

# Piraté, Baidu porte plainte contre Register.com

Voilà une semaine, le moteur de recherche chinois Baidu (plus de [55 % du marché](#) chinois) subissait une [attaque informatique](#). En **ciblant son DNS**, l'attaque a permis le défacement pendant plusieurs heures de sa page d'accueil.

Baidu cherche des réponses. L'attaque orchestrée contre ses services n'avait été revendiquée seulement par l'obscur «**cyberarmée iranienne**». Une organisation inconnue si tant est qu'elle existe mais qui est parvenue à rendre indisponible Baidu pendant plusieurs heures. Aucune information ne circule encore sur l'identité de cette faction. Pour autant, une semaine auparavant, **le site [Twitter](#) avait connu les mêmes affres.**

Là aussi le *modus operandi* s'avérait être une [modification de DNS de Twitter](#) même si, à la loupe, l'attaque permettait que le nom de domaine Twitter.com **n'arrive plus sur l'adresse IP du serveur du site**, mais sur une autre adresse IP, celui contenant les images affichées.

Toujours est-il que Baidu pointe du doigt une manipulation de son DNS administré aux Etats-Unis et a donc déposé plainte devant un tribunal de New York à l'encontre du gestionnaire de nom de domaine **Register.com**.

Plus précisément, Baidu accuse le registrar de négligence sur son territoire puisque la **version [chinoise \(.cn\)](#) du moteur n'aurait pas été touchée par l'attaque.**

Cette panne de son service contraint donc Baidu à déposer une plainte aux Etats-Unis et cherche à obtenir des **dommages-intérêts**. Nul doute que cette action comporte une connotation politique puisque, comme nous l'indiquions précédemment, le mode d'attaque ne s'est concentré que sur une partie du Web, américain en l'occurrence.

Michel Lanaspèze, directeur marketing de Sophos commentait ainsi : « *Quelqu'un a pu **modifier le système de consultation**, ce qui signifie qu'à chaque fois que les utilisateurs tapaient baidu.com dans leur navigateur, ils étaient redirigés vers un autre site, hors du contrôle du moteur de recherche. Si ce site extérieur avait contenu du **code malveillant, des millions d'ordinateurs auraient pu être infectés** ».* Ce qui n'a apparemment pas été le cas. Un piratage *a minima* mais une action en justice qui risque de faire des remous.