Monster ciblé par les pirates, admet perdre des données

Monster.com, un des sites les plus importants en matière de recrutement en ligne connaît un **épisode douloureux**. Dans un communiqué, la société éditrice de **Monster.com** et de **USAjobs.com** explique que certaines informations de sa base de données ont été dérobées.

Les dirigeants témoignent : « *Monster est la **cible de tentatives illégales d'accès et d'extraction des données de notre base.** Nous avons récemment appris que **certaines informations de contact et de compte ont été prises**, notamment des identifiants utilisateur et des mots de passe, des adresses **e-mails**, des **noms**, **numéros de téléphone** et certaines données démographiques basiques*** **« .**

Le site explique alors qu' « *il est important de savoir que nous surveillons continuellement tout usage illicite des informations de notre base de données, et jusqu'ici, nous n'avons **détecté aucune mauvaise utilisation de ces informations*** **«** . Pour autant, le risque de voir cette faille être utilisée n'est pas à omettre.

Des attaques par ***phishing*** pourraient alors être mises en oeuvre par les détenteurs des informations. De même, du **spam ciblé** concernant la recherche d'emplois serait une hypothèse tout à fait probable.

De son côté, le site a prévenu que par mesure de sécurité, les utilisateurs pourraient être amenés à **changer de mot de passe** lors d'une prochaine connexion. Dans ce cas, Patrick Manzo, le vice président de Monster rappelle de bon ton que : « *Monster ne vous envoie **jamais d'e-mail non sollicité** vous demandant de confirmer votre nom d'utilisateur ou mot de passe, ni ne vous demande de télécharger aucun logiciel »*.

Le site avait déjà été victime d'une telle attaque en **août 2007**. Le p-dg de Monster Sal Iannuzzi avait alors dû **formuler des excuses.** Les pirates étaient parvenus à disposer des informations qui permettent aux entreprises de se connecter au site. C'est un malware de type **cheval de Troie** qui avait transmis ces informations ainsi dérobées vers un serveur.

Des attaques qui indiquent combien ce type d'informations intéresse au plus haut point les *hackers*. D'un autre côté, elles mettent le doigt sur un manque de sécurité du site.