Source:
IT Connect

Un experto en seguridad de Kaspersky Lab ha descubierto un ataque de malware que engañó a cerca de 10.000 usuarios de Facebook en todo el mundo e infectó sus dispositivos, después de recibir el mensaje de un amigo que aseguraba que otra persona lo había mencionado en la red social.

Los dispositivos comprometidos se utilizaron para secuestrar cuentas de Facebook, con el fin de propagar la infección a través de los propios contactos de la víctima y permitir otras actividades maliciosas. Las regiones más afectadas fueron América del Sur y Europa, además de Túnez e Israel.

Entre el 24 y 27 de junio, miles de consumidores confiados recibieron un mensaje de un amigo de Facebook diciendo que habían sido mencionados en un comentario. El mensaje había sido iniciado por ciberdelincuentes y desató un ataque en dos etapas. La primera, bajaba un troyano en la computadora del usuario que instaló, entre otras cosas, una extensión maliciosa del navegador Chrome. Esto permitió la segunda etapa, la toma del control de la cuenta de Facebook de la víctima, cuando ésta iniciaba una nueva sesión en la red social a través del navegador comprometido.

Un ataque exitoso le dio al ciberdelincuente la capacidad de cambiar la configuración de privacidad, extraer datos y mucho más, lo que permitió que la infección se propagara a través de los amigos de Facebook de la víctima y realizara, además, otras actividades maliciosas como spam, robo de identidad y la generación fraudulenta de ‘me gusta’ y compartir’. El malware trató de protegerse a sí mismo por el acceso a la lista negra de ciertos sitios web, como los que pertenecen a los proveedores de software de seguridad.

La red de Seguridad de Kaspersky Lab registró alrededor de 10.000 intentos de infección en todo el mundo. Los países más afectados fueron Brasil, Polonia, Perú, Colombia, México, Ecuador, Grecia, Portugal, Túnez, Venezuela, Alemania e Israel.

Disponible en:

http://itconnect.lat/latinoamerica/3723 [1]

Links
[1] http://itconnect.lat/latinoamerica/3723