1,2 milliard d’identifiants volés par des pirates russes – Vol d’identifiants au dessus d’un nid de coucou

1,2 milliard d’identifiants volés par des pirates russes – Vol d’identifiants au dessus d’un nid de coucou

Le vol d'identifiants est passé à l'échelle supérieure avec la découverte que des cybercriminels russes avaient détourné 1,2 milliard de noms et mots de passe. A ce niveau, cela touche tout le monde, estime la firme de sécurité Hold Security qui a découvert ce groupe de pirates qu'il désigne sous le nom de CyberVor.
En Russie, des criminels ont constitué une énorme base constituée de 1,2 milliard de noms d'utilisateurs et de mots de passe volés, auxquels s'ajoutent 500 millions d'adresses e-mail, selon Hold Security, une société américaine spécialisée sur la sécurité Internet. Il s'agit probablement de la plus grosse base d'identifiants dérobés, récupérés d'attaques conduites dans tous les coins du web et qui ont touché environ 420 000 sites. « Jusqu'à présent, nous étions stupéfaits lorsque 10 000 mots de passe avaient été compromis, maintenant nous en sommes au stade du vol massif », a confié Alex Holden, fondateur de Hold Security, à nos confrères d'IDG News Service. Sa société n'a pas communiqué le nom des sites qui avaient été attaqués, invoquant des accords de confidentialité avec ses clients, mais elle a indiqué que cela incluait des familles et de petits sites web.

Le New York Times, qui fut le premier à rapporter ce vol, s'est adressé à un expert en sécurité indépendant pour vérifier que les données volées étaient authentiques. L'ampleur de la base constituée semble éclipser les précédentes découvertes de données compromises. Par comparaison, le vol subi par Target (révélé en janvier dernier) a affecté 40 millions de cartes de débit et 70 millions d'informations personnelles. C'est, en matière de détournement d'identifiants, l'un des faits de cybercriminalité les plus importants constatés jusqu'à présent et qui porte ce type de délit à un niveau supérieur. « Ces gens n'ont rien fait de nouveau ni d'innovant », constate Alex Holden. « Ils l'ont juste fait mieux et à un niveau de masse ce qui touche absolument tout le monde ».

Le gang CyberVor est constitué d'une douzaine de jeunes gens
Le groupe derrière l'attaque semble être basé dans le centre-sud de la Russie, a indiqué Alex Holden au New York Times. Selon les informations qu'il a communiquées au quotidien américain, il s'agit d'une douzaine de personnes d'une vingtaine d'années qui ne semblent pas avoir de liens avec le gouvernement. Avec des serveurs basés en Russie, le groupe a étendu ses activités cette année, probablement après avoir été en contact avec une organisation plus importante. Hold Security a dénommé le gang CyberVor d'après le mot russe « vor » (voleur). La société a indiqué qu'elle fournirait un service pour permettre aux utilisateurs de vérifier si leurs identifiants figurent parmi ceux qui ont été volés. L'information sera disponible dans deux mois environ. Le pré-enregistrement pour y accéder est possible dès maintenant.
Ce détournement massif de noms d'utilisateurs et de mots de passe met une fois de plus en lumière le peu de sécurité apportée par ces méthodes d'authentification, en particulier si les personnes se servent des mêmes noms et passwords pour plusieurs sites. Le recours à une méthode d'authentification à deux niveaux (avec envoi d'un code par SMS) renforce la sécurité mais ne constitue pas une garantie comme un utilisateur de PayPal vient tout juste de le démontrer. Après avoir, sans succès, alerté PayPal sur cette faille, il a expliqué comment cette fonction pouvait, en l'occurrence, être détournée via une connexion eBay.
Article de Martyn Williams / IDG News Service (adapté par Maryse Gros)

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

Références :
http://www.lemondeinformatique.fr/actualites/lire-des-pirates-russes-ont-amasse-1-2-milliard-d-identifiants-58272.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter