La faille DNS qui fait trembler le monde de la sécurité

Sun, Microsoft ou encore Cisco ont semble t'il saisi l'ampleur de la menace qui pèse sur le Web. Le Département de la Défense Nationale américaine est également sur le coup, averti depuis plusieurs mois de la vulnérabilité et travaille main dans la main avec les grands acteurs du secteur. Dans la plus grande discrétion. Explications de cette union sacrée.

Le spécialiste en sécurité Dan Kaminsky, d'IO Active, a découvert , parfaitement par hasard (!) il y a 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, c'est **tout le réseau mondial qui est concerné** par le risque de voir des pirates s'emparer de l'ensemble du trafic.

Cette faille aurait pu permettre à des pirates de rediriger n'importe quelle adresse Internet vers d'autres sites de leur choix ou leurs propres systèmes. Les spécialistes évoquent alors un risque accru de « *phishing*« , déjà très en vogue dans les milieux pirates.

Evidemment, personne ne désire en dire plus sur les détails techniques de cette faille afin d'éviter toute exploitation indirecte. Ce n'est pas la première fois qu'une faille DNS est mise à jour, mais combinée aux potentiels du phishing, la vulnérabilité découverte démultiplie les dégâts potentiels.

Une majorité des éditeurs impliqués a déjà lancé une série de correctifs automatiques pour un nombre important de systèmes d'exploitation et de logiciels. Le but étant de minimiser les risques de retour de flamme après la publication des mises à jour. Le patch day de Microsoft de ce jour comporte d'ailleurs un correctif pour le DNS Windows. Idem pour Cisco qui a mis à jour IOS, Network Registrar, Application and Content Networking System, et Global Site Selector à travers un massif bulletin de sécurité.

Un patch géant est donc actuellement diffusé pour éviter toute propagation. Néanmoins, Dan Kaminsky tient à rassurer tous les internautes : « *Les gens peuvent être inquiets mais ne doivent pas paniquer, car nous avons gagné autant de temps que nous pouvions, afin de tester et de mettre en application le patch*« . Par ailleurs, selon les experts, ces vulnérabilités n'ont pas été exploitées notamment grâce à la discrétion des acteurs qui ont développé ces correctifs.

D'ordinaire, les experts en sécurité vendent aux entreprises les détails sur les failles qu'ils découvrent. **Signe de l'importance de l'enjeu, entreprises et professionnels ont décidé d'agir de concert.** Une première historique ! On assiste donc à une convergence significative de vues sur des questions de sécurité critiques. De là à imaginer une réelle gouvernance internationale…

A noter : un **site Internet** a été mis en place pour permettre aux internautes de tester leur vulnérabilité à cette faille.

A lire : une interview de Mauro Israël, expert en sécurité : 'On a frôlé le Big One'

A lire également : un entretien avec Christophe Perrin, responsable développement marché Sécurité pour Cisco France