Nouveau vol de données : Home Depot victime d'une cyberattaque et d'un vol massif de données ?

Nouveau vol de données : Home Depot victime d'une cyberattaque et d'un vol massif de données ?

Après Target, auprès de qui des pirates avaient dérobé des millions de données bancaires de clients, Home Depot pourrait bien être le dernier sur la liste. Les informations des clients de ses 2200 magasins aux US auraient été exposées pendant plusieurs mois.

Home Depot pourrait bien être la dernière enseigne américaine de la distribution à avoir fait l'objet d'une attaque informatique de grande envergure avec pour conséquence le vol de données bancaires de ses clients.
Toutefois, pour l'heure, l'entreprise ne confirme pas une telle menace. Le commerçant se borne pour le moment à faire savoir qu'il a identifié une « activité inhabituelle » en lien avec ses données de clientèle.
Néanmoins, plusieurs éléments semblent attester d'une fuite de données sensibles, dont l'ampleur reste à évaluer. D'après Brian Krebs, un spécialiste de la sécurité, Home Depot collabore avec les forces de police et « plusieurs banques » soupçonnent l'enseigne d'être la source de l'utilisation illicite de données bancaires vendues au marché noir.

Dernier naufrage d'une enseigne de distribution ?
« Protéger les données de nos clients est pour nous un sujet de très grande importante et nous faisons actuellement tout notre possible pour réunir des faits tout en nous efforçant de protéger les clients » commente auprès de la presse une porte-parole de Home Depot, qui admet la possibilité d'une faille.
« Si nous confirmons qu'une fuite s'est produite, nous nous assurerons que nos clients sont prévenus immédiatement » précise-t-elle ainsi. Et pour Brian Krebs, il y a bien eu fuite. Celle-ci aurait débuté en avril dernier et concernerait les 2.200 magasins de Home Depot aux US.
La faille pourrait ainsi s'avérer de plus grande ampleur que celle qui a touché Target en 2013, et pourtant déjà affecté plus de **110 millions de données clients (numéros de cartes, codes PIN et informations personnelles)**.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

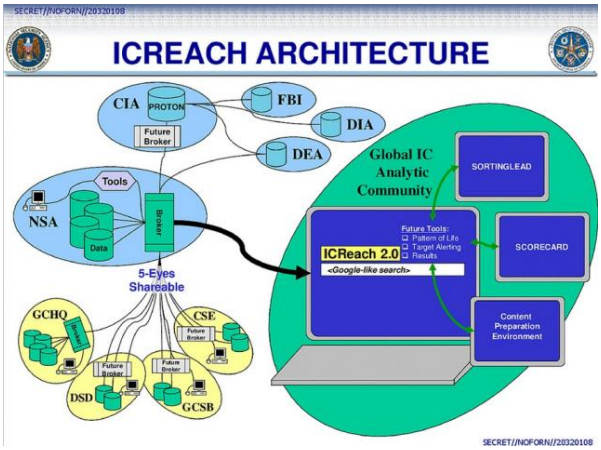
Source :
http://www.zdnet.fr/actualites/home-depot-victime-d-une-cyberattaque-et-d-un-vol-massif-de-donnees-39805665.htm

ICReach, le moteur de recherche secret «à la Google» de la NSA

ICReach, le moteur de recherche secret «à la Google» de la NSA

Certes, la NSA est une agence secrète, mais entre bons amis, elle concède volontiers de partager des informations. Et même beaucoup d'informations, comme le prouve l'existence d'ICReach.

Révélé par The Intercept, sur la base de documents d'Edward Snowden, ce programme de surveillance compile plus de 850 milliards de métadonnées récoltées dans le monde entier et les rend accessibles au travers d'un moteur de recherche « à la Google » auprès d'une vingtaine d'agences gouvernementales américaines. Comme par exemple la CIA (service secret), le FBI (police fédérale) ou le DEA (agence de lutte anti-drogue).



Plus d'un millier d'agents gouvernementaux américains ont ainsi accès à une véritable mine d'or informationnelle. En effet, ICReach compile non seulement des métadonnées téléphoniques, mais aussi des métadonnées relatives aux communications emails et aux messageries instantanées. Au total, ce moteur de recherche référence plus d'une trentaine de champs : temps et durée d'appel, numéros d'appel, protocole, IMEI (identifiant unique du smartphone), identifiant de la cellule mobile de réception, adresse email, identifiant chat, etc. Les données proviennent d'une multitude de bases de données gérées par la NSA, mais aussi par les partenaires du club « Five Eyes » (Royaume-Uni, Australie, Nouvelle-Zélande, Canada).

Les métadonnées surveillées par ICReach.
Ainsi, l'enquêteur pourra savoir qui communique avec qui et depuis quel endroit. Mais ce n'est qu'un début. En croisant toutes ces données, l'objectif est de pouvoir extraire les habitudes de vie quotidienne d'une cible : quels endroits elle fréquente, avec qui et à quel moment, etc. La NSA appelle cela « pattern of life analysis » (« analyse du mode de vie »).
Il est difficile de savoir combien de personnes peuvent être potentiellement surveillées par cet outil. Il concerne principalement des non-Américains, dans la perspective d'un « renseignement extérieur » (« foreign intelligence »). Ce qui est assez vague et peut aller de la guerre anti-terroriste à l'espionnage économique, en passant par la lutte contre la criminalité organisée.
Comme bon nombre de programmes de surveillance de la NSA, ICReach trouve son origine dans les attentats du 11 septembre, qui avaient révélé un manque de communication entre les différentes agences gouvernementales américaines. Un problème qui, visiblement, a été résolu. Attention, ICReach n'est pas à confondre avec XKeyscore, un autre moteur de recherche célèbre de la NSA. Mais celui-ci est davantage restreint au monde de l'espionnage. Par ailleurs, il ne cible que les données du web.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Sources :
http://www.01net.com/editorial/625470/icreach-le-moteur-de-recherche-secret-a-la-google-de-la-nsa/#?xtor=EPR-1-NL-01net-Actus-20140826
https://firstlook.org/theintercept/article/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/