AFNIC : « Les attaques visent de plus en plus souvent le DNS »

Déjà recommandé par le chercheur en sécurité Dan Kaminsky, expert au sein de l'équipe d'IO Active, l' AFNIC (Association française pour le nommage Internet en coopération) conseille aux professionnels de la sécurité de prendre des mesures en faveur d'une prise en compte générale de la sécurité des réseaux.

En cause, la technologie de défense **DNSSEC**. Ce protocole qui permet de protéger certains réseaux devrait, selon les spécialistes, être généralisé de manière permanente car il offre **une meilleure méthode d'authentification et de protection des données** contre les attaques d'empoisonnement du cache (**cache poisonning**) encore appelées pollution de cache.

Voilà presque une année, Dan Kaminsky commentait la situation ainsi : « *La technologie DNSSEC peut apparaître terrifiante lorsque l'on doit l'implémenter.**Il y a tellement d'administrateurs qui sont censés le faire mais peu ont encore essayé***« . Une position proche de celle de l'Afnic.

Si le **DNS** (Domain Name System) fonctionne comme une **base distribuée sur des milliards de machines**, il repose sur les interactions entre elles. Mathieu Weill, directeur général de l'Afnic commente ainsi : « *Les attaques visent de plus en plus souvent le DNS.**Le DNSSEC a pour objet d'ajouter des clés afin d'authentifier les échanges.** Le problème demeure qu'avec des clés, il est facile de se retrouver coincé devant la porte. Il faut pour cela que tous les acteurs déploient cette solution et sachent l'interpréter. Le gros du chantier à venir va donc être de **favoriser la prise en main des procédures de déploiement de la technologie**. Dans 3 ou 4 ans, cela devrait être fait***« .

Les vulnérabilités du DNS sont encore une fois mises en lumière. L'Afnic rappelle néanmoins que, concernant les noms de domaines, nombre d'attaques figurent encore au sommaire des pirates. Loïc Damilaville, responsable marketing et communication de l'Afnic fait un résumé des attaques courantes : « *Chacun doit bien prendre en compte que les attaques classique de type **injections SQL** qui visent à récupérer des données clients sensibles sont encore importantes, sans parler des **attaques de type DoS (deny of service), le phishing ou encore le typo-squatting***« . Traduire, le squattage de noms de domaines (Gooogle, tvvitter, silikon.fr…). Ce dernier point, pose toujours des interrogations en matière de légalité et de juridictions compétentes…

L'Afnic milite donc en faveur d'un **rapprochement des vues en matière de déploiement de solutions de sécurité**. Un peu à l'image du déploiement contre la faille DNS, l'association espère voir se diffuser globalement des méthodes de protection telles que le DNSSEC. Un vœu pieux ?