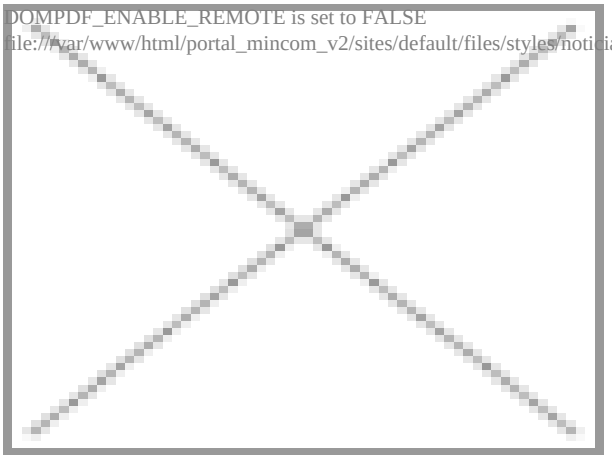
DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/all/themes/mincom/logo.png

DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/default/files/styles/noticias/public/facebook.jpg



Fuente:
TyN Magazine

Parece que, a pesar de los esfuerzos, Facebook sigue teniendo agujeros de seguridad. Ahora, la empresa propiedad de Mark Zuckerberg está investigando un informe según el cual una base de datos con los nombres, números de teléfono y de identificación dentro de la plataforma (ID) de más de 267 millones de usuarios. Información que ha estado expuesta y al alcance de cualquiera.

«Estamos investigando este problema, pero creemos que que se trata de información obtenida antes de los cambios que hicimos en los últimos años para proteger mejor la información de las personas», dijo un portavoz de Facebook a AFP. Según el blog especializado en ciberseguridad « Comparitech», la base de datos, extraída posiblemente por un grupo de cibercriminales de origen vietnamita, estuvo disponible para su descarga en un foro de hackers durante dos semanas. Entre el 4 de diciembre y el 19 del mismo mes. Es decir, ayer.

«La información contenida en la base de datos podría utilizarse para realizar campañas de spam y phishing (estafa en la que se suplanta una fuente legítima para robar datos a la víctima) a gran escala, entre otras amenazas para los usuarios finales», explican en el blog. El investigador Bob Diachenko, que se dedica a buscar en la red bases de datos expuestas, quien descubrió la publicación. Después de que comunicase el hallazgo al proveedor de servicios, la información de los usuarios fue eliminada del sitio.

Según explican en «Comparitech», la mayoría de las personas afectadas son de origen estadounidense. Por el momento, se desconoce el método empleado por los ciberdelincuentes para hacerse con la información, aunque apuntan diferentes posibilidades. De acuerdo con una de ellas, es probable que los datos fuesen adquiridos antes de que la red social restringiera el acceso a los números de teléfono de los usuarios en 2018.

«Podrían haber empleado «scraping». Es un programa que sirve para arañar información de una web. Funciona de forma parecida a que una persona se pusiese a visitar perfiles de forma manual y fuese apuntando nombres ID y números de teléfono en el caso de que el usuario los tuviesen públicos. Si las bases de datos solo cuentan con nombres y teléfonos estamos hablando de información pública. Antes de 2018 Facebook permitía el acceso a los números de los usuarios que los tuviesen publicados», explica a ABC el hacker

Deepak Daswani.

Existe otra posibilidad que se acerca más a lo que hizo Cambridge Analytica en su momento. «Cambridge Analytica se aprovechaba de un fallo de seguridad de Facebook que permitía tener acceso a la información de los «likes» de los usuarios, entre otras cosas, así como de los amigos que tenían en la red social. Según afirman en Comparitech, a pesar de que Facebook ha restringido el acceso a los teléfonos, podría haber algún fallo de seguridad que hayan podido aprovechar los ciberdelincuentes en este caso para acceder a la información», dice Daswani.

Cabe recordar que desde que se conoció el escándalo de Cambridge Analytica, la filtración de los datos de más de 87 millones de usuarios (136.985 españoles), Facebook se encuentra en el ojo del huracán. Investigada en Estados Unidos, la plataforma fue condenada en julio a pagar una multa de 5.000 millones de dólares por su gestión de la privacidad de los usuarios. A su vez, está siendo controlada de cerca por la FTC (Comisión Federal de Comercio) estadounidense.

Sin embargo, en opinión del experto, en lo que respecta a este caso no hay razones para echarse las manos a la cabeza, ya que tanto el nombre de los usuarios como el número de identificación (ID) de Facebook es información pública. Lo mismo ocurre con el número de teléfono para aquellos que no lo tengan privado: «No hay información referente a la contraseña de los usuarios, por lo que no es tan grave. Se trata de información pública y técnica que podría haberse recabado utilizando OSI (Open Source Intelligence), que básicamente consiste en tomar información urilizando sitios web públicos».

Daswani hace hincapié, a su vez, en la importancia de que los usuarios tengan cuidado con la información que comparten en redes sociales. Y es que los números de teléfono resultan muy interesantes a ojos de los ciberdelincuentes, ya que pueden emplearse para realizar ataques de phishing, enviar virus informático o realizar campañas de spam, entre otras cosas.

Disponible en :

https://www.tynmagazine.com/otra-vez-falla-facebook/ [1]

Links
[1] https://www.tynmagazine.com/otra-vez-falla-facebook/