# Plus de 1500 attaques DDoS au 3e trimestre 2015

Trimestres après trimestres, le nombre d'attaques DDoS (Distributed Denial of Service) ne cesse de progresser. Pour le seul troisième trimestre, Akamai en a comptabilisé 1□510 depuis son réseau. Soit une hausse de près de 23% par rapport au deuxième trimestre 2015 et de près de 180% comparé au troisième trimestre 2014. Des chiffres issus du dernier rapport State of the Internet de l'opérateur de CDN (content delivery networks).

Si le nombre d'attaques augmente, le volume de trafic généré s'affiche, en moyenne, en recul.

Seules 8 attaques à plus de 100 Gbit/s ont ainsi été comptabilisées au 3e trimestre. Contre 12 trois mois auparavant et 17 il y a un an. De même, l'attaque la plus massive a connu un pic de trafic de 149 Gbit/s (issues du botnet XOR) bien loin derrière les 250 Gbit/s constatés au précédent trimestre.

## Un risque significatif pour la sécurité du Cloud

De quoi se rassurer□? Pas vraiment. *« Bien que les récentes attaques DDoS étaient en moyenne plus petites et plus courtes, elles continuent de poser un risque significatif pour la sécurité du Cloud*, soutient John Summers, vice-président de la division Cloud Security d'Akamai. *Les attaques sont alimentées par la disponibilité triviale de sites de locations de services de DDoS qui identifient et abusent de services Internet exposés, tels que SSDP, NTP, DNS, CHARGEN, et même Quote Of The Day. »*

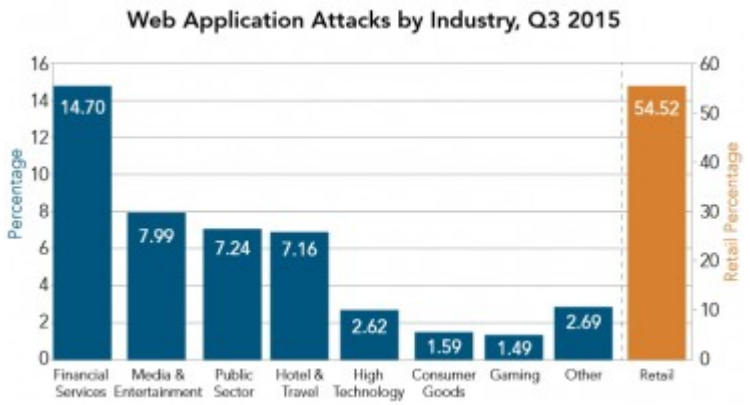
Et si les records ne s'inscrivent pas dans la comptabilité unitaire des actions ou du trafic, ils se déplacent sur d'autres critères de mesures. Un site de média a ainsi subi une attaque DDoS de 222 millions de paquets par seconde (Mpps). Un cran au dessus du record des 214 Mpps constatés au 2e trimestre. *« Une attaque de cette ampleur peut faire tomber un routeur tier 1, comme ceux utilisés par les fournisseurs d'accès Internet »*, précise Akamai.

## La réflexion monte en gamme

Côté méthodologie, les cyber-attaquants montrent de plus en plus de préférences pour les attaques par réflexion aux dépens des DDoS par infection. *« Au lieu de passer du temps et des efforts à construire et entretenir les botnets DDoS comme ils le faisaient dans le passé, les attaquants ont plus exploité le paysage existant d'appareils réseau exposés et de protocoles de services non sécurisé »*, souligne le CDN. Résultat, le taux d'attaques par réflexion est monté à plus de 33% au troisième trimestre alors qu'il ne dépassait pas les 6% il y a un an. Une tendance qui risque de se poursuive à la hausse au cours des prochains trimestres.

Médias et e-commerces auront particulièrement été exposés au cours du trimestre. Sur les 8 attaques à plus de 100 Gbit/s, trois ciblaient les secteurs des médias et divertissement. Les sites de jeux ont subi 50% des attaques et celui des logiciels et technologies 25%. Les sites de vente en ligne ont, eux, subi 55% des attaques par applications web qui sévissent sur les botnets. Suivi du secteur

de la finance à hauteur de 15% des attaques.




# Les États-Unis , première cible

Dans ce cadre, si Akamai note un net ralentissement des attaques HTTPS exploitant la faille Shellshock découverte en septembre 2014 (avec un taux retombé à 12% en recul de 79%), le fournisseur craint que *« l'utilisation d'applications web HTTPS pour mener des attaques est susceptible d'augmenter à mesure que davantage de sites adoptent TLS comme couche de sécurité standard. Les attaquants peuvent également utiliser le protocole HTTPS pour tenter de pénétrer dans les bases de données back-end, généralement accessibles à partir d'applications fournies via HTTPS »*.

Sous l'angle géographique, les États-Unis sont à l'origine de 59% du trafic des attaques et la cible dans 75% des cas.

---

**Lire également**
Quand les attaques DDoS servent à leurrer les équipes IT
Failles NTP : la machine à détraquer le temps menace aussi le chiffrement
Les protocoles Internet de plus en plus exploités par les attaques DDoS

**crédit photo © Duc Dao – shutterstock**