DDoS : la menace de moins en moins fantôme

Mise à jour le 23/12 à 10h50 (remerciements à Olivier Rigole)

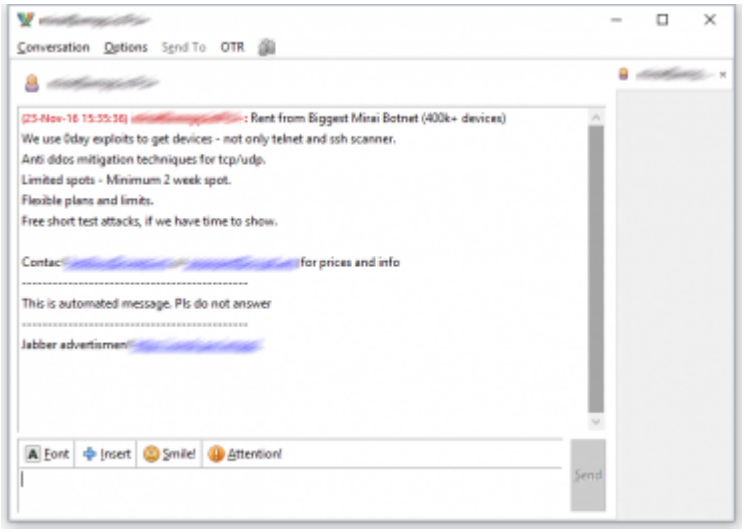
Spécial Bilan 2016. Pour les experts en sécurité, c'est une des tendances majeures de 2016. Au cours de l'année, le DDoS, autrement dit l'attaque par déni de services distribué, basée sur l'envoi de millions de requêtes à un serveur afin d'en saturer les capacités, a pris une nouvelle dimension. Et, pour tout dire, une dimension inquiétante. Celle-ci est attestée par les volumes de trafic générés par ces attaques. 655 Gbit/s contre le site Krebsonline, le blog tenu par le journaliste Brian Krebs ; le site spécialisé dans la cybersécurité n'a pas tenu la charge, malgré la protection que lui offrait Akamai. 1,1 Tbit/s contre l'hébergeur français OVH, qui a bien résisté à cet assaut impressionnant. Mais l'affaire la plus médiatisée concerne un prestataire de DNS (le rapprochement entre l'IP et l'URL d'un site) ayant pignon sur rue, Dyn.

Victime le 21 octobre d'une attaque DDoS massive, ce prestataire a pendant quelques heures baissé pavillon, rendant inaccessibles certains de ses prestigieux clients, dont Amazon, Netflix, Reddit, Twitter, GitHub, Soundcloud, Spotify ou PayPal. L'affaire a évidemment fait grand bruit. Si Dyn n'a pas précisé la bande passante de trafic pirate qu'il a dû encaisser (le chiffre de 1,2 Tbit/s circule), le prestataire n'en a pas moins désigné le coupable : environ 100 000 objets connectés, détournés de leur usage premier par un malware spécialisé appelé Mirai.

Botnet #14 : l'Etoile noire des botnets Mirai

Cette souche, dont le code est librement disponible depuis la fin septembre, cible en effet les nombreuses vulnérabilités des objets connectés, comme des backdoors ou des failles de sécurité grossières (par exemple la présence d'accès de débug) enfouies dans des caméras, des enregistreurs vidéo, des routeurs ou autres. Ainsi, des chercheurs en sécurité ont mis en évidence les faiblesses de nombreux modèles de caméras IP, y compris celles de grandes marques comme Sony. Plutôt que d'asservir des PC d'utilisateurs, les cybercriminels se tournent donc vers ces machines aisément piratables et disponibles en très grand nombre sur la Toile.

Selon deux chercheurs en sécurité, qui via le compte Twitter @MiraiAttacks, suivent l'activité de ces botnets Mirai, la plupart d'entre eux sont relativement petits. Mais l'un d'entre eux serait colossal, « *comptant plus de machines zombies que tous les autres botnets Mirai réunis* ». Suivi sous l'appellation de Botnet #14, ce dernier regrouperait désormais pas moins de 400 000 objets connectés détournés, selon les deux pirates à la tête de cette grosse Bertha de la requête illégitime. Les 'publicités' de ces deux criminels (comme celle reproduite ci-dessus) laissent apparaître des tarifs de DDoS qui varient selon le nombre d'objets enrôlés, la période de pause entre deux attaques et la durée des attaques. A titre d'exemple, 50 000 bots menant, pendant deux semaines, des attaques d'une heure, séparées par 5 à 10 minutes de pause coûtent entre 3 000 et 4 000 dollars.



DDoS pour tester les défenses

Tant et si bien que ces attaques à la capacité de nuisance redoutable semblent à la portée de d'individus frustrés. Après l'interruption de service de Dyn, les experts, comme FlashPoint ou Mikko Hypponen de F-Secure, penchaient plutôt pour une attaque menée par des pirates amateurs. De son côté, le RSSI de Level 3 Communication expliquait, lors d'une audition devant un parterre d'élus américains, qu'il s'agissait probablement une vengeance d'un pirate amateur cherchant à mettre hors ligne un site de jeux vidéo (le Playstation Network de Sony selon le *Wall Street Journal*).

Pas suffisant néanmoins pour atténuer l'inquiétude bien réelle des autorités de divers pays. Car, comme l'a noté l'expert en sécurité Bruce Schneier, depuis environ 12 à 24 mois, un acteur mystérieux teste les défenses des entreprises qui font tourner des infrastructures critiques d'Internet. Via des attaques DDoS calibrées cherchant à évaluer la résistance qui leur est offerte.

Faire tomber les connexions d'un Etat

Les experts relèvent aussi avec inquiétude que le puissant Botnet #14 s'est attaqué, toujours en octobre 2016, à un pays entier, le Libéria. L'attaque était particulièrement violente avec des pics de 500 Gbit/s sur de courtes durées. Coincé entre la Sierra Leone et la Côte d'Ivoire, ce pays africain est connecté à Internet via un câble sous-marin posé en 2011 et qui irrigue l'ensemble du pays. Une proie facile pour un déni de service. L'attaque DDoS a bloqué par intermittence l'ensemble des sites Internet du pays, selon un salarié du principal opérateur mobile du Liberia. Pour le chercheur en sécurité Kevin Beaumont, « *ce type d'attaques est particulièrement inquiétant, car elles suggèrent qu'un botnet Mirai peut avoir suffisamment d'impact pour faire tomber un Etat* ».

Dans le même temps, le fournisseur de solutions anti-DDoS Corero note l'irruption d'un nouvelle technique, capable de générer des attaques courtes mais avec un important facteur d'amplification

(soit la capacité des requêtes illégitimes à générer du trafic inutile sur le réseau de sa cible, engorgeant un peu plus les infrastructures). Selon Corero, qui il est vrai prêche ici pour sa paroisse, cette technique est susceptible de générer des attaques dépassant les 10 Tbit/s dans *« un futur pas très éloigné ».*

« Le début de l'utilisation de l'IoT pour le DDoS »

Dans ce contexte, pas étonnant de voir les grands acteurs d'Internet se lancer dans une course aux armements afin de protéger leurs infrastructures. En France, OVH, cible régulière de DDoS massifs, déploie un nouveau système basé sur des FPGA (Field-programmable gate array), des puces reprogrammables que l'hébergeur place à l'entrée de son réseau pour filtrer les paquets IP illégitimes qui lui parviennent. « *Nous n'en sommes qu'au début du phénomène d'utilisation de l'IoT pour le DDoS* », explique Octave Klaba, le directeur technique et fondateur d'OVH.

De l'autre côté du Rhin, fin novembre, une variante de Mirai a provoqué des ralentissements et des pannes sur des routeurs Zyxel employés par Deutsche Telekom auprès de ses clients haut débit. Le malware semblait vouloir recruter de nouvelles machines zombies pour faire grossir un botnet. A ce titre, les routeurs de box fournis par les FAI sont particulièrement intéressants pour les cybercriminels, car ils sont, par construction, branchés sur une liaison haut débit et sont actifs en permanence. En novembre toujours, la Commission européenne était à son tour victime d'un DDoS, dont l'intensité n'a pas été précisée. L'institution de Bruxelles a vu ses connexions Internet saturées pendant quelques heures.

L'année 2016 dans le rétroviseur :

Comment le ransomware est devenu le gagne-pain des cybercriminels

2016, une année en enfer pour SFR

2016, l'année des vols de données massifs

La longue marche de Microsoft pour imposer Windows 10 au marché

Crédit photo : Rusty Russ via VisualHunt / CC BY-NC-ND