Les protocoles Internet de plus en plus exploités par les attaques DDoS

Les attaques DDoS (Distributed Denial of Service) ont continué de s'intensifier au cours du second trimestre 2015. C'est notamment ce qui ressort du «State of the Internet Security Report» que vient de livrer Akamai (disponible depuis cette page). Un rapport dédié à la sécurité désormais indépendant de l'analyse historique propre au trafic Internet et qui s'appuie notamment sur les données recueillies par Prolexis, spécialiste anti DDoS que le CDN a racheté en décembre 2013. Dans cette édition – la seconde sous cette forme -, Akamai a observé **352,55 millions d'attaques** d'applications Web depuis son réseau.

Il en résulte que, entre début avril et fin juin 2015, pas moins de 12 attaques DDoS ont dépassé les 100 Gbit/s en intensité. **La plus importante ayant atteint les 245 Gbit/s**. Sur ces 12 épisodes, le taux d'envoi moyen de paquets IP par seconde s'est élevé à 46 millions (46 Mpps). Un record. 5 attaques dépassent les 50 Mpps et 1 atteint 214 Mpps. *« Ce volume de paquets est capable d'emporter des routeurs de tiers 1 (chez les principaux opérateurs Internet de la planète, NDLR), comme ceux utilisés par les fournisseurs d'accès »*, signale Akamai pour souligner la puissance de ces agressions.

Le nombre d’attaques a doublé

Si les pics de bande passante sont en progression par rapport à ceux observés au cours des trois premiers mois de l’année, 62 des 85 attaques répertoriées sur la période étudiée, inférieurs à ceux de 2014. Mais le nombre d’attaques DDoS à plus de 100 Gbit/s a doublé au second trimestre 2015 par rapport à la période équivalente de l’année dernière, et a progressé de 50% par rapport aux 8 attaques similaires du premier trimestre 2015.

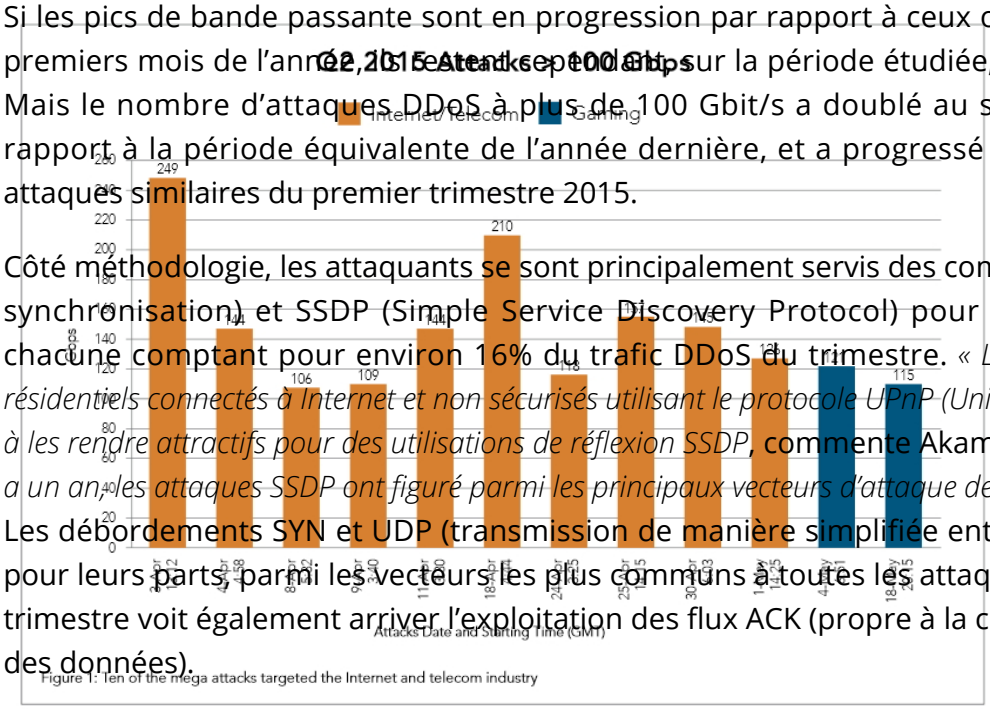

Figure 1: Ten of the mega attacks targeted the Internet and telecom industry

Côté méthodologie, les attaquants se sont principalement servis des commandes SYN (demande de synchronisation) et SSDP (Simple Service Discovery Protocol) pour opérer leurs manœuvres, chacune comptant pour environ 16% du trafic DDoS du trimestre. *« La prolifération des appareils résidentiels connectés à Internet et non sécurisés utilisant le protocole UPnP (Universal Plug and Play) continue à les rendre attractifs pour des utilisations de réflexion SSDP*, commente Akamai. *Pratiquement absentes il y a un an, les attaques SSDP ont figuré parmi les principaux vecteurs d’attaque de ces trois derniers trimestres. »* Les débordements SYN et UDP (transmission de manière simplifiée entre deux machines) restent, pour leurs parts, parmi les vecteurs les plus communs à toutes les attaques volumétriques. Mais ce trimestre voit également arriver l’exploitation des flux ACK (propre à la confirmation de la réception des données).

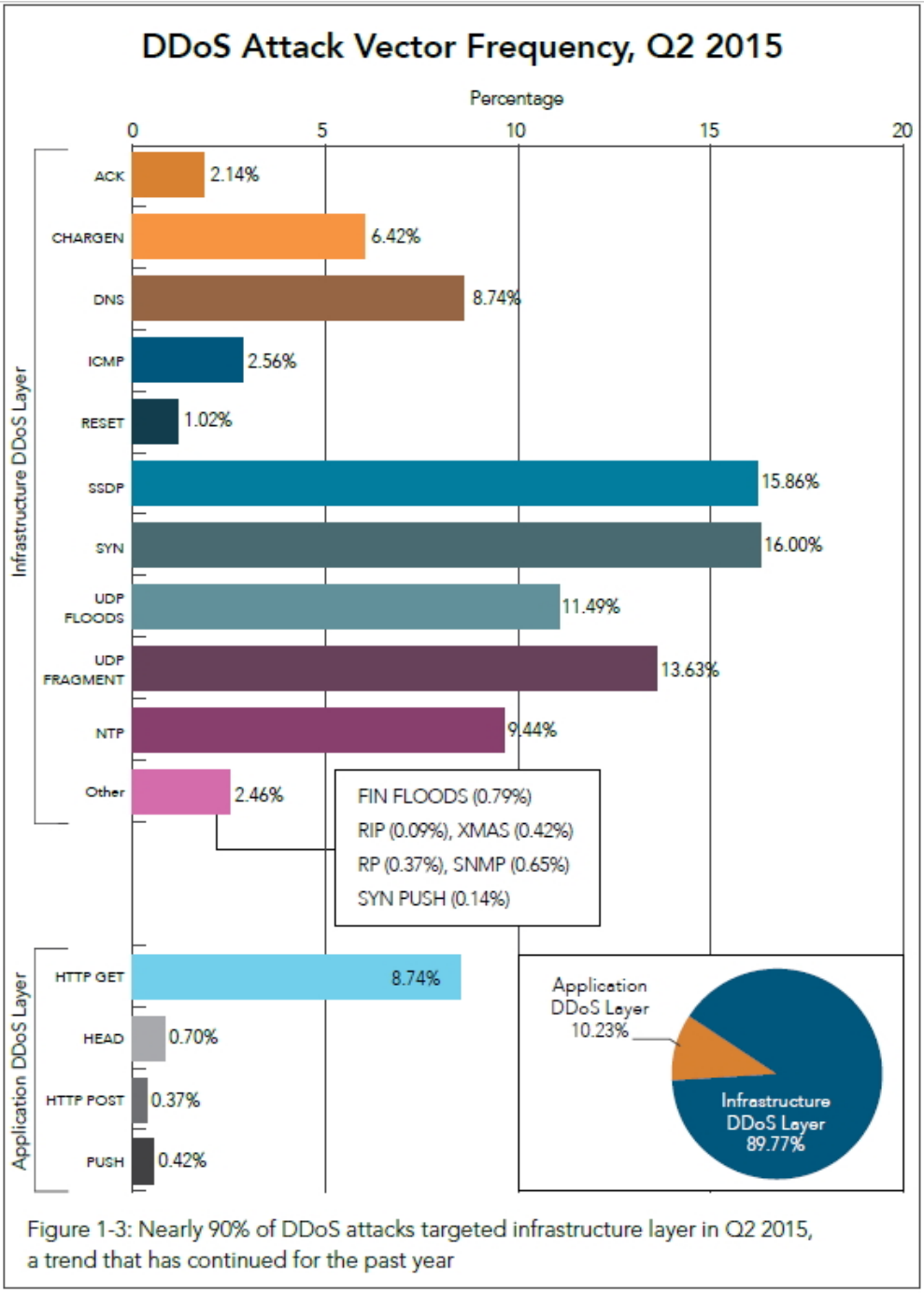

Figure 1-3: Nearly 90% of DDoS attacks targeted infrastructure layer in Q2 2015, a trend that has continued for the past year

La faille Shellshock vecteur d'attaques

Si, comme par le passé, la moitié des attaques DDoS du deuxième trimestre exploitent plusieurs méthodes d'attaque simultanées, une stratégie masquant souvent des services en ligne dédiés à ce genre d'opérations malveillante selon Akamai, une partie de l'autre moitié s'en distingue en s'appuyant sur des bots (ordinateurs contrôlés par les pirates) similaires à Spike et IptabLes/IptabLex, le réseau de machines Linux infectées récemment exploité pour lancer des attaques DDoS.

L'exploitation de la faille Shellshock, un bug de l'interpréteur de commande Bash révélé en septembre 2014, figure en bonne place dans les vecteurs d'attaques aux côtés de XSS (cross-site scripting), SQLi (injection SQL) et LFI (local file inclusion) notamment. Shellshock se retrouve en effet

dans 49% des attaques d'applications Web. Et compte pour 95% de toutes les attaques en HTTPS. *« Néanmoins*, modère Akamai, *95% des attaques Shellshock ont visé un unique client de l'industrie des services financiers, dans une campagne persistante qui s'est déroulée sur les premières semaines du trimestre. »* Le nom de l'entreprise en question reste évidemment confidentiel. Mais la part des attaques HTTPS face à HTTP passe de 9% au premier trimestre à 56% au deuxième. Shellshock, SQLi et LFI combinent à eux trois 93% de l'ensemble des attaques.

WordPress, un vivier de bot

Selon Akamai, la plate-forme WordPress constitue un vivier de réseaux bot pour les pirates. Un phénomène qui s'explique par le manque de sécurisation des plugins de l'outil d'édition de sites web. Sur 1 322 greffons et thèmes publics étudiés par le CDN, 25 affichaient une ou plusieurs vulnérabilités totalisant 49 exploitations potentielles pour dresser des armées de PC zombies. Quant on sait que WordPress motorise environ 25% de l'ensemble des sites Web de la Toile, ça laisse songeur.

Akamai s'est également penché sur le cas de Tor, le réseau de routeurs décentralisés qui accorde un certain niveau d'anonymat à ceux qui l'utilisent. Il s'avère que, si 99% des attaques constatées ne sont pas lancées depuis Tor, 1 requête sur 380 provenant du réseau anonyme est d'origine malveillante. Contre 1 pour 11 500 requêtes pour les adresses IP non-Tor. *« Pour autant, bloquer le trafic Tor pourrait avoir des conséquences négatives sur les affaires*, commente Akamai. *[…] Si le réseau Tor représente un risque élevé pour les sites en matière de sécurité, il fournit également un bénéfice économique potentiel à certaines industries. »* Le commerce en ligne, en premier lieu.

Lire également

Recrudescence d'attaques DDoS depuis de «vieux» routeurs
Une faille BIND ouvre la voie aux attaques DDoS des serveurs DNS
Jérôme Renoux, Akamai : « On déporte la sécurité dans le Cloud »

crédit photo © Duc Dao – shutterstock