Cyberattaque par détournement d'objets connectés

written by Jacques-André Fines Schlumberger | 24 novembre 2016

En septembre dernier, le leader européen de l'hébergement, OVH, a fait l'objet d'une attaque informatique sans précédent. Les pirates ont détourné près de 145 000 caméras connectées à distance pour engorger l'accès à ses serveurs et faire tomber son infrastructure. Sans succès.

En 2015, l'Agence nationale de sécurité des systèmes d'information (ANSSI) a traité près de 4 000 signalements de problèmes liés à la cybersécurité, soit 50 % de plus qu'en 2014 : 61 % de ces incidents étaient des détournements de sites web ; 12 %, des « *compromissions des systèmes d'information* » ; 8 % étaient liés à des courriels malveillants ; 6 % concernaient des fuites de données ; 5 % étaient des « *infections* » virales ainsi que des attaques par déni de service ; et 3 % des maliciels (logiciels malveillants développés dans le but de nuire à un système informatique sans le consentement de l'utilisateur « infecté »).

L'attaque par déni de service consiste à saturer de connexions un serveur ou le centre de données d'un hébergeur, ce dernier ayant alors les plus grandes difficultés pour « trier » les bonnes données à rediriger vers leurs serveurs. Parmi les attaques par déni de service, celle qui est dite distribuée – DDoS, *Distributed Deny of Service* – consiste à engorger le serveur ou le centre de données d'un hébergeur par l'intermédiaire d'une multitude d'ordinateurs et de machines dont le trafic est dirigé en même temps sur cette seule cible. L'attaque dure en général quelques minutes et peut être répétée toutes les dix ou quinze minutes pendant plusieurs heures, jours, voire semaines. Elles utilisent en général un réseau de « machines zombies » dites *botnets*, machines infectées, souvent à l'insu de leur propriétaire, à la suite d'un courriel malveillant ou d'un téléchargement de logiciel infecté, puis réveillées pour envoyer simultanément des données vers la cible lors d'une attaque. Le service Xbox Live de Microsoft a ainsi été pris pour cible en décembre 2015 par une attaque DDoS visant à démontrer la faiblesse de la sécurité des services de Microsoft.

Jusqu'à ce jour, le réseau de « machines zombies », utilisé pour ce type d'attaque était constitué d'ordinateurs, souvent personnels, sur lesquels était installé un programme caché, téléchargé à l'insu de son utilisateur imprudent. Or, le 22 septembre 2016, le leader européen de l'hébergement, OVH, a fait l'objet d'une attaque DDoS dont la grande majorité des machines programmées pour envoyer des requêtes vers leur centre de données, à Roubaix, était des caméras connectées au réseau.

Selon l'enquête interne menée par OVH, il y avait également, parmi les objets connectés, *« des DVR infectés (Digital Video Recorder, soit les petits serveurs domestiques utilisés pour enregistrer les images des caméras de vidéosurveillance), ainsi que des NAS, des routeurs (des Box xDSL), ainsi que des Raspberry pi »* (un nano-ordinateur de la taille d'une carte de crédit, destiné à programmer et équiper des objets connectés au réseau, voir *La rem*, n°28, p.17).

Ce type d'attaque est nouveau. En décembre 2013, la société de sécurité Proofpoint avait découvert l'un des tout premiers *IoT botnet*, réseau de machines zombies dont 25 % n'étaient pas des ordinateurs personnels, mais des téléviseurs connectés, des interphones pour bébés ou encore des appareils ménagers.

L'intérêt pour les pirates informatiques d'utiliser des objets connectés, et tout particulièrement des caméras, est triple : d'une part, la sécurisation de ces équipements connectés au réseau est quasi nulle. Octave Klaba, le fondateur d'OVH explique que *« tous ces équipements connectés ont en commun l'existence de failles de sécurité relevant de défauts dans leur conception logicielle, de la négligence des constructeurs, qui souvent attribuent le même mot de passe usine par défaut à tous leurs produits, ou de la négligence des installateurs, qui ne prennent pas la peine de le modifier lorsqu'ils les déploient ! »*. Le second intérêt pour les pirates est que la vidéo constitue un document très lourd, et donc gourmand en bande passante.

Chaque caméra pouvant envoyer jusqu'à 30 Mbps de trafic malveillant vers une cible, lorsqu'un réseau de 150 000 caméras est coordonné en même temps pour se connecter vers une seule cible, le trafic auquel est confronté l'hébergeur est considérable et, dans le cas présent, *« a pu s'élever à 1,5 Tbps »*. Enfin, ces caméras, de plus en plus nombreuses, sont en permanence connectées, contrairement aux ordinateurs personnels, et elles disposent de fonctionnalités permettant à leur tour de scanner le réseau à la recherche d'autres équipements sur lesquels installer le programme malveillant. En effet, *« la capacité à accéder aux séquences à distance constitue à la fois l'un des grands arguments de vente* [de] *ces caméras, mais si elles ne sont pas correctement configurées,* [c'est] *leur plus grande faiblesse en matière de sécurité »*, avertissait déjà en 2014 le bureau du commissaire à l'information du Royaume-Uni.

La puissance d'une attaque se mesure à la quantité de données envoyées par le réseau de machines détournées. Peu de serveurs sont capables de résister à quelques dizaines de gigabits de données par seconde (Gbs), et l'on qualifie une attaque majeure lorsque le débit dépasse les 100 Gbs. Sans que l'on sache si c'est une coïncidence, ce même 22 septembre 2016, le blog de Brian Krebs, chercheur en sécurité informatique, régulièrement pris pour cible par des pirates, a également subi une

attaque DDoS d'un débit de 620 Gps, ce qui en faisait l'attaque la plus puissante jamais enregistrée. La société Akamai, qui assurait la sécurité du blog, avait jeté l'éponge au bout de quelques jours, arguant que la facture allait s'élever à 200 000 dollars par an. Incapable de souscrire ce type de contrat, c'est Google en personne qui a offert d'héberger et de protéger sur ses plates-formes le blog de Brian Krebs, dorénavant accessible.

Avec des pointes de trafic à 1,5 térabit de données par seconde, l'attaque contre OVH détient désormais la palme de l'attaque DDoS la plus puissante de l'histoire de l'internet. Octave Klaba précise cependant que *« ce n'est pas à proprement parler OVH qui a été attaqué, mais une poignée de clients hébergés par OVH, dont les attaquants ont tenté de mettre leurs sites KO »*. La société reste très discrète sur la manière dont elle a pu faire face à l'attaque sans que s'écroulent ses centres de données, même si, selon Octave Klaba, *« les internautes originaires des pays d'Europe du Sud ont pu subir des ralentissements lorsqu'ils tentaient d'accéder aux serveurs hébergés chez OVH, et ce parce que les DDoS en provenance de cette région ont été massifs »*. L'hébergeur a d'ailleurs consolidé son infrastructure à certains endroits sensibles. Parce qu'il est directement connecté avec presque tous les acteurs de l'internet en Europe et aux États-Unis, OVH dispose d'une bande passante de 7 Tbs, ce qui explique comment le centre serveur a pu résister à une attaque d'une telle ampleur.

Ce type d'attaque informatique de très grande envergure, lancé à partir d'objets non protégés connectés à internet, quasiment inexistant en 2014, aura tendance à se développer dans un avenir proche. Entre les troisième et quatrième trimestres 2015, le nombre d'attaques DDoS a progressé de près de 40 % selon le rapport de la société Akamai *« State of the Internet/security »*. Et l'internet des objets semble constituer un vivier inépuisable de machines à utiliser pour mener ce genre d'attaque. Alors que la société Level3 estime à 1 million le nombre d'objets connectés potentiellement exploitables pour mener une attaque DDoS de ce type, la société de sécurité NS Focus en aurait identifié 7 millions.

Néanmoins, même si les scénarios catastrophes impliquant l'internet des objets ont fleuri au rythme de leur progressive adoption par le grand public depuis 2013-2014, les utilisateurs y sont encore trop peu attentifs. C'est dans cette optique que John Matherly a créé Shodan, en 2009, un moteur de recherche qui balaie l'adresse IP de l'ensemble des objets connectés sans aucune protection, en fournissant certaines informations dites sensibles. Les données du moteur, payant, après identification, peuvent être intégrées à des programmes informatiques en tout genre. Dans ce même esprit de sensibilisation, un pirate informatique russe a mis en ligne en 2014 le site web insecam.org, qui permet de visualiser les images en temps réel de caméras mal protégées,

disséminées aux quatre coins du monde, 4 700 aux États-Unis, 1 300 au Japon, près de 1 000 en France ou encore 330 en Allemagne.

Les constructeurs d'objets connectés – caméras, téléviseurs, pèse-personnes ou voitures – devront prendre leurs responsabilités quant à la prolifération de ce genre d'attaque, non seulement en sécurisant les objets connectés qu'ils mettent sur le marché, mais aussi en livrant à leurs clients les rapides manipulations nécessaires à la protection de leurs objets. Gageons que les uns comme les autres réagiront face à ce défi.

Sources :

- « 2015 DDoS attacks on the rise, attackers shift tactics », Sharon Sea, Techtarget.com, 22 may 2015.
- State of the Internet Security Report, Akamai, akamai.com, Q2 2016.
- « Derrière une série d'attaques informatiques très puissantes, un réseau d'objets connectés piratés », Pixels – Chroniques des (r)évolutions numériques, *Le Monde*, 26 septembre 2016.
- « Ces cyberattaques dopées par des réseaux d'objets connectés », Sébastien Dumoulin, *Les Echos*, 27 septembre 2016.
- « La goutte DDoS n'a pas fait déborder le VAC », dossier rédigé par OVH, OVH News, ovh.com, 5 octobre 2016.
- « Attaque par déni de service », Wikipedia.org, consulté le 9 octobre 2016.