Cybersécurité : 3 points à retenir du rapport Netscout

Netscout a livré son rapport de renseignement sur les menaces* DDoS pour le premier semestre 2020 (« Netscout Threat Intelligence Report »).

Les attaques par déni de service distribué (DDoS pour Distributed Denial of Service) ont proliféré. Et leur fréquence s'est intensifiée sur la période, selon le rapport Netscout.

Une attaque DDoS vise à rendre inaccessible un serveur ou un service en ligne par l'envoi de requêtes multiples ou l'exploitation d'une faille de sécurité visant à le submerger.

Pour Richard Hummel, responsable du renseignement sur les menaces chez Netscout, les initiateurs de ces cyberattaques opèrent un changement « radical » d'approche.

Les entreprises et secteurs visés sont davantage confrontés à des attaques DDoS multi-vectorielles (différentes couches réseau sont ciblées). Ces attaques sont surtout « plus complexes, courtes, rapides et percutantes » que par le passé. Et la tendance devrait se poursuivre, selon le fournisseur américain de la performance réseau et applicative.

Fréquence, rapidité, bande passante

Voici 3 des principaux résultats à retenir de ce rapport :

1. Fréquence accélérée des attaques DDoS

4,93 millions d'attaques DDoS ont été repérées par les systèmes de Netscout au premier semestre 2020 (+15% par rapport au S1 2019). 929 000 environ ont été menées en mai 2020. Un niveau jamais atteint en un mois, selon les données Netscout.

De surcroît, la fréquence des attaques DDoS a bondi de 25% de mars à juin 2020. En plein confinement mondialisé pour tenter d'endiguer la pandémie de Covid-19.

2. Elles sont aussi plus complexes et rapides

Les attaques DDoS de très grande ampleur (plus de 15 vecteurs d'attaque) ont augmenté de 125% (101% en France) par rapport à la même période l'an dernier.

En revanche, la durée de ces attaques DDoS a baissé de moitié (51%) en un an. En outre, 92% des attaques DDoS répertoriées au S1 2020 ont duré moins d'une heure…

Pour quelles raisons ? « Tout est une question d'argent. Les attaques DDoS plus courtes consomment moins de ressources pour leurs initiateurs. Mieux encore (les concernant), le temps de réponse de la partie adverse est réduit », ont souligné les auteurs du rapport.

3. Qui paie la bande passante ?

Netscout a développé un coefficient d'attaque DDoS (DAC ou DDoS Attack Coefficient). Ce coefficient représente la quantité de trafic d'attaque DDoS dans le flux Internet une minute durant pour une région ou un pays donné.

Le DAC le plus élevé (877 Mbps) a concerné la région Asie-Pacifique sur le semestre. La bande passante la plus importante (2,8 Tbps) a été affichée dans la zone Europe, Moyen-Orient, Afrique (EMEA). Or, les cybercriminels ne paient pas pour la bande passante qu'ils empruntent à des fins illicites… Les entreprises et les particuliers en supportent le coût.

En France, la tendance se confirme. Aussi, en mars 2020, au début du confinement national, les équipes ASERT de Netscout ont observé une hausse significative de la bande passante dans l'Hexagone, passant de 68 Mbps en février à 275 Mbps en mars.

*Le « Threat Intelligence Report » s'appuie sur l'analyse des données couvertes par ATLAS (Arbor Active Threat Level Analysis System) et les recherches de l'équipe ASERT (ATLAS Security Engineering and Response) de Netscout.

(crédit photo de une © Shutterstock)