Faille DNS : êtes-vous vulnérable ?

Découverte début juillet par Dan Kaminsky, la faille qui touche les serveurs de résolution de noms de domaine (DNS pour *Domain Name System*) n'en finit pas de faire parler d'elle. Les serveurs qui n'implémentent pas un correctif sont effectivement vulnérables aux attaques du type ***« man in the middle »***, les requêtes pouvant être interceptées assez facilement.

Selon NBS System, société spécialisée dans la sécurité informatique, **près de 33% des DNS français sont encore sensibles à cette faille**. La société précise que *« le correctif n'élimine pas le risque à 100%, mais vise plutôt à rendre l'attaque beaucoup plus difficilement réalisable »*. NBS System propose (sur cette même page web) de tester vos DNS.

Le fournisseur d'accès à Internet Celeste va plus loin, en vous offrant de **tester tout DNS accessible depuis Internet**. L'outil est d'une utilisation très simple. Confronté à plusieurs serveurs DNS publics populaires, il s'avère que ceux de Cisco (San Jose), Verizon (Reston) et OpenDNS (San Fransisco) sont très bien sécurisés.

Pour Level 3 Communications (Broomfield) le résultat est tout juste correct, alors que **les données sont très inquiétantes pour One Connect IP** (Albuquerque), pourtant très présent dans le monde professionnel (en particulier dans les hôtels américains). Attention lorsque vous partirez en voyage.

Notez que la plupart des DNS des fournisseurs d'accès à Internet français ne sont pas publics. Ceci limite les effets de cette vulnérabilité. En tout état de cause, à notre connaissance, tous sont aujourd'hui *patchés* contre cette faille.