Faille DNS : les pirates diffusent un logiciel d'exploitation

La faille DNS découverte par Dan Kaminsky s'annonce comme le feuilleton de l'été. Début juillet, le spécialiste en sécurité informatique révèle avoir mis à jour un défaut qualifié de très sérieux dans le protocole DNS (Domain Name System).

Dès lors, on découvre rapidement que **les entreprises ont eu connaissance de la faille depuis plusieurs mois** et qu'elles ont, semble- t-il, réussi à corriger les problèmes. Sun, Microsoft , Cisco ou encore le Département de la Défense Nationale américaine sont alors sur le coup. Dans la plus grande discrétion, les patchs massifs sont élaborés puis diffusés quelques temps après la « révélation ».

Ensuite tout va très vite. La discrétion apparente saute rapidement lorsque les patchs commencent à se diffuser. Deux semaines plus tard, les détails de la faille sont diffusés par la société Matasano, officiellement par erreur…

La stratégie de rester discret sur les éventuelles exploitations de la faille vole alors en éclats. En effet, **tous les acteurs en présence se sont bien gardés de donner des détails sur cette vulnérabilité** sinon qu'elle est dérivée de la technique de cache poisonning et combine des vulnérabilités connues du protocole DNS et du *phishing*.

Très vite, Matasano Security, retire l'information de son blog. ..Trop tard. Dès ce jeudi, des hackers diffusent déjà des codes d'attaque clé en main pour exploiter la faille informatique. Selon ses auteurs, de fausses données DNS peuvent alors être insérées dans la cache d'un name-server. Un attaquant peut alors afficher une mauvaise réponse pour n'importe quelle requête.

A ce stade, on se rend compte que si des rustines existent, grâce notamment aux mises à jours et autres patchs, le danger peut subsister. Du côté de Sophos, on tient néanmoins à rester pragmatique. Selon Michel Lanaspèze, directeur marketing de l'éditeur de sécurité, **l'important est de savoir si les patchs ont été correctement installés au niveau des entreprises :** « *il n'y a, à mon sens, pas de doute sur les mesures prises par les FAI ou les grandes entreprises. Restent vulnérables ceux qui n'ont pas pris les mesures nécessaires. C'est aux sociétés d'identifier le personnel qui n'aurait pas patché*« . La balle est dans le camp des administrateurs réseaux qui doivent vérifier au plus vite que les patchs ont été bien installés.

Le risque est donc toujours bel et bien présent et fait encore parler de lui. Au moins jusqu'au 6 août prochain, date à laquelle Dan Kaminsky rendra public les détails de la vulnérabilité, pendant le Black Hat. Un secret déjà bien éventé.