Quand la Toile se déchire…

Vous prendrez bien un peu une petite DDoSe de paranoïa ce matin ? Blague à part, j'avais choisi de ne pas vous proposer la traduction de cet article de Bruce Schneier, lorsqu'il est paru au mois de septembre, en pensant qu'il allait un peu loin dans l'énoncé de la menace : en route vers la cyberguerre, pas moins.

L'épisode récent qui a vu hier « tomber » des sites populaires comme Twitter ou eBay et bien d'autres m'incite à y revenir.

Attention toutefois : cette récente attaque n'a probablement rien à voir avec ce que décrit Schneier (voyez par exemple cet article sur la récente « panne »), et par ailleurs les intuitions ou soupçons de ce spécialiste de la cybersécurité ne sont nullement des preuves : il serait trop « facile » d'accuser des puissances présumées hostiles quand de « simples » négligences, des erreurs humaines ou la zombification d'objets connectés sans sécurité peuvent s'avérer responsables.

L'intérêt de cet article est plutôt de montrer la toile de fond de la Toile, sa fragilité surtout dont nous ne prenons véritablement conscience que lorsqu'elle se déchire brutalement, révélant un bric-à-brac high-tech dont on se demande par quel miracle il ne tombe pas en panne de lui-même plus souvent.

Pas grand-chose à faire, conclut de façon pessimiste Bruce Schneier.

Re-décentraliser Internet, peut-être ?

Quelqu'un est en train d'apprendre à faire tomber Internet

par Bruce Schneier

article original sur son blog : *Someone Is Learning How to Take Down the Internet*

Depuis un ou deux ans, quelqu'un a sondé les défenses des entreprises qui font tourner des composantes critiques d'Internet. Ces sondes prennent la forme d'attaques précisément calibrées destinées à déterminer exactement comment ces entreprises peuvent se défendre, et ce qui serait nécessaire pour les faire tomber. Nous ne savons pas qui fait cela, mais ça ressemble à un grand État-nation. La Chine ou la Russie seraient mes premières suppositions.

Tout d'abord, voyons la toile de fond. Si vous voulez vous emparer d'un réseau sur Internet, la meilleure façon de le faire est avec une attaque (DDoS) distribuée par déni de service. Comme son nom l'indique, il s'agit d'une attaque destinée à empêcher les utilisateurs légitimes d'accéder au site désiré. Ça peut être plus subtil, mais, fondamentalement, cela signifie saturer le site cible de tellement de données qu'il est débordé. Ces attaques ne sont pas nouvelles : les pirates l'utilisent contre des sites qu'ils n'aiment pas, et les criminels l'utilisent comme une méthode d'extorsion. Il y a toute une industrie, avec un arsenal de technologies, consacrée à la défense DDoS. Mais surtout, il est une question de bande passante. Si l'attaquant a un plus gros pipeline pour déverser ses données que le défenseur, c'est l'attaquant qui gagne.

Récemment, quelques-unes des grandes entreprises qui fournissent l'infrastructure de base qui fait fonctionner Internet ont vu une augmentation des attaques DDoS contre elles. De plus, elles ont repéré un certain type d'attaques. Ces attaques sont nettement plus importantes que ce qu'elles sont habituées à voir. Elles durent plus longtemps. Elles sont plus sophistiquées. Et elles ressemblent à des coups de sonde. Une semaine, l'attaque commencera à un niveau particulier d'attaque et progressera lentement avant de cesser. La semaine suivante elle commencera à ce point élevé et continuera. Et ainsi de suite, selon ce même processus, comme si l'attaquant était à la recherche du point exact de fragilité fatale

Les attaques sont également configurées de manière à voir la totalité des défenses de l'entreprise ciblée. Il existe de nombreuses façons de lancer une attaque DDoS. Plus vous utilisez de vecteurs d'attaque simultanément, plus le défenseur doit multiplier ses diverses défenses pour les contrer. Ces entreprises

voient davantage d'attaques qui utilisent trois ou quatre vecteurs différents. Cela signifie que les entreprises doivent utiliser tout ce qu'elles ont pour se défendre. Elles ne peuvent pas garder de munitions. Elles sont obligées de démontrer leurs capacités de défense face à l'attaquant.

Il m'est impossible de donner des détails, parce que ces entreprises m'ont parlé sous couvert d'anonymat. Mais tout cela est conforme à ce que Verisign rapporte. Verisign est le registraire pour de nombreux domaines Internet parmi les plus populaires, comme.com et.net. Si Verisign tombe, on assiste à une panne mondiale de tous les sites et adresses électroniques des domaines les plus courants. Chaque trimestre, Verisign publie un rapport sur les tendances DDoS. Bien que sa publication n'ait pas le niveau de détail des propos que m'ont confié des entreprises, les tendances sont les mêmes : « au 2e trimestre 2016, les attaques n'ont cessé de devenir plus fréquentes, persistantes et complexes »

Il y a plus. Une entreprise m'a parlé d'une variété d'attaques par sondage associées aux attaques DDoS : elles consistent à tester la capacité de manipuler des adresses et des itinéraires Internet, voir combien de temps il faut à la défense pour répondre, et ainsi de suite. Quelqu'un est en train de tester en profondeur les capacités défensives de base des sociétés qui fournissent des services Internet critiques.

Qui pourrait faire cela ? Ça ne ressemble pas à ce que ferait un activiste, un criminel ou un chercheur. Le profilage de l'infrastructure de base est une pratique courante dans l'espionnage et la collecte de renseignements. Ce n'est pas ce que font normalement les entreprises. En outre, la taille et l'échelle de ces sondes – et surtout leur persistance – pointe vers les acteurs étatiques. Tout se passe comme si l'armée électronique d'une nation essayait de calibrer ses armes dans l'éventualité d'une cyberguerre. Cela me rappelle le programme de la guerre froide des États-Unis qui consistait à envoyer des avions à haute altitude au-dessus de l'Union soviétique pour forcer son système de défense aérienne à s'activer, et ainsi cartographier ses capacités.

Pouvons-nous y faire quelque chose ? Pas vraiment. Nous ne savons pas d'où viennent les attaques. Les données que je vois suggèrent la Chine, une évaluation partagée par les gens auxquels j'en ai parlé. Mais d'autre part, il est possible de dissimuler le pays d'origine de ces sortes d'attaques. La NSA, qui exerce plus de surveillance sur la colonne vertébrale d'Internet que tout le reste du monde

combiné, a probablement une meilleure idée, mais à moins que les États-Unis ne décident d'en faire un incident diplomatique international, on ne nous dira pas à qui l'attribuer.

Mais c'est ce qui se passe. Et ce que les gens devraient savoir.

- Pour aller plus loin, un article en anglais qui reprend et discute des arguments de Bruce Schneier, sans le contredire toutefois.

Photo de Bruce Schneier par Terry Robinson CC BY-SA 2.0

Attaque sournoise