Faille DNS: D. Kaminsky dévoile le fin mot, au Black Hat

L'intervention de Dan Kaminsky, chercheur vedette en matière de sécurité informatique, était attendue, même si beaucoup de détails de cette affaire touchant à une faille DNS étaient déjà connus.

Rappel pour ceux qui sont partis en vacances (plusieurs mois..., loin de toute connexion Internet...), ce spécialiste en sécurité d'IO Active a découvert, il y a plus de six mois un défaut de taille dans la cuirasse du DNS, le système central qui met en relation les adresses des sites et les pages stockées sur des serveurs. Par cette découverte, **tout le réseau mondial d'Internet a pris conscience du risque de voir des pirates s'emparer de l'ensemble du trafic.**

La riposte est alors arrivée par des patchs proposés par Microsoft et les éditeurs de sécurité puisque la vulnérabilité du protocole DNS affectait aussi bien les serveurs de cache déployés par les fournisseurs d'accès à Internet que les postes clients utilisés par les internautes. Par la technique dite du *cache poisoning*, il devenait alors possible de rediriger les requêtes d'un internaute vers le site Web de son choix.

Kaminsky a donc révélé lors du Black Hat que 70% des entreprises présentes au classement *Fortune 500* auraient aujourd'hui procédé aux corrections nécessaires à la résolution de cette faille. 15% d'entre elles auraient essayé, mais auraient été confrontées à des problèmes de translations d'adresses IP. Enfin, les **15% restants n'auraient appliqué aucun correctif à l'heure actuelle.**

Le chercheur s'est encore refusé à rendre publique les modalités d'exploitation de la faille (d'autres s'en sont chargés à sa place). Il a néanmoins mis en ligne quelques précisions sur son site web doxpara.com, et a terminé sa présentation en estimant que « *chaque réseau possède un risque. Nombreux sont les chemins qui mènent à la désolation...*«