Principales conclusions du rapport

Les chercheurs d'Akamai ont observé que le nombre d'attaques DDoS dans la région EMEA n'a cessé d'augmenter, avec des pics plus élevés, depuis le début de l'année 2019.

Plus d'un tiers des attaques DDoS dans le monde se produisent dans cette région.

La complexité et la gravité des attaques DDoS s'y sont accrues pour des motifs géopolitiques, tels que l'hacktivisme, avec des conséquences potentiellement mortelles.

Parmi tous les types d'attaques DDoS, les attaques DDoS DNS sont les plus répandues, selon une étude d'Akamai. Plus précisément, nous avons observé que le vecteur NXDOMAIN (domaine inexistant), également appelé vecteur Pseudo-Random Subdomain, inondait les serveurs de noms DNS de requêtes pour des domaines inexistants.

Plus d'un tiers des événements DDoS ont utilisé plusieurs vecteurs d'attaque (jusqu'à 12) pour accroître leur efficacité.

Dans la région EMEA, les services financiers sont le segment de marché qui connaît le plus grand nombre d'attaques de couche 3 et 4, tandis que le commerce est le secteur qui subit le plus grand nombre d'attaques de couche 7.

Les gouvernements et les nations de la région EMEA ont repensé le pouvoir de l'infosécurité en adoptant de nouvelles mesures législatives, telles que les directives NIS2 et DORA, afin d'influencer positivement les stratégies informatiques et de cybersécurité, notamment en améliorant la résilience et la protection contre les attaques DDoS.