# Des pirates se lancent à l'assaut de Monster.com

Des milliers de données sur les usagers du site se retrouvent dans la nature alors que selon Cyber-Ark le pire aurait dû être évité…

La faute a un maudit 'trojan', ou cheval de Troie, a déclaré l'éditeur Symantec. Ce 'malware' a permis à des cybercriminels de s'introduire discrètement dans les serveurs Web du site américain.

Et d'y dérober des informations bancaires, des comptes de cartes de crédit, des identifiants et mots de passe, des courriels, etc. La plupart des victimes ont été infectées en visitant le site.

Selon Zataz.com, ces données ont ensuite été acheminées sur 20 serveurs répartis dans différents pays du globe, et un seul de ces serveurs rassemblait ces données personnelles. Le gang de pirates à l'origine de ces vols de données sensibles serait baptisé « Car groupe ».

Bien entendu, ces données peuvent parfaitement être réutilisées pour alimenter du 'spam' ou du 'phishing' (hameçonnage), histoire pour les pirates de rentabiliser le temps perdu à créer le 'trojan'.

Pour propager rapidement et auprès d'un maximum de personnes cet intrus, les pirates ont utilisé de façon détournée les bannières publicitaires de Monster.com. Un clic suffisait pour être infecté. Enfin, le code malveillant était mis à jour pratiquement tous les jours, afin de rester dans l'ombre des pare-feu et autres détecteurs de code?

Selon, Cyber-Ark, groupe d'experts en sécurité informatique, *« ce cybercambriolage aurait pu être évité si le site avait mieux sécurisé sa base de données, par exemple en ne stockant que des données cryptées. »*

Pour Calum Macleod, directeur de Cyber-Ark EMEA, *« Monster.com pouvait très simplement empêcher cette attaque qui a utilisé une méthode simpliste. Les méthodes de cryptage et l'application d'une politique de sécurité stricte auraient pu empêcher ce vol de données. Les véritables conséquences de cette attaque risquent d'être dramatiques. »*