Internet : un énorme danger qui ne repose sur aucune faille

- Informatique - Internet -

Date de mise en ligne : jeudi 28 août 2008

Spyworld Actu

Depuis des années, de nombreuses sociétés commercialisent des solutions de sécurité pour compenser les dangers inhérents à l'utilisation d'Internet aujourd'hui. Antivirus certes, mais également pare-feu, anti-spyware, filtre contre les spams. Des protections qui sont le plus souvent très efficaces, mais également en bout de chaine. Le véritable problème se trouve entre les extrémités, et l'exemple du spam est révélateur : si vous ne recevez pas de spam grâce à votre filtre, cela ne signifie pas pour autant qu'Internet en est débarrassé. Bien au contraire.

Il n'y a rien à corriger

Et c'est l'essence même de cette histoire de sécurité : on peut investir des centaines d'euros dans des solutions performantes de sécurité, mais si l'un des principaux protocoles utilisés pour l'acheminement des données sur Internet permet de dévier un flux d'informations, tous vos outils ne vous serviront à rien. Et c'est bien ce que permettrait le BGP (Border Gateway Protocol), selon deux hommes qui en ont fait la démonstration récemment.

« Il ne s'agit pas d'une faille ou de la défaille d'un logiciel », prévient Anton Kapela, directeur réseau et centre de données chez 5Nines Data. Avec Alex Pilosov, PDG de Pilosoft, ils ont démontré lors de la dernière DefCon que le BGP pouvait être utilisé pour détourner le trafic de sa destination vers une nouvelle choisie arbitrairement. La démonstration a été réalisée en direct, en détournant le trafic de la conférence pour le renvoyer vers une machine installée à New York, avant de le faire revenir à Las Vegas.

Un changement dans les fondations à prévoir ?

Le BGP est en fait utilisé pour déterminer le meilleur chemin pour aller d'un point à un autre à travers les routeurs des fournisseurs d'accès principalement. Le problème avec ce protocole c'est qu'une fois le chemin trouvé, les routeurs font intrinsèquement confiance à ce qu'indique le protocole. Or, c'est justement cette confiance qui est la faille, sans en être une réellement.

À chaque fois qu'un utilisateur a besoin de quelque chose, comme la consultation d'un site web, le serveur DNS traduit l'adresse de ce site en une adresse IP. Chez le fournisseur d'accès de l'utilisateur, un routeur consulte une table BGP pour déterminer quel est le plus court chemin jusqu'à la destination. Les tables sont constituées à partir de déclarations d'autres fournisseurs d'accès qui indiquent les plages d'adresses IP vers lesquelles ils pourront envoyer des données.

Les deux attaquants ont publié une plage d'adresses IP considérées comme « plus proches » par les routeurs. La publication de ces données est très rapide et n'a besoin que de quelques minutes pour faire le tour de la planète. De fait, toutes les demandes adressées à ces adresses ont été réorientées vers une nouvelle cible. Ensuite, le flux peut être renvoyé vers sa destination initiale.

En silence messieurs

La technique est parfaitement silencieuse, contrairement à toutes les redirections d'adresses IP qui avaient été utilisées jusqu'à présent. Car c'est justement parce que les précédentes techniques faisaient du « bruit » qu'elles ont été détectées, car elles devaient systématiquement « casser » quelque chose à un moment donné : « Si rien n'est cassé, qui le remarquera ? », s'interroge Anton Kapella.

Les deux hommes ont expliqué que les fournisseurs d'accès peuvent en théorie arriver à différencier un trafic normal d'un dévié. Le plus gros souci sera que le travail demandé sera énorme et donc très coûteux. Une autre solution

serait de se tourner vers le SBGP pour Secure BGP, qui demande alors aux routeurs concernés de signer par une clé numérique toutes les publications d'adresses IP qu'ils propagent. Une solution idéale, certes, mais qui demande que les routeurs disposent d'une mémoire et d'une puissance supérieures à ce que possèdent nombre d'entre eux.

Le Conseil National de Sécurité américain ainsi que des instances officielles telles que la NSA (National Security Agency) ont été informés de la situation dans ses moindres détails. En attendant, il va falloir patienter, et les deux hommes espèrent simplement que pour l'instant personne ne trouvera la technique. Un voeu pieux ?

Post-scriptum :

http://www.pcinpact.com/actu/news/4...