Botnets

Serez-vous complice ?

Quelqu'un essaye de casser l'Internet.

Depuis plusieurs mois, les attaques DDOS (déni de service distribué) sont en pleine recrudescence et il est fort probable que quelqu'un (ou peut-être une organisation étatique) soit en train de tester les limites de l'Internet.

Ces attaques utilisent des milliers d'ordinateurs ou d'objets connectés dont l'attaquant a pris le contrôle pour envoyer en même temps des requêtes vers une cible unique. Cette charge exceptionnelle de trafic peut réduire considérablement la disponibilité de la cible en question qui ne parvient plus à répondre correctement aux requêtes légitimes. Dans ce cas de figure, ce sont les clients du service en ligne ou du site visé par l'attaque qui ne parviendront plus à utiliser normalement le service. Dans le pire des cas, les serveurs de la cible sont complètement débordés et ne répondent plus. Le service est alors totalement interrompu.

Parmi les dernières victimes, OVH, l'un des hébergeurs les plus importants en Europe, a subi une attaque par déni de service avec un débit supérieur au térabit par seconde. Selon lui, cette attaque est due à un botnet qui est constitué de 145 607 caméras de surveillances IP, visiblement non protégées, et qui ont été capables de lancer une attaque DDoS de plus de 1,5 térabit par seconde. L'attaque n'a pas réussi à faire plier les serveurs d'OVH mais a tout de même provoqué quelques ralentissements. Si une plus petite structure avait été ciblée, les conséquences auraient sans doute été beaucoup plus graves. Selon le chercheur en sécurité Mustafa Al-Bassam, il s'agissait là de la plus violente attaque DDoS jamais enregistrée dans l'histoire de l'Internet.

Il ne s'agit pas de la première attaque par déni de service qui s'appuie sur des caméras connectées. En juin 2016, la société Sucuri avait détecté un botnet de 25.000 caméras connectées.

Comment se développent les botnets ?

Pour créer un botnet, les hackers ont besoin de nombreux dispositifs dotés d'une connexion Internet. Ces dispositifs peuvent servir 2 « maîtres » en même temps. Pour leurs propriétaires, ils fonctionnent comme d'habitude. Mais sans se faire remarquer, ils se mettent à attaquer d'autres sites web sous les ordres d'un cybercriminel.

Dernièrement, un malware nommé « Mirai » a été diffusé. Il s'agit d'un outil permettant aux hackers de construire leur botnet plus facilement. Mirai analyse les objets connectés à Internet et tente un mot de passe sur tout ce qu'il trouve. En général, les gens ne changent pas les paramètres par défaut de leurs appareils ni les mots de passe, ce qui fait que les dispositifs sont faciles à pirater, c'est de cette façon qu'ils sont enrôlés dans les armées de zombies (les botnets).

Les attaques qui sont survenues ces derniers mois risquent donc de se multiplier à l'avenir, car le nombre d'objets connectés ne cesse d'augmenter, et l'exploitation de leurs vulnérabilités est facilitée par des outils disponibles sur Internet.

Qui est responsable ?

Caméras de surveillance, imprimantes Wi-Fi, montres ou bracelets connectés, télévisions, jouets, consoles de jeu, appareils électroménagers connectés à Internet… La liste ne cesse de s'allonger, avec une constante : ces objets sont pour la plupart connectés en permanence à Internet et leurs vulnérabilités sont multiples.

En voici les principales :

- les systèmes d'exploitations des objets connectés présentent souvent des failles de sécurité ;
- internet est la solution la plus rentable et la plus simple pour l'interconnexion des objets avec leurs « centres de contrôle ». Les moyens d'échanges ne sont pas toujours sécurisés (versions de SSL / TLS pas à jour, donc potentiellement vulnérables);
- les fabricants d'objets connectés veulent réduire au maximum leur temps de développement pour arriver sur le marché avant leurs concurrents. L'accent est mis sur l'ergonomie et le design et la sécurité se retrouve souvent mise sur la touche;
- le mode connecté 24/7 fait qu'il est très compliqué de faire des mises à jour et de corriger les failles.

Pour toutes ces raisons, les objets connectés sont plus faciles à trouver que les équipements installés sur un réseau d'entreprise mieux sécurisé… qui malgré leur niveau de protection nettement plus élevé, ne sont pas à l'abri. La morale de cette histoire est que nous sommes tous concernés, voire potentiellement « complices », à notre insu. L'armée des botnets est déjà composée de millions de petits « soldats » invisibles et prêts à entrer en action. Comment faire pour ne pas en créer de nouveaux ?

Que peut-on faire?

Une seule personne ne peut pas empêcher des botnets de faire planter Internet, mais si chacun prend conscience du problème et essaye de prendre des précautions, le nombre d'objets connectés corrompus pourrait arrêter de croître, voire diminuer. Tout le monde peut participer à l'effort commun en protégeant davantage ses dispositifs de façon à ce que Mirai et des malwares similaires ne puissent pas prendre le contrôle sur eux. Si tout le monde le faisait, les armées de botnets seraient considérablement réduites.

Pour empêcher votre imprimante, routeur, ou objet connecté d'être utilisé par des botnets, vous pouvez prendre quelques précautions simples:

1. Changez vos mots de passe par défaut pour tous vos dispositifs.
   Utilisez des combinaisons fiables qui ne peuvent pas être forcées facilement.
2. Mettez à jour votre firmware pour tous vos appareils (surtout les plus anciens), si possible.
3. Soyez sélectif au moment de choisir vos objets connectés. Demandez-vous s'il a réellement besoin d'une connexion Internet ? Si c'est le cas, penchez-vous attentivement sur ses caractéristiques et son mode de fonctionnement. Si vous vous apercevez qu'il a des mots de passe difficiles à coder, alors choisissez un autre modèle.
4. Et surtout, demandez-vous si vous avez réellement besoin que vos appareils soient connectés en permanence. La connexion permanente peut sembler apporter un confort supplémentaire mais elle peut également se retourner contre ses « bénéficiaires ». Les caméras de surveillance par exemple, peuvent se mettre à vous espionner si des personnes malveillantes en prennent le contrôle…
5. Les objets connectés à domiciles passent en général par le routeur Wi-Fi pour accéder à Internet. Selon le modèle du routeur, il sera possible de contrôler la manière dont les objets se connectent à Internet et d'éviter que des objets se connectent automatiquement sans autorisation préalable.

En conclusion, la lutte contre les Botnets et les attaques par déni de service doit être menée collectivement par tous les acteurs du marché des objets connectés, y compris les utilisateurs. Mais les fabricants doivent également prendre leurs responsabilités en renforçant le niveau de sécurité des objets connectés qu'ils mettent sur le marché. Sinon, quelqu'un arrivera réellement un jour à « casser » l'Internet.

Pour toute question au sujet de l'arnaque en ligne
ou sur l'utilisation d'Internet en général,
contactez la BEE SECURE Helpline:

BEE SECURE HELPLINE
CONSEIL & AIDE
8002-1234

Éditeur : BEE SECURE · B.P. 707 · L-2017 Luxembourg
Tel.: (+352) 247-86427 · Fax.: (+ 352) 46 41 86
bee-secure@snj.lu · www.bee-secure.lu

THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
Co-financed by the European Union
Connecting Europe Facility