Parole d'expert – Jean-Nicolas Piotrowski – Président fondateur d'ITrust
« La Créature de Frankenstein reprend vie grâce à l'IoT »

Suite à une attaque DDoS (déni de service distribué), menée contre le service informatique DynDNS[1], un grand nombre de sites Internet ont été inaccessibles le 21 octobre dans la zone outre-Atlantique. Les échos se sont ressentis jusqu'en Europe et le knock-out du web qui a fait trembler les Etats Unis n'est en quelque sorte que la partie émergée de l'iceberg.

Rappelons-nous début octobre, il y au le malware Mirai, l'une des plus puissante cyber-menace des objets connectés. Sans trop tarder, les pirates ont encore une fois fait honneur à leur réputation avec une cyber-frappe qui a marqué les esprits à travers le monde entier. L'attaque subi par DynDNS le 21 octobre dernier semble être une version améliorée de l'attaque connue en début de mois, avant que le code source de Mirai soit mis en ligne. Cependant cette fois, le nombre des dispositifs connectés à Internet s'élevait à des centaines de milliers. Des webcams, des routeurs, des interphones de surveillance bébé et plein d'autres objets smart installés à domicile ont contribué à l'effondrement total du web aux Etats Unis.

Comme notre titre le dit si bien, avec le développement continu des applications liées à l'IoT, nous venons de recréer le monstre 3.0 de Frankenstein. Avec des fournisseurs comme XiongMai Technologies, vendent des dispositifs smart présentent des vulnérabilités, nous ne devrions pas nous étonner que le rôle du savant fou nous revient. Le producteur chinois est aujourd'hui soupçonné d'être partialement responsable de lancement de l'attaque DDoS contre le fournisseur de service DNS. Dans le roman de Mary Shelley, Victor Frankenstein avait fui face à l'atrocité de sa création. De la même manière, XiongMai Technologies s'absout de toute culpabilité sur son blog officiel, en affirmant que le véritable problème provient des utilisateurs qui ne changent pas les mots de passe par défaut.

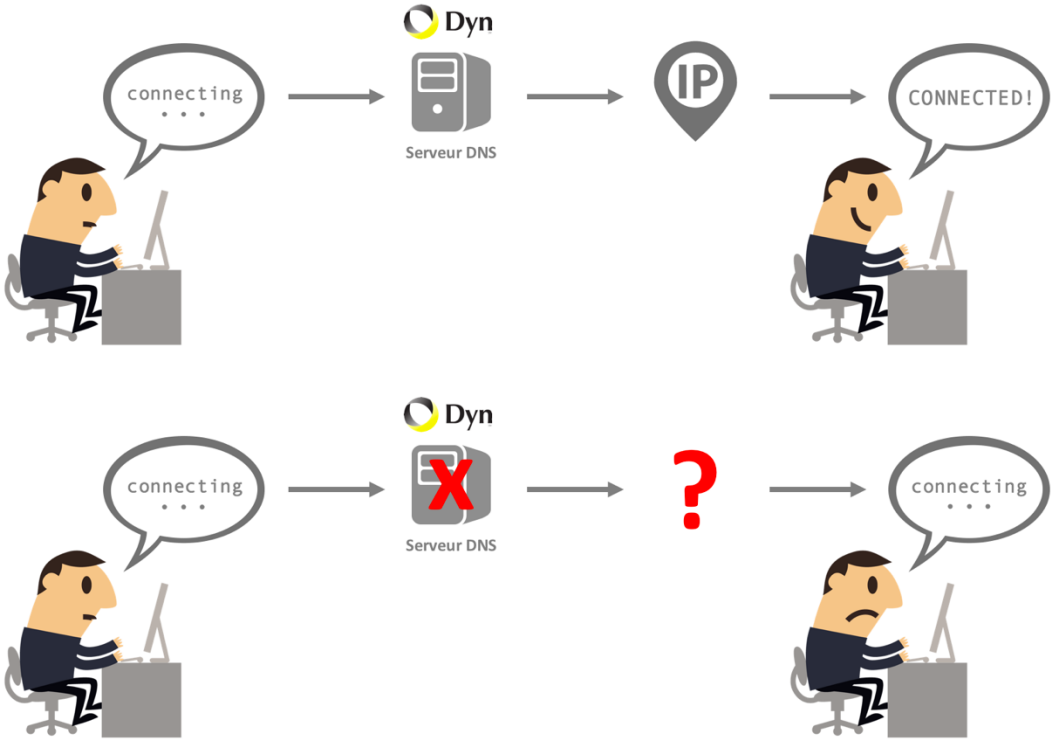
Le gourou de la sécurité informatique, Bruce Schneier, a annoncé le mois dernier que l'avenir des attaques reposera sur les botnets IoT. Et la réalité est loin de changer, tant que nous n'ouvrirons pas les yeux et que nous n'affronterons pas les conséquences de nos actions. Nous avons créé une infrastructure Internet même avant que la cybersécurité ne soit un terme utilisé dans la vraie vie. Nous avons voulu jouer le Prométhée moderne et désormais on récolte ce que l'on a semé.

L'expérimentation DDoS : un succès redouté

Lors de cette cyber-attaque massive, les premiers inconvénients ont parus sur la côte Est, pour se propager dans les heures suivantes vers la côte Ouest. Selon le blog high-tech Gizmodo, presque la « moitie d'Internet » s'est retrouvé dans le noir. Une trentaine de sites importants ont rejoint la chute, dont Twitter, Airbnb, Etsy, GitHub, Paypal, Reddit, eBay et encore Spotify. En France, les sites utilisant le service Dyn ont également enregistré des délais anormaux de connexion (cf. Dynatrace, spécialiste en performance applicative).

Mais pourquoi prendre la peine de s'attaquer à un fournisseur DNS ? La réponse est simple : c'est l'expérimentation parfaite. En touchant à ce dernier, les cybercriminels font couler toutes les sites associés à ce service. Pour faire plus simple, un service DNS permet aux utilisateurs d'accéder un site en utilisant son nom et non pas son adresse IP numérique. Si vous rentrez, par exemple, le nom twitter.com, qui est rattaché à un certain DNS, ce dernier va vous traduire cette demande dans une adresse IP spécifique et envoyer une requête, afin de router le trafic réseau vers la bonne adresse. Cette explication, pour schématique qu'elle soit, a pour but de vous faire mieux comprendre comment une attaque de type DDoS peut impacter une infrastructure managée DNS, que cela appartient au Dyn ou pas.

[1] DynDNS est un service informatique offert par la société américaine Dyn, spécialisée dans la surveillance et le reroutage du trafic Internet. Il permet aux hébergeurs de sites d'associer à un nom de domaine une adresse IP dynamique (c'est à dire, une adresse IP qui change à chaque connexion). Le serveur DNS (Domain Name System) reçoit la nouvelle adresse IP via un logiciel installé sur la machine de l'hébergeur et met à jour le nom de domaine attaché à celle-ci.



Typiquement, au moment où vous allez tenter de vous connecter sur Twitter, l'effet DDoS rend le service DNS inaccessible (voir image) et, par conséquence, ne lui permet plus de « traduire » le nom du site en une adresse IP. Le résultat ? Vous tapez et tapez et tapez... mais ça n'abouti à rien. Dans le cas présent, la récente attaque DDoS contre l'infrastructure managée de DNS a mis le fournisseur Dyn dans l'incapacité de rediriger les connexions pour approximativement 12 heures.

Réécrire une histoire qui peut finir tragiquement

Dans l'œuvre originale de Shelley, Victor Frankenstein et sa créature meurent à la fin. Voulons-nous prendre le risque de subir le même sort tragique ? Bien sûr que non, mais il faut se méfier. Si les pirates sont capables de faire tomber Internet, qui sait de quoi d'autre ils seront capables. Enfin, si ce n'est qu'une seule chose qui est bien dans toute cette histoire c'est le fait que l'attaque du 21 octobre mets en évidence le maillon faible du web : tel un château de cartes, si nous enlevons une, tout s'éclate.

La récente expérimentation DDoS souligne aussi la problématique de la centralisation des applications dans le milieu informatique. Éric Freyssinet, spécialiste dans le fonctionnement des armées zombies, appuie sur la nécessité de ne pas placer toutes ses espoirs sur un seul serveur DNS.

Très intéressant, certes, est le fait que des sites bénéficiant d'une popularité moins exceptionnelle (voir Reddit) étaient mieux préparés pour faire face à ce type de situation. En suivant tout simplement les bonnes pratiques existantes, la communauté de partage avait fait affaire avec plusieurs fournisseurs de DNS, au lieu de compter juste sur Dyn. Encore une leçon en sécurité informatique que certains apprendrons seulement au lendemain de la catastrophe.

Cela veut dire que nous devrons nous contenter de l'étiquette de Frankenstein ? Absolument pas. Avant que le rideau tombe définitivement, il reste encore de temps pour réécrire l'histoire en notre faveur.