Clusif.

"Aquí, la debilidad demostradas por Twitter es muy preocupante y plantea la pregunta de la importancia de las plataformas sociales en periodo electoral".

Para el profesor Alan Woodward, del centro de ciberseguridad de la Universidad de Surrey, este ataque "muestra que organizaciones como Twitter pueden ser objeto de ataques a través de su personal y que tienen que repensar su funcionamiento".

## ¿Cómo protegerse?

Muchas reglas simples permiten en general evitar los pirateos de cuentas personales: evitar cliquear sobre archivos adjuntos que pueden parecer sospechosos en un correo, no dar el nombre de usuario incluso si lo pide un correo que procede de un servicio utilizado, o recurrir a un sistema de doble certificación.

El problema es que muchas de estas precauciones no hubiesen servido de nada contra el ataque que afectó a Twitter, en caso de que se confirme que se debió a un fallo humano en el interior mismo de la plataforma.

El caso recuerda que "detrás de las máquinas hay seres humanos que pueden tener acceso a nuestros mensajes privados y a las informaciones que colocamos allí. Esos sistemas no son cerrados, lo que se intercambia puede ser accesible", subraya Gérôme Billois.

Con información de agencia AFP y 800 Noticias