http://www.techno-science.net/?onglet=news&news=5588
Posté par Adrien le Samedi 12 Juillet 2008

Faille DNS mondiale: lorsque l'Internet a failli s'écrouler

Faille DNS mondiale: lorsque l'Internet a failli s'écrouler Une faille de sécurité touchant la plupart des serveurs DNS au monde a été révélée il y a quelques jours. Découverte en début d'année, cette faille est restée secrète le temps que les principaux acteurs de l'Internet aient le temps de la corriger. Elle aurait pu remettre en question toute la confiance du monde de l'Internet, et écrouler l'économie associée.

Dan Kaminsky, expert en sécurité au sein de la société IOActive, a découvert début 2008 une faille dans la gestion des caches des serveurs DNS. Rappelons que le serveur DNS est la clé permettant de passer du langage humain au langage informatique au niveau des adresses internet, comme celles des urls visibles sur votre navigateur. Par exemple, l'adresse google.fr (langage humain) correspond à une adresse ip (langage informatique) telle que 216.239.59.104.

Ce problème de sécurité, vieux comme l'Internet mais seulement découvert il y a quelques mois, pourrait permettre à des pirates de modifier la correspondance "adresse standard" <-> "adresse ip" de n'importe quel enregistrement sur le serveur DNS. Cas concret: si le serveur DNS de votre fournisseur d'accès est piraté, par exemple google.fr se réfère maintenant à une autre adresse ip, alors sur votre navigateur en entrant google.fr vous vous retrouverez diriger vers l'ordinateur du pirate. Et si celui-ci vous présente une page web clonée de celle de google.fr, vous ne verrez pas la différence. Mais maintenant, si il ne s'agit pas de google.fr mais d'un site d'e-commerce ou celui de votre banque, ce sont des informations extrêmement sensibles que vous pourrez livrer au pirate sans vous en rendre compte. Le risque de phishing (tromper un internaute en lui faisant croire qu'il est sur un autre site que sur celui qu'il croit être) est donc extrêmement élevé.

On le voit, cette faille aurait pu provoquer une situation de crise dans le monde de l'Internet. C'est pourquoi qu'une fois découverte, elle est restée dans le plus grand secret, le temps pour les acteurs concernés de fournir des correctifs de sécurité. Il était important que les serveurs DNS soient corrigés avant qu'un quelconque pirate n'ait connaissance de cette faille. Parmi les acteurs concernés, notons Microsoft, IBM, Cisco Systems, Sun Microsystems, Akamai, Alcatel, Siemens ou encore Apple. Des correctifs ont été mis "discrètement" à dispositions cers dernières semaines pour les différents équipements, et bien qu'il ne pourra jamais être certain que la faille soit partout colmatée, les serveurs DNS les plus sensibles comme ceux des fournisseurs d'accès à internet se doivent de l'être.

Saluons donc la gestion de cette crise qui fut extrêmement professionnelle. Des acteurs pourtant concurrents ont su travailler de concert et effectuer des échanges technologiques, et ceci en respectant le plus grand secret, afin de résoudre au mieux cette situation.