Bruce Schneier est un expert en sécurité informatique. Il est reconnu depuis de nombreuses années principalement pour son livre mythique « Applied Cryptography » qui fête cette année son vingtième anniversaire. Il tient également depuis 2004 un blog assez fréquenté où il y dispense ses idées et ses vues sur le monde. Ce mardi 13 septembre, il y annonce que depuis une ou deux années, quelqu'un testerait des attaques de type déni de service distribué (distributed denial of servie ou DDoS) auprès d'acteurs majeurs d'Internet. Ces attaques, bien qu'elles n'aient rien de nouveau en soi, seraient ici plus sophistiquées et plus intenses qu'à l'accoutumée. D'après lui, elles pourraient s'apparenter à des tests de calibrage en vue d'une attaque de plus grande ampleur.

Le principe de déni de service est assez simple à comprendre, il s'agit tout simplement de rendre indisponible un service pour empêcher à ses utilisateurs légitimes d'y accéder. Peu importe d'ailleurs par quel moyen.

Mettons par exemple que vous n'êtes pas très sympa (je suis sûr que ce n'est pas vrai) et que vous vouliez pourrir une connaissance. Vous pourriez par exemple passer votre temps à l'appeler sur son téléphone. Pendant ce temps, personne d'autre ne peut la joindre. Vous commettez alors un déni de service. Mission accomplie. Cependant, votre innocente victime n'est pas si bête et va très rapidement mettre en place des mesures de protection, comme bloquer votre numéro. Mais malheureusement pour elle, votre génie maléfique ne s'arrête pas là. Vous appelez tous les restaurants du coin si bien qu'un florilège de livreurs se tient maintenant devant sa porte. Elle est bloquée. Il s'agit ici de nouveau d'un déni de service mais cette fois-ci utilisant une technique différente. Et pour finir votre sinistre affaire, comme vous êtes populaire, vous demandez à tous vos amis de faire de même. Il s'agit maintenant d'un déni de service distribué, c'est à dire à plusieurs : un DDoS.

En informatique, c'est exactement la même chose. Il existe de très nombreuses techniques de déni de service. Et comme nous l'avons vu précédemment avec notre pauvre victime, en en fonction des cibles certaines techniques marchent mieux que d'autres. C'est pour cela qu'un assaillant aura tout intérêt à tester son arsenal pour mieux l'affiner. Et d'après Bruce, c'est exactement ce qui est en train de se passer depuis un ou deux ans.

Bien qu'Internet soit un système de communication décentralisé, il n'est pas impossible de perturber très sérieusement la machine au point de la rendre inutilisable. Il existe ce que l'on appelle des dorsales Internet (Internet backbones). Ce sont des sortes d'autoroutes reliant des réseaux longues distances. Il est possible de faire une analogie avec le réseau routier, lui aussi décentralisé. Si les principaux axes de circulation rapide sont coupés, les usagers seront forcés de se rabattre sur des voix plus petites comme les nationales et départementales, créant ainsi des embouteillages monstres et amenant potentiellement au

blocage d'un pays. D'ailleurs en 2011, une grand-mère de 75 ans en tentant de voler des câbles de cuivres, a coupé d'Internet une bonne partie de la Géorgie et de l'Arménie en sectionnant le câble optique d'une dorsale Internet qui n'en avait pas d'autres de secours.

Du point de vue défensif, il est très difficile voire impossible de se protéger à 100% de ce type d'attaque. Nous l'avons vu, il existe des très nombreuses techniques de DDoS différentes. Et on ne peut tout simplement pas « débrancher le câble » de l'agresseur. Dans le cas d'une attaque distribuée, cela arrive de toutes parts, autant de l'intérieur que de l'extérieur. Si votre ordinateur est vérolé, vous pourriez totalement faire partie des assaillants.

Il existe bien sûr des stratégies de protections et des solutions de redondance. Mais immanquablement celui qui a « la plus grosse connexion » gagnera toujours. À cela s'ajoute le fait qu'il est aussi très difficile de tester les infrastructures en place. Si vous voulez reproduire l'attaque « livraison de pizza », vous allez non seulement impacter la victime, mais également tous les restaurants de la région, qui ne seront probablement pas très coopératifs.

Alors de qui viennent ces attaques ? Pour Bruce probablement d'une puissance étrangère mondiale. Mais il est impossible réellement d'en dire plus sans en connaître les détails techniques. Dans un monde où l'informatique a pris une telle ampleur, il n'est guère surprenant que certains états veulent testent leurs armes électroniques dans la nature.

Et alors nous dans tout ça ? De mon point de vue, il n'y a aucune raison s'inquiéter et je ne pense pas qu'un tel scénario soit probable. De toute façon, il n'y a pas grand-chose à faire. Assurez vous que votre ordinateur ne soit pas infecté pour éviter de relayer une attaque. Prévoyez la vie pendant quelques semaines sans Internet ou téléphone, ça veut dire sans Facebook :-), et assurez vous d'avoir à votre disposition des moyens de communications alternatifs: radio FM, talkie-walkie, pigeons baroudeurs. Et bien sûr une bonne autonomie de vie et une bonne résilience.

Article rédigé par **Shankara**