L'Iranian Cyber Army pirate le site du géant chinois de la recherche en ligne

Déjà auteurs d'une attaque sur Twitter, les pirates ont détourné Baidu.com, le plus grand site web chinois.

Paris, le 12 janvier 2010 – Sophos, un des leaders mondiaux de la sécurisation et de la protection des données, rappelle à tous les opérateurs de sites Web la nécessité de protéger efficacement leurs systèmes, comme le montre l'attaque menée la nuit dernière contre Baidu.com, le plus important site chinois. Les pirates sont en effet parvenus à afficher un message de la « Iranian Cyber Army » sur la page d'accueil du principal moteur de recherche de Chine.

Les visiteurs de baidu.com ont été accueillis avec le message en anglais « This site has been hacked by Iranian Cyber Army », surmontant une image du drapeau national iranien. Cette attaque semble avoir été conduite par le même groupe qui avait posté en décembre des messages similaires sur le site de Twitter, perturbant des millions d'utilisateurs du service de micro-blogging.

« En Chine, Baidu dépasse Google comme moteur de recherche de référence, avec des millions de visites par jour. Cela en fait une cible extrêmement attractive pour les cybercriminels, qui ont l'assurance d'obtenir un impact maximal s'ils parviennent à trouver une brèche dans sa sécurité », commente Michel Lanaspèze, Directeur Marketing et Communication de Sophos Europe du Sud. *« Les internautes chinois doivent être grandement soulagés que les pirates n'en aient pas profité pour infecter les ordinateurs, se contentant de ce qui apparaît comme un 'graffiti politique'. Des questions se posent cependant sur la manière dont un tel piratage a été possible. »*

Le soupçon grandit en effet que ce ne sont pas les serveurs Web de Baidu eux-mêmes qui ont été piratés, mais plutôt que les enregistrements DNS du site ont été compromis. C'est ainsi que Twitter avait été touché le mois dernier par l'Iranian Cyber Army.

« Les enregistrements DNS fonctionnent comme un annuaire téléphonique, en convertissant les noms de sites tels que baidu.com en séquences de chiffres utilisables par internet », explique Michel Lanaspèze. *« 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. De telles attaques rappellent à chacun qu'il est indispensable de disposer d'un système de sécurité capable de vérifier chaque page Web visitée, même s'il s'agit d'un site légitime et bien identifié. »*

Des informations complémentaires, ainsi qu'une image du site piraté, sont disponibles sur le blog de Graham Cluley, à l'adresse : http://www.sophos.com/blogs/ gc/g/2010/01/12/baidu.

A propos de Sophos.

Plus de 100 millions d'utilisateurs dans 150 pays ont retenu Sophos comme la meilleure défense du marché contre les menaces complexes et les risques de pertes de données. Ses solutions intégrées de sécurisation et de protection des informations sont simples à déployer, à administrer et à utiliser, et offrent le coût global de possession le plus avantageux du marché. Elles permettent le chiffrement des données, la protection des systèmes d'extrémité, la sécurisation du Web et de la messagerie et le contrôle d'accès réseau avec le support permanent desSophosLabs, le réseau mondial de centres d'analyse des menaces de Sophos. Avec plus de deux décennies d'expérience, Sophos est reconnu comme un leader de la

sécurisation et de la protection des données par les principaux analystes du marché, et ses produits ont reçu de nombreuses récompenses.
http://www.sophos.fr