Vol de données Twitter, LinkedIn… qui est à l’origine ?

	Vol de données Twitter, LinkedIn… qui est à l’origine ?

Les annonces fracassantes de vols de mots de passe se sont multipliées ces derniers temps. Attribuées dans un premier temps à un cybercriminel connu sous le nom de Peace of Mind, un second cybercriminel connu sous le nom de tessa88 clame aujourd'hui être la source originale des bases de données.

Les fuites de mot de passe se sont multipliées ces dernières semaines : Tumblr, LinkedIn, Myspace ou encore le réseau social russe Vkontakte, autant de services web qui ont vu les identifiants de leurs utilisateurs vendus à bas prix sur le web. Ces différentes fuites de données présentaient néanmoins plusieurs points communs : les données vendues étaient toutes plus ou moins datées, les entreprises concernaient ne confirmaient pas systématiquement avoir détecté un piratage de leur côté et les données étaient vendues sur une place de marché noir par un internaute répondant au pseudo Peace of Mind.
Naturellement, ce rôle de revendeur a rapidement fait peser les soupçons sur Peace Of Mind, celui-ci ne précisant pas la provenance exacte des identifiants volés qu'il proposait à la vente.

Selon Motherboard et ZDNet.com néanmoins, l'affaire est un peu plus complexe que cela et Peace Of Mind ne pourrait être qu'un vulgaire revendeur. C'est tout du moins ce que clame l'internaute dissimulé derrière le pseudo Tessa88. Ce dernier, contacté par nos confrères, clame être à l'origine des piratages massifs d'identifiants ayant surgi ces dernières semaines. Peu de détails sont connus sur la personne qui se cache derrière ce pseudonyme, mais on sait que celui-ci est apparu sur des forums russophones spécialisés dans la cybercriminalité aux alentours du mois d'avril 2016. À cette époque, elle propose à la vente des bases de données contenant des identifiants VKontakte ou Myspace parmi d'autres services.

Recel et rivalités

Pour Motherboard, plusieurs personnes pourraient se cacher derrière le pseudonyme Tessa88. Si l'internaute utilise un prénom féminin pour parler de lui sur différents forums dédiés à la cybercriminalité, le site américain soupçonne que ce pseudonyme pourrait être un avatar manipulé par un groupe de cybercriminels. Le pseudonyme avait déjà été mentionné par le site LeakedSource, qui avait fait partie des premiers sites à confirmer l'authenticité des informations contenues dans les bases de données volées mises en vente. Ceux-ci expliquaient avoir obtenu les échantillons des bases de données grâce à l'entremise de Tessa88.
Peu de temps après, Peace Of Mind propose lui aussi des bases de données similaires sur le marché noir The Real Deal : on retrouve les mêmes sites et des bases de données de tailles comparables. Mais Tessa88 n'est pas tendre avec Peace Of Mind : celle-ci clame en effet être l'auteur des piratages ayant permis de récupérer les identifiants et dénonce le fait que Peace of mind n'est qu'un revendeur, pour qui Tessa88 ne semble pas avoir beaucoup d'estime.
Peace Of Mind n'est pourtant pas un total inconnu : c'était déjà ce pseudonyme qui revendiquait la cyberattaque ayant visé le site de la distribution Linux Mint en début d'année 2016. Peace Of Mind n'a fait aucun commentaire sur les déclarations de Tessa88 et se contente de laisser entendre que la vente d'identifiants va continuer. Tessa88 laisse également entendre qu'elle n'a pas écoulé entièrement son stock et que de nouvelles ventes sont à prévoir. Tous deux clament ainsi être en possession de bases de données contenant des identifiants de connexions Instagram, là aussi dans des volumes particulièrement importants.
De nombreuses zones d'ombres persistent malgré les déclarations concurrentes des deux cybercriminels. Ainsi, ceux-ci restent muets sur l'origine exacte des données : certaines entreprises touchées n'ont reconnu aucun piratage au sein de leurs systèmes.
Impossible de savoir également pourquoi exactement ces données ressortent aujourd'hui : Tessa88 explique à Motherboard avoir exploité ces identifiants pour ses activités pendant plusieurs années, mais avoir aujourd'hui choisi de les vendre afin de faire face à des soucis de santé. La seule chose sur laquelle les deux cybercriminels s'accordent, c'est sur le fait qu'ils entendent bien continuer à revendre ces identifiants.
Article original de Louis Adam

Réagissez à cet article

Original de l’article mis en page : Twitter, LinkedIn… qui est à l’origine des vols de données ?