# Les attaques DDoS en pleine expansion au 1er trimestre 2017… ou pas

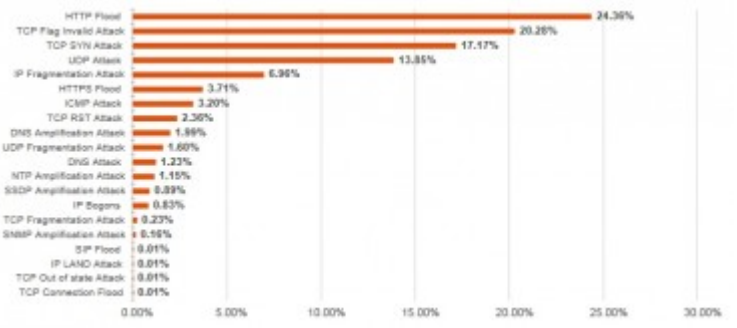
Le volume des attaques DDoS a encore augmenté en 2017. Au cours du premier trimestre, leur nombre a progressé de 380% par rapport à la même période de 2016, rapporte Nexusguard. L'entreprise spécialisée dans les solutions préventives d'attaques par déni de service distribué s'est appuyé sur les données collectées à l'échelle mondiale auprès de ses clients entreprises et opérateurs mais aussi des honeypots (pièges à attaquants), scanner de botnet et autre analyse de trafic entre les cyber-assaillants et leurs victimes.

## Puissance et durée en hausse

La fréquence des attaques DDoS n'est pas la seule à la hausse. Celle de leur puissance aussi. Dans son rapport, Nexusguard avance qu'une attaque de 275 Gbit/s s'est illustrée le 14 février, jour de la Saint Valentin. Le taux d'attaques puissantes (plus de 10 Gbit/s) a progressé significativement au cours du trimestre passant de plus de 48% en janvier à plus de 64% en mars. Elles constituent désormais plus de 23% des attaques, dont 2,67% dépassent les 200 Gbit/s.

Les durées battent aussi des records. Le Nouvel an chinois, le 28 janvier, a vu une charge qui a duré plus de 67 heures (4□060 minutes). Pour la grande majorité (48%), les durées des pilonnages dépassent 90 minutes. Et plus de 4% vont au-delà de 24 heures. La société précise encore les attaques HTTP ont augmenté de plus de 147% entre le dernier trimestre de 2016 et le premier de 2017 (4□053 attaques contre 1□640) sur un total de 15□842 qui s'est limité à 37,6% de croissance sur la période.

## De plus en plus d'attaques multi-vecteurs




Plus inquiétant encore, *« les attaques multi-vecteurs ont joué le rôle de premier plan »*, considèrent les auteurs du rapport. Au cours du premier trimestre, à peine 31% des attaques étaient lancées à partir d'un unique vecteur. Près de 30% des attaques s'appuient aujourd'hui sur deux techniques d'attaques et plus de 20% sur trois. Un certain nombre (1,35%) utilisent même jusqu'à 6 et même 10 vecteurs d'attaque. De fait, les tentatives de saturation des réseaux par HTTP composent aujourd'hui près d'un quart des vecteurs de charges (24,36%) devant les tentatives d'interruption TCP/IP (TCP Flag Invalid) qui constituent plus d'une attaque sur cinq (20,28%). Les assauts via les protocoles TCP SYN, UDP et par fragmentation IP suivent à hauteur de 17,17%, 13,85% et 6,96% respectivement.

Sous l'angle régional, c'est aux Etats-Unis que les DDoS se sont le plus abattus (23,75%) avec la Chine (17,83%) et le Japon (15,35%). L'Europe arrive ensuite à travers l'Allemagne (7,78% des attaques) et la France (6,69%). Notons que, selon Nexusguard, Proxad, l'infrastructure d'Iliad notamment utilisée par Free, constitue l'un des principaux réseaux utilisés pour les DDoS par réflexion avec près de 12% des attaques juste derrière AS-Pnaptor de PNAP (30,6%). Un autre réseau français, celui d'OVH, arrive en 8e place (5,8%).

# Moins de DDoS chez Akamai

Les résultats de Nexusguard contredisent néanmoins ceux d'Akamai. Dans son rapport sur «l'Etat des lieux d'Internet/Sécurité» du premier trimestre 2017, le fournisseur de CDN (content delivery networks) enregistre une baisse annuelle de 30% du nombre total des attaques DDoS sur la période. Et le nombre de celles à plus de 100 Gbit/s est tombé de 19 à 2. Qui plus est, l'attaque la plus puissante du trimestre n'a pas dépassé les 120 Gbit/s même si les DDoS qui génèrent plus de 100 Gbit/s restent *« suffisamment courants pour être préoccupants »*.

Néanmoins, les deux entreprises s'accordent sur l'usage de plus en plus fréquent des botnets d'objets connectés pour actionner des attaques durables et à forte charge. *« Les réflecteurs SSDP, généralement des terminaux IoT grand public, restaient la principale source d'attaques DDoS par réflexion au 1er trimestre »*, considère Akamai dans son document. *« L'exploitation des vulnérabilités qui résultent [des appareils IoT mal sécurisés] a alimenté la croissance rapide de Botnets, qui, à leur tour, fournissent aux attaquants une myriade d'adresses IP détournées, leur permettant de lancer des attaques sophistiquées plus longtemps »*, indique Nexusguard.

---

**Lire également**
**Les attaques DDoS, l'autre machine à cash des cybercriminels**
**Attaques DDoS : une facture moyenne de 2,5 M$ pour les entreprises**
**Quand le protocole CLDAP amplifie les DDoS**