25 octobre 2016
THE DAILY BEAST

Mega attaque sur le web mondial : comment les caméras de surveillance connectées sont devenues une arme de destruction massive

Vendredi dernier, tout un pan essentiel d'Internet a vacillé. Et les pirates responsables de ce bug géant ont utilisé de petits équipements électroniques, tels que les caméras de surveillance. Comment est-ce possible ?

Avec Robert Graham

The Daily Beast - Robert Graham

Vendredi dernier, des hackers ont piraté une grande partie du web américain et tout particulièrement des services situés sur la côte Est des Etats-Unis. Ils ont utilisé une vieille technique connue depuis 20 ans : une attaque "DDos" contre un service DNS.

Cependant, au lieu de lancer l'attaque à partir d'ordinateurs infectés par des virus comme il est d'usage, les pirates ont lancé l'attaque depuis de petits appareils connectés au web, tels que des caméras de sécurité. C'est une évolution inquiétante : ces appareils offrent aux hackers une nouvelle arme très puissante.

La révolution de l'"Internet des objets" est en train d'envahir Internet, avec une armée de voitures, de pacemakers, de robots industriels et de grille-pains. Si vous possédez un appareil ménager qui fonctionne à l'électricité, vous pouvez trouver un appareil similaire qui se connecte à Internet. Avec un dispositif de commande vocale comme Amazon Echo, vous pouvez ordonner à l'eau du café de commencer à bouillir, à la voiture de commencer à chauffer, et aux lumières de s'allumer le matin, le tout avant même d'être sorti du lit. Selon le groupe de recherche Gartner, plus de 6 milliards d'appareils seront ainsi connectés à Internet d'ici fin 2016.

La cyber-sécurité est le prix à payer pour cette nouvelle tendance. Certains appareils bas-de-gamme rognent sur les dépenses de sécurité. Bien qu'ils ne soient pas aussi vulnérables que les ordinateurs domestiques face à certaines attaques (comme les e-mails d'hameçonnage), ils rencontrent d'autres problèmes récurrents (comme les mots de passe appelés "portes dérobées" ou *"backdoor passwords"*). Ce sont des mots de passe comme le mot "assistance", que les fournisseurs paramètrent en secret par défaut dans leurs appareils pour différentes raisons. Tandis que leurs vendeurs se croient malins et discrets, les hackers, eux, trouvent ces mots de passe sans effort. Ils créent des listes de mots de passe répandus et se les échangent entre eux.

Heureusement, les appareils installés chez vous sont protégés derrière votre pare-feu : ils sont donc à l'abri de la plupart des attaques de pirates informatiques. Un pare-feu est un outil de sécurité répandu qui autorise les communications sortantes vers Internet, mais bloque la plupart des communications entrantes. La plupart des appareils qui connectent les habitations à Internet contiennent un pare-feu. Cependant, beaucoup d'autres sont reliés directement à Internet, où les hackers peuvent facilement en prendre le contrôle.

Voilà pourquoi lors des attaques de vendredi, la plupart des appareils étaient des caméras de surveillance plutôt que des moniteurs pour bébés. Les deux appareils font la même chose : de l'enregistrement vidéo. Ils possèdent généralement la même structure interne et les mêmes logiciels sont installés à l'intérieur. Mais les moniteurs pour bébés sont généralement installés dans des maisons,

derrière des pare-feu, auxquels les hackers ne peuvent pas accéder directement. Les caméras de surveillance sont installées dans des immeubles isolés, avec souvent une connexion Internet dédiée spécialement pour la caméra, sans protection par un *firewall*.

La plupart des gens partent du principe qu'il est trop difficile de repérer ces appareils sur Internet. Par exemple, certains villages reculés de Mongolie ont peut-être des caméras de sécurité dotées de liaisons satellite. Mais quel est le risque que les hackers les trouvent ?

La réponse est : 100%. De la même façon qu'il vous suffit d'avoir le numéro de téléphone de quelqu'un pour l'appeler, vous n'avez besoin que d'une adresse Internet pour vous connecter à un appareil. Lorsque vous composez le numéro de téléphone de quelqu'un, le fait que la personne se trouve dans le centre-ville de Berlin ou en Mongolie n'a aucune importance. C'est la même chose pour une adresse Internet. Il y a moins d'adresses Internet que de numéros de téléphone, et seulement environ 4 milliards de combinaisons possibles. Il est possible de toutes les essayer en l'espace de quelques heures.

L'image ci-dessous illustre l'utilisation d'un outil de balayage de port appelé masscan, qui explore toutes les adresses Internet possibles. Comme vous pouvez le voir, en 6 heures environ, il aura scanné tout l'Internet et détecté tous les objets connectés du type de ceux qui ont été utilisés vendredi. Il interroge toutes les adresses possibles et imaginables sur Internet, quelle que soit leur localisation géographique. Si vous examinez attentivement votre pare-feu domestique, vous verrez que quelqu'un avec l'adresse IP 209.126.230.72 a essayé de vous contacter samedi. C'était moi. Et cela vaut même si vous vivez au beau milieu de la Mongolie.

Mais cela n'est même pas nécessaire. Plusieurs sites web gardent une trace de tous ces résultats d'exploration, de telle façon que de simples recherches Internet peuvent être effectuées pour trouver certains types d'appareils. Le plus populaire d'entre eux est Shodan, un moteur de recherche qui peut rapidement générer une liste de millions de cibles dont il est possible de prendre contrôle.

Lors de l'incident de vendredi, les pirates ont utilisé leur propre logiciel de piratage sur-mesure connu sous le nom de MiraiLe blog ThreatPost, spécialisé dans les questions de sécurité, rapporte que 550 000 appareils sont infectés par Mirai, et que 10% d'entre eux ont été utilisés pendant l'attaque.

Mirai scanne Internet. Lorsqu'il repère des cibles, il tente de se connecter en utilisant de nombreux mots de passe "portes dérobées" bien connus.

Lorsque Mirai parvient à infecter un appareil, il prévient alors le hacker qui contrôle maintenant cet appareil. Il est devenu un robot en réseau (*botnet*) sous le contrôle du pirate informatique. Une commande courante consiste à exécuter une attaque DDos. Ce sigle signifie "*Distributed Denial of Service"*(ou "déni de service distribué"). L'attaque provient de milliers d'appareils, la source étant distribuée à travers tous ces appareils. Le terme "déni de service" est un ancien terme informatique qui désigne le fait de faire planter, de ralentir, ou encore de "dénier" aux utilisateurs le "service" fourni par l'outil ciblé.

Le (ou les) hacker(s) derrière Mirai ont commencé à construire leur réseau d'objets connectés "contaminés" depuis quelques mois. On en a vu les scans sur Internet. Et vendredi dernier, au matin, ils ont donné comme instruction aux machines de choisir une cible, en l'occurrence l'un des principaux fournisseurs de DNS (ou fournisseur de noms de domaine, ndlr.). Un DNS est une sorte de répertoire téléphonique d'Internet : il traduit les adresses web exprimées en langage humain en séries de chiffres correspondantes en langage informatique. Quand le DNS plante, techniquement, Internet continue de fonctionner, mais quiconque dépend de ce service DNS se trouve incapable de trouver ce qu'il cherche. La victime de cette attaque, Dyn.com, était un gigantesque fournisseur de nom de domaine, et par conséquent, l'impact de l'attaque a été d'une envergure inédite.

Et le plus alarmant dans l'attaque de vendredi, c'est qu'elle ne requiert aucune compétence particulière. N'importe qui peut utiliser masscan ou Shodan pour détecter des systèmes potentiellement vulnérables. N'importe qui peut infecter ces systèmes avec Mirai et les télécommander. Certains ont suggéré que des gouvernements étrangers pourraient être à l'origine de ces attaques - mais jusqu'ici, nous n'avons rien observé de sophistiqué, rien qui ne nécessite un budget d'État. Tout cela est dans les cordes d'un adolescent un peu geek travaillant depuis le garage de sa mère.

Lorsque les gens ouvrent la boite pour la première fois, ils voient un appareil en apparence innocent. C'est avec ce sentiment qu'ils le connectent à leur réseau. Mais Internet ne les perçoit pas comme des appareils. Internet les voit comme de véritables ordinateurs, sur lesquels tourne le dernier logiciel Windows ou Linus, dotés de grandes capacités de mémoire et une puissance d'ordinateur, et reliés à des liens Internet rapides. Aujourd'hui, les pirates exploitent cette contradiction, en prenant le contrôle de ces appareils, et en les utilisant pour faire planter Internet, et vous ne pouvez rien y faire.