Quelqu'un se prépare à détruire Internet

15.09.2016
5 min

Le spécialiste de la cybersécurité Bruce Schneier a posté un article alarmiste sur son blog, des menaces pèseraient sur les structures de l'internet.

Illustration d'une explosion• *Crédits : Mopic / AWO / Science Photo Library - AFP*

C’est très sérieux. C’est LE grand expert de la cybersécurité Bruce Schneier qui l’a écrit sur son blog hier “quelqu’un est en train d’apprendre à détruire Internet” ce sont ses mots. Quand Bruce Schneier dit quelque chose comme ça, il faut mieux y prêter attention….

Schneier explique que depuis un ou deux ans, les entreprises critiques de l’internet, subissent des attaques précises, calibrées, dont le but semble être de tester leurs défenses, et d’évaluer les moyens nécessaires pour les mettre à bas. C’est le cas par exemple de Verisign, dont lerapport trimestriel de ce type d’attaques. Verisgn, c’est l’entreprise américaine qui gère notamment les noms de domaine en .com et .net si Verisign tombe, c’est tout un pan de l’Internet mondial qui disparaît.

Qu’est-ce que ces attaques ont de particulier ? Schnieier l’explique très bien.

Les attaques les plus courantes sur Internet, sont ce qu’on appelle les attaques en déni de service (en Ddos). En gros, il s’agit d’empêcher les usagers de se rendre sur le site visé. Pour ça, même s’il y a des subtilités, le moyen est toujours le même : adresser au site tellement de requêtes qu’il sature et devient inaccessible, c’est ensevelir le site sous les données. Les attaques en déni de service sont vieilles

comme Internet, les hackers y recourent pour faire tomber les sites qu'ils n'aiment pas, les cybercriminels pour obtenir des rançons (car on peut prendre un site en otage). Il y a toute une industrie de la défense contre les attaques en déni de service, mais, à la base, ça revient toujours à une question de bande passante (c'est-à-dire de débit, pour faire une analogie avec la plomberie). Si l'attaquant en a plus que le défenseur, il gagne.

Depuis quelques mois donc, les entreprises critiques de l'internet subissent ce genre d'attaques en déni de service, mais elles ont un profil particulier. Elles portent sur un spectre plus large que d'habitude, et elles durent plus longtemps. Elles sont plus sophistiquées aussi. Mais surtout, elles donnent l'impression de tester des choses. Par exemple, une semaine, une attaque va commencer à un certain niveau, monter en grade, puis s'arrêter. La semaine suivante, elle va reprendre à ce niveau, puis monter encore. Comme si elle cherchait l'exact point de rupture. Et puis ces attaques semblent configurées pour voir les contours des défenses. A chaque fois, elles utilisent différents points d'entrée en même temps, ce qui est rare, obligeant les entreprises à mobiliser l'ensemble de leurs capacités de défense; à montrer tout ce qu'elles ont à disposition, ce qui n'est jamais bon.

Tout converge donc vers le constat que quelqu'un est bien en train de tester les défenses des entreprises les plus critiques de l'Internet mondial. Mais qui ? Schneier ne croit pas à un criminel, un activiste ou chercheur. Ce genre de méthode passant par le test des infrastructures centrales, ça ressemble beaucoup plus selon lui à un acte d'espionnage ou de renseignement. Et puis la puissance et l'échelle de temps sur laquelle s'étendent ces attaques désignent un Etat. Comme si le cybercommandement d'une armée était en train de calibrer ses armes en cas de cyberguerre. Ca rappelle à Schneier quand, pendant la guerre froide, les Américains envoyaient dans le ciel soviétique des avions de très haute altitude pour que la défense anti-aérienne soviétique se mette en alarme, et pouvoir donc la cartographier.

Que faire ? Rien, dit Schneier. On ne sait pas d'où ça vient. Les données qu'il a en sa possession le ferait pencher pour la Chine, et il n'est pas le seul à le penser. Mais ce type d'attaque permet de masquer le pays d'origine. La NSA, explique-t-il, qui exerce sur la colonne vertébrale de l'Internet (pour traduire "backbone") la surveillance la plus approfondie, doit avoir une idée plus précise, mais à moins que les Etats-Unis ne veuillent déclencher une crise diplomatique, nous n'en saurons rien.

Ainsi commence ce John Le Carré au pays des gigabits.