28 octobre 2016
THE DAILY BEAST

Méga panne mondiale d'Internet : pourquoi la cyberattaque actuelle n'est qu'un début

Grâce à de puissants et nouveaux "botnets" (contraction de "robot" et "réseau"), les hackers ont désormais la possibilité de faire tomber des entreprises de premier plan, et même des pays entiers.

Avec Kevin Beaumont

Kevin Beaumont. *The Daily Beast.*

En septembre dernier, Bruce Schneier, un spécialiste de la sécurité informatique de renommée mondiale, avaitécrit sur des hackers qui sondaient les points faibles de l'internet en vue d'une tentative de mettre le réseau entier hors ligne. Beaucoup de personnes ont considéré que l'article était exagéré et irréaliste. C'était avant les attaques de vendredi qui ont momentanément mis hors service certains des plus grands noms de l'internet.

D'autres ont essayé de faire cela auparavant, en attaquant les serveurs Dns (*Domain Name System*) à la source, les pages jaunes de l'internet en quelque sorte, mais sans y parvenir. Dns répertorie toute notre navigation sur internet. C'est le lien qui nous donne la direction vers chacun de nos sites internet favoris. Ce qui se passe aujourd'hui, c'est que des hackers ciblent délibérément une entreprise appelée Dyn, en utilisant la technique du 'déni de service'.

Cette technique consiste à envoyer une très large quantité de données corrompues pour bloquer une entreprise. Dyn est une société de services informatiques virtuels dans le Cloud, qui fournit ce qu'on appelle des "services Dns" à ses clients. Si le Dns est un peu comme les pages jaunes, où vous tapez www.twitter.com et êtes redirigé vers le bon serveur internet, Dyn est la plateforme qui accueille environ un quart de million de ces adresses des pages jaunes. C'est pour cela que des sites importants comme Twitter ou Reddit ont mal fonctionné vendredi.

Ce qui se passe depuis quelques années, c'est que des entreprises externalisent leurs services de gestion de Dns - ironiquement en partie - car elles n'arrivaient pas à gérer les attaques par déni de service toutes seules. Cela a créé des plateformes centralisées, plus faciles à cibler pour les hackers. Et elles sont bel et bien ciblées.

Durant le mois dernier, une attaque distribuée de déni de service a totalisé un trafic de plus de 1 000 gigabits par seconde. C'est un volume de trafic très impressionnant, bien plus important que ce qui avait été vu avant. (En 2015, l'entreprise Arbor Networks avait rapporté que la plus grande Ddos - *Distributed denial of service* - du monde était de l'ordre de 334 gigabits par seconde). Cela va bientôt devenir normal. Il très difficile et très couteux de se défendre contre cela. Seule une poignée d'entreprises est capable de le faire. Ces attaques sont en partie possibles grâce à "l'internet des objets', des objets comme les caméras de surveillance et les magnétoscopes numériques qui sont directement reliés à l'internet, et n'offrent qu'un faible niveau de sécurité.

Les hackers s’attaquent à ces objets, dans des entreprises ou les domiciles, partout dans le monde, afin de créer des "botnets", une meute d’objets infectés à partir desquels ils peuvent lancer une attaque concertée. Des criminels vendent aussi des attaques à partir de ces "botnets" pour pas cher, permettant ainsi à n’importe quel budget de lancer des attaques contre des cibles.

submarinecablemap.com

Il y a beaucoup d’exemples, mais en voici un. Prenons une carte des câbles sous-marins qui connectent à internet plusieurs pays. Sur bien des câbles, souvent posés il y a longtemps (le premier câble sous-marin transmettant des données date de 1850), la bande passante est limitée. Par exemple, le câble Lion – propriété du groupe Orange – qui connecte Madagascar, La Réunion et l’île Maurice, a une capacité maximum de 1 280 gigabits par seconde, et cette bande passante est divisée entre fournisseurs de services de télécommunication et point d’atterrissage. Ces câbles sous-marins sont également très sollicités par le trafic quotidien. Ce qui veut dire que, grâce à ces nouveaux dénis de services XXL, nous avons atteint un point où les attaques peuvent bloquer des pays entiers.

Dans le cas des pannes de vendredi, il semble que des gens utilisent des "botnets" pour attaquer des serveurs Dns qui hébergent un grand nombre de sites internet, via des entreprises privées qui concentrent leurs sites internet chez un petit nombre de fournisseurs de services Dns. Cela s’avère être une façon unique d’attaquer les services de base de l’internet. Un autre problème est la nature même de ceux qui lancent ces attaques. Par exemple, l’attaque de déni de service qui a duré le plus longtemps au monde a été celle lancée contre le site web de Brian Krebs, un journaliste et chercheur reconnu sur les questions de sécurité informatique. Akamai, son fournisseur de solutions anti-déni de service, a choisi de ne plus fournir ce service à cause du coût que cela générait. Son site web est désormais hébergé par Google Project Shield, qui a pour objectif de protéger les journalistes des dénis de service.

Au moment de l’attaque, Brian Krebs enquêtait sur une opération de déni de service, et sur deux adolescents qui tentaient de vendre du déni de service "à la demande" à ceux qui seraient prêts à les payer. Lorsque vous avez des petits groupes de gens assez outillés pour déstabiliser l’internet de façon significative – internet où les économies occidentales sont établies désormais – cela provoque une situation de plus en plus intenable. Les gouvernements et les acteurs du marché doivent prendre une résolution sérieuse. En particulier les fournisseurs d’accès à internet, qui doivent regarder de plus près le type de flux qu’ils laissent passer dans leurs réseaux, et notamment détecter l’usurpation d’adresses IP. Les gouvernements devront probablement légiférer en la matière.

Cet article a été adapté de celui originellement publié sur Medium.