

Ce que les espions de l'Amérique savent de nous...

Les dernières informations publiées par le Washington Post, à l'origine de la révélation du scandale PRISM, viennent confirmer la participation active de certaines grandes entreprises du web à la collecte d'informations par la NSA et le FBI, aussi appelée cyber-espionnage.

Les collaborateurs

Elles sont 9 entreprises du web à figurer nommément dans le document, qui par ailleurs indique depuis combien de temps elles collaborent : Microsoft (depuis le 11/09/2007), Yahoo (12/03/2008), Google (14/01/2009), Facebook (03/06/2009), PalTalk (07/12/2009), YouTube (24/09/2010), Skype (06/02/2011), AOL (31/03/2011) et Apple (10/2012).

Les sources

Le document, classé « TOP SECRET », révèle également les sources dont ces sociétés peuvent dévoiler le contenu aux espions de la NSA : emails, chats, vidéos, photos, données stockées, VoIP, transferts de fichiers, conférences vidéo, notifications de cibles (login, etc.), et les détails publiés sur les réseaux sociaux. Le document précise même que les services américains peuvent les interpellier pour des « *special requests* », des demandes spécifiques.

Les selectors

Dans leurs requêtes, les 'enquêteurs' doivent spécifier les « *selectors* » sur lesquels portent les recherches, une expression qui renvoie vers les types de fichiers, chacun étant identifié par une lettre : A pour Stored Comms (recherches sur les moteurs) ; B pour les messageries instantanées (chat) ; C pour RTN-EDC (la notification d'un e-mail en temps réel) ; D pour RTN-IM (la notification d'un chat en temps réel) ; E pour E-Mail ; F pour VoIP ; G pour Full (forums web) ; H pour les messages OSN Messaging (photos, activité, etc.) ; I pour OSN Basic Subscriber Info ; J pour les vidéos ; et le 'dot' « . » pour un choix multiple.

Qu'avez-vous publié ?

Alors, qu'est-ce que la NSA et le FBI peuvent bien savoir de nous ? La réponse est très simple : rappelez-vous les informations qui figurent sur les documents, messages, mails, etc., que vous avez expédiés ou reçus ; également les informations que vous avez introduites sur les réseaux sociaux ; les informations qui accompagnent les images, les vidéos que vous avez publiées, ou que d'autres ont publiées mais sur lesquelles vous figurez.

Ces informations vont du générique identitaire, nom, prénom, localisation, téléphone, etc., à des choses beaucoup plus personnelles, voire intimes, que vous seul et vos correspondants

connaissent.

1 trillion

Vous pensez peut-être encore que vous pouvez échapper aux opérations menées à l'aide de PRISM ? Selon le Secret Source Operations (SSO), qui au sein de la NSA est en charge des process appliqués sur les métadonnées collectées par la NSA, 75 % du trafic Internet passerait par filtres de PRISM. Soit une collection de 1 trillion de métadonnées !

Vous avez du mal à mesurer le trillion ? Il représente 10 puissance 18, ou 1 000 000 000 000 000 000, ou encore un milliard de milliards, ou enfin un million de millions de millions... Et la NSA dispose d'un accès privilégié aux données qui transitent via les services de Microsoft, Yahoo, Google, Facebook, YouTube, Skype, AOL et Apple. Il est peu probable que vous ne soyez en relation avec aucun d'entre eux.

La NSA en embuscade

Le Washington Post indique que la NSA peut recevoir des notifications en direct dès qu'une cible identifiée se connecte sur l'un des services qui sont surveillés, ou lorsqu'elle expédie un e-mail, un SMS ou encore un message vocal.

La NSA dispose-t-elle d'un accès direct aux serveurs de ces grands acteurs du web ? Ces derniers affirment que non, mais l'on peut légitimement s'interroger. Le seul fait de recevoir des notifications en direct révèle l'existence de liens entre eux et la NSA et/ou le FBI. Le doute subsiste.

Les cibles

Toujours selon ce document, au 5 avril dernier, le terme 'cible' qualifierait 117 675 cibles (!) activement surveillées, sans indiquer s'il s'agit d'individus ou d'organisations. Ni s'il s'agit de cibles qui peuvent potentiellement menacer les intérêts américains, et surtout si ces cibles peuvent potentiellement être innocentes !

A venir...

Le Washington Post et le Guardian sont certainement encore loin de nous avoir tout révélé de cette affaire. Edward Snowden, à l'origine des fuites, aurait remis une collection de documents sur PRISM dont les deux journaux n'ont révélé qu'une partie. La suite pourrait bien se révéler croustillante !

Voir aussi

[Silicon.fr étend son site dédié à l'emploi IT](#)

[Silicon.fr en direct sur les smartphones et tablettes](#)