FriendFinder Networks : un piratage dépouille 412 millions de comptes

C'est le plus gros hack de l'année pour LeakedSource : plus de 400 millions de comptes rattachés à des sites du réseau FriendFinder Networks ont été piratés. Un piratage qui chamboule le classement des « plus gros hacks de l'année 2016 » tenu par LeakedSource.

Le moteur spécialisé dans l'indexation des jeux de données piratés a donc réactualisé son classement, en tête duquel ne figure plus MySpace. Le réseau social dominait le palmarès depuis le mois de mai et les révélations sur cette attaque informatique qui avait entraîné la fuite de données associées à 360 millions de comptes.

Il semble que le réseau **FriendFinder Networks** a fait mieux : plus de 412 millions de comptes, dont environ 339 millions rattachés au site de rencontres « hot » AdultFriendFinder, 62 millions à Cams.com, 7 millions à Penthouse.com, ainsi qu'un peu plus d'un million respectivement liés à Stripshow.com et iCams.com.

Un récidiviste

Ce n'est pas la première alerte sur AdultFriendFinder, déjà victime, l'année passée, d'assaillants qui auraient mis la main sur les données de 64 millions de membres, exposant entre autres leur orientation sexuelle et leurs centres d'intérêt parfois très intimes.

Bis repetita ? Pas tout à fait. Concernant les informations exfiltrées, on en reste cette fois-ci à des noms d'utilisateurs, des adresses IP, des logs de connexion et quelques éléments complémentaires qui concernent tout particulièrement l'éventuelle détention du statut VIP…

… Mais il ne faut pas oublier les mots de passe, dont la protection n'a pas été assurée, selon LeakedSource.

Près d'un tiers d'entre eux étaient tout simplement stockés en clair. Les autres ont été protégés avec un algorithme cryptographique obsolète (SHA1) et systématiquement passés en bas de casse avant chiffrement.

Bilan : sur les 339 millions de mots de passe associés à AdultFriendFinder, LeakedSource en a découvert 99,3 %. Les taux sont similaires pour Cams.com (96,8 %) et Penthouse (99,9 %).

Un site vulnérable

L'attaque se serait déroulée au mois d'octobre, dans la foulée des révélations d'un chercheur en sécurité connu sous le pseudo Revolver (1×0123 sur Twitter ; son compte a été suspendu).

Ce dernier avait repéré, sur AdultFriendFinder, une vulnérabilité de type LFI (inclusion de fichier local) potentiellement exploitable pour injecter et exécuter du code à distance. Sa découverte a vraisemblablement été mise à profit dans ce sens.

Du côté de FriendFinder Networks, qui dispose de liens avec 49 000 sites apparentés et plus de 300 000 affiliés pour une base revendiquée de « plus de 700 millions de membres » à travers des déclinaisons comme AsiaFriendFinder et FrenchFriender.com, on ne confirme pas les faits.

On reconnaît toutefois avoir reçu des alertes sur de « possibles failles de sécurité », dont certaines émanant de sources légitimes… et avoir pris des mesures en conséquence, en sollicitant l'assistance des « partenaires adéquats ».

Entre les différents sites du réseau, la communication n'est pas uniforme. Ainsi Penthouse explique-t-il à *ZDNet.com* être « au courant d'un hack » et attendre le compte rendu détaillé de la maison mère.

On notera que sur les 412 millions de comptes prétendument touchés, plus de 15 millions étaient censés avoir été supprimés, précise *ITespresso*.

A lire aussi :

Piratage de Yahoo : des employés savaient dès 2014
Spécial Halloween : la liste des adresses IP utilisées par la NSA pour ses piratages