Des hackers iraniens derrière de faux profils LinkedIn

Des chercheurs en cybersécurité de **Dell SecureWorks** déclarent avoir mis au jour un réseau de faux profils sur **LinkedIn**. Ces faux profils seraient utilisés par des hackers présumés iraniens dans le but d'entrer en contact avec des cibles potentielles dans le monde, les manipuler et leur extirper de l'information sensible (ingénierie sociale), selon l'analyse de la firme de sécurité.

25 faux profils sont décrits. Des comptes de consultants en recrutement ont été créés en détournant le nom de grands groupes (Airbus Group, Northrop Grumman, Teledyne Technologies, etc.).

Des espions grimés en recruteurs

Les pirates se seraient ainsi connectés à plus de 200 profils LinkedIn *« légitimes ».* Ces derniers appartiendraient, dans leur majorité, à des individus basés au Moyen-Orient et travaillant dans **les télécoms et la défense**. Leurs informations et celles des entreprises qui les emploient, seraient la cible du groupe de hackers iraniens nommé « TG-2889 » par les chercheurs. Or, ce même groupe de hackers serait à l'origine d'une vaste campagne d'espionnage sur 16 pays, dont la France. Il s'agit de l'opération « Cleaver », décrite par la firme de sécurité Cylance en décembre 2014…

Concernant l'affaire du moment, LinkedIn a indiqué au *Wall Street Journal* avoir retiré les faux profils incriminés. Le réseau social professionnel américain a rappelé, par ailleurs, qu'une équipe se consacre à la protection de ses membres contre ces risques… Et la prudence s'impose. Selon les services de sécurité de Dell, il est probable que de faux profils maintenus par le groupe de hackers TG-2889 n'ont pas encore été identifiés et que d'autres organisations utilisent ce même subterfuge.

Lire aussi :

Opération Cleaver : la riposte des Iraniens à Stuxnet ?
Un outil pour débusquer les espions sur Linkedin