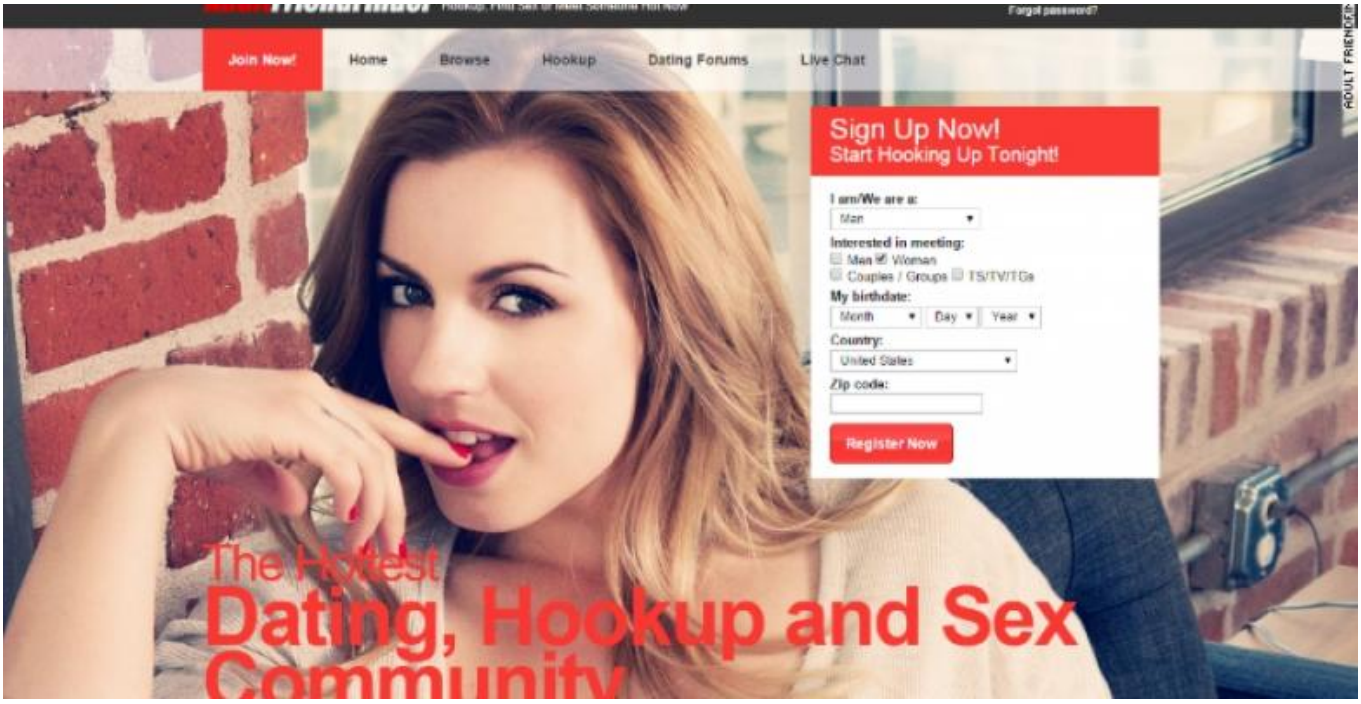
Ciberataque pone al descubierto secretos sexuales de millones de personas

24/05/2015



Adult FriendFinder les pide a los clientes que detallen sus preferencias y, con base en esos criterios, forma parejas para que las personas tengan encuentros sexuales.

El sitio, que cuenta con 64 millones de miembros, afirma haber "ayudado a millones de personas a encontrar parejas tradicionales, grupos de desinhibidos, tríos, y una diversidad de otras parejas alternativas".

La información que recoge Adult Friend Finder es de naturaleza extremadamente personal. Cuando crean una cuenta, los clientes deben informar sobre su sexo, si están interesados en hombres o mujeres y qué tipo de situaciones sexuales desean.

Las sugerencias que Adult FriendFinder brinda para el campo "cuéntales a otros acerca de tí" incluyen "Me gusta que mi pareja me diga qué hacer en la habitación", "Tiendo a ser algo pervertido" y "Estoy dispuesto a probar una forma de juego con cuerdas y vendas".

El ataque, perpetrado en marzo, fue descubierto inicialmente por la consultora independiente de tecnología de la información Bev Robb en su blog Teksecurity, hace un mes. Pero Robb no identificó al sitio que fue objeto del ataque cibernético.

No fue sino hasta esta semana, cuando Channel 4 News de Inglaterra informó sobre el ataque cibernético, que Adult FriendFinder fue identificado como el objeto del mismo.

Parte de la información personal que fue filtrada son las direcciones de correo electrónico de los clientes, nombres de usuario, contraseñas, fechas de cumpleaños y códigos postales, además de sus preferencias sexuales. Aún no se ha dejado al descubierto información de tarjetas de crédito como parte del ataque cibernético.

Esos datos son increíblemente reveladores y posiblemente perjudiciales, particularmente si un hacker busca extorsionar a un cliente de Adult Friend Finder en línea.

Por ejemplo, Robb informó que una persona cuya información fue comprometida en el ataque era un hispano de 62 años de edad, de Nueva Jersey, quien trabajaba en publicidad y tiene una preferencia por el foro "subporno". Eso, combinado con su nombre de usuario y otros detalles de la cuenta, le dio a Robb suficiente información como para buscarlo en Google, descubrir su nombre real, y encontrar sus páginas de redes sociales.

La información expuesta puede ser particularmente devastadora para las personas que viven en pueblos pequeños, donde es más fácil identificarlos. Por ejemplo, una persona que quedó expuesta en el ataque es un soldador de 40 años de un pueblo pequeño de Illinois de unos pocos miles de habitantes.

Él dijo que "se convertiría en el esclavo de cualquier persona" y mintió sobre su edad en el sitio, al afirmar tener 29 años.

El ataque fue llevado a cabo por un hacker que se conoce por el alias de ROR[RG].

En un foro en línea de hackers, dijo que chantajeó a Adult FriendFinder, al decirle al sitio que los datos en línea a no ser que la compañía le pagara 100.000 dólares.

En el foro, los hackers inmediatamente elogiaron a ROR[RG], y dijeron que tenían planificado utilizar los datos para atacar a las víctimas.

"Los estoy cargando en el programa de correo ahora / te enviaré alguna pasta de la que haga / ¡gracias!", escribió un hacker cuyo alias es "MAPS".

FriendFinder Network Inc., la compañía matriz de Adult FriendFinder y otros sitios y publicaciones para adultos de los que también es parte Penthouse, dijo en un comunicado que acababa de enterarse del ataque, y estaba trabajando en estrecha colaboración con la policía y con la empresa de informática forense Mandiant, una filial de FireEye.

La compañía dijo que aún no tiene conocimiento de todo el alcance del ataque, pero prometió "trabajar vigilantemente", y señaló que FriendFinder Networks "aprecia plenamente la seriedad del asunto".

"No podemos especular más allá sobre este asunto, pero pueden estar seguros de que nos comprometemos a tomar las medidas adecuadas y necesarias para proteger a nuestros clientes si se ven afectados", dijo la compañía.