Faille DNS : 30% du parc de serveurs DNS en France seraient toujours vulnérables

- Informatique - Sécurité Informatique -

Date de mise en ligne : mercredi 10 septembre 2008

Spyworld Actu

C'est la "statistique choc" d'une société de conseil en sécurité informatique en France, qui propose un test gratuit en ligne.

Alors que l'on pensait la faille béante portant sur les serveurs DNS était corrigée ou presque depuis fin juillet, des experts en sécurité issus de NBS System viennent de lancer une alerte à destination des responsables de la sécurité des systèmes d'information (RSSI) sur les risques qu'ils encourent s'ils ne mettent pas à jour rapidement leur service DNS.

En effet, selon ce cabinet français de conseils en sécurité informatique, 30% du parc de serveurs DNS français seraient toujours vulnérables face à "l'exploit" remis au goût du jour par Dan Kaminsky en juillet dernier.

"Suite à la conférence Black Hat où nos experts ont assisté à la présentation de Dan Kaminsky à ce sujet, NBS System, en accord avec M. Kaminsky, a décidé de proposer un test gratuit en ligne afin de savoir où en était l'avancement des correctifs sur le territoire français", a indiqué la société de sécurité IT dans un communiqué.

Ce test gratuit est disponible sur le site Internet de NBS. Il est anonyme et seul le pourcentage d'avancement des correctifs est envoyé à l'auteur de cette faille afin qu'il puisse établir des comparatifs.

Entre service rendu et marketing

D'après les premiers résultats, il resterait donc en France de nombreux serveurs pouvant être attaqués. La mise en place des patches n'a jamais été aussi importante.

On notera que si l'idée première est sans doute de rendre service, l'approche marketing basée sur la peur et la paranoïa pour vendre un produit ou service, est toujours aussi efficace dans le petit monde de la sécurité..

Dans une interview à Vnunet.fr, Christophe Perrin, responsable du marché de la sécurité chez Cisco France, avait déclaré à l'époque que "cette attaque peut être utilisée à des fins de phishing, la vulnérabilité est donc importante".

Depuis, la concertation organisée par Kaminsky avec les géants du secteur IT (Microsoft, Cisco...) a permis de régler le problème en grande partie. S'il est touché, l'internaute n'a aucun moyen de détecter qu'il a été redirigé ou qu'il est écouté. La meilleure solution restent une véritable protection du service DNS.

Post-scriptum :

http://www.vnunet.fr/news/faille_dn...