Les attaques DDoS en hausse de 40% au 4e trimestre 2015

Entre les 3e et 4e trimestres 2015, le nombre d'attaques DDoS a progressé de près de 40%. Et de près de 149% sur 12 mois. Les attaques d'applications web ont pour leur part augmenté de plus de 28% sur le trimestre (dont 28,65% pour les applications en HTTP et 24,05% en HTTPS). Le rapport d'Akamai, d'où sont issus ces chiffres, note par ailleurs que les recours aux injections SQL connaissent une recrudescence de plus de 12% sur les trois derniers mois de l'année 2015.

Globalement sur cette période, le fournisseur de solutions de CDN mâtinées de service de sécurité a recensé pas moins de 3□693 tentatives d'attaques depuis sa plate-forme de routage du trafic. Soit une hausse séquentielle de 38%. *« Cette augmentation a largement été tirée par les attaques répétées sur quelques clients plutôt qu'un élargissement du nombre de cibles »*, souligne les auteurs du rapport. En moyenne, chaque client d'Akamai a subi 24 agressions numériques contre 17 sur le précédent trimestre. Mais la durée moyenne des attaques recule□: elle passe de près de 19 heures à moins de 15 heures. Tout comme leur intensité avec 5 attaques à plus de 100 Gbit/s contre 8 précédemment.

Très loin du record des 17 méga attaques constatées au 3e trimestre 2014. Néanmoins, l'attaque la plus massive a atteint les 309 Mbit/s, plus de deux fois plus que la plus imposante du 3e trimestre 2015 avec 149 Gbit/s.

Les test de charge toujours plus utilisés

Selon Akamai, ces résutats s'expliquent notamment par l'adoption toujours plus grande d'outils de test de charge réseau dans les attaques DDoS fournis par des services en ligne et qui permettent aux attaquants d'inonder leurs cibles de trafic massif par des technologies dites de réflexion. *« Parce que la grande majorité de ces sites sont utilisés sur la base d'un abonnement et permettent habituellement seulement des attaques de 20 à 60 minutes, leur utilisation a diminué la durée moyenne des attaques »*, explique le rapport. Que ce soit DNS, Chargen (Character Generator Protocol), UDP ou SNMP, la plupart des services IP ont vu leur trafic augmenter dans le cadre des attaques (respectivement de 92%, 52%, 20% et 57%). Les méthodes d'attaques DDoS multivectoriels (qui utilisent plusieurs outils simultanément) sont désormais utilisées dans 66% des cas (dont 35% à deux vecteurs et 13% à trois vecteurs).

Depuis le 2e trimestre 2014, les sites de jeux en ligne restent la première cible des attaquants. Particulièrement au cours de ce trimestre où ils concentrent 54% des charges. L'industrie IT (notamment les fournisseurs de Saas et particulièrement les services de messagerie instantanée) sont prisées par les acteurs malveillants à hauteur de 23%, un léger mieux en regard des 25% précédents. Mais le nombre des assauts est en croissance, note Akamai. Suivent les services financiers (7%), les média et divertissements (5%), Internet et les télécoms (4% mais à travers les sites hébergés par les fournisseurs), le commerce en ligne (3%), l'éducation (3%) et le secteur public (1%). Mais sur les attaques d'applications, le *retail* revient en première ligne (dans plus de 58% des cas).

La Chine, premier lanceur de DDoS

Plus d'un quart (27,6%) de ces attaques proviennent de Chine (ce qui ne signifie pas nécessairement qu'elles sont opérées depuis ce pays). Précédemment deuxième, l'Empire du milieu détrône le Royaume-Uni qui tombe à la 9e position. Surprise, la Turquie arrive ce trimestre en 2e place des régions les plus agressives avec 22% des attaques. *« La hausse du trafic des attaques de la Turquie était due à un événement impliquant l'utilisation illégitime d'un site générateur de revenus affilié protégé par Akamai »*, justifie néanmoins le CDN. Les Etats-Unis restent en 3e position (15% des attaques) mais en première sur les charge contre les applications web (56%). Sur ce point, la France arrive en 5e place avec 6% des attaques d'applications web derrière le Brésil (8%), la Russie (7%), les Pays-Bas (7%) et devant la Chine (5%). En revanche, l'Hexagone n'entre pas dans le classement des 10 premiers pays visés par les attaques d'applications largement dominé par les Etats-Unis (77% à eux seuls) et alors que nos voisins britanniques (4%), allemands (3%) et néerlandais (2%) y figurent. Sommes-nous à ce point si peu attractifs aux yeux des pirates ?

Lire également
12% des attaques DDoS menées par des concurrents
Sécurité : les DDoS applicatifs montent en puissance
Attaques DDoS : bluffer suffit pour bien gagner

Crédit Photo : Lightspring-Shutterstock