Attaques DDoS en baisse, les cybercriminels ne lâchent rien

Internet

Posté par : JulieM

Publié le : 29/6/2022 13:00:00

Sur la seconde partie de l'année 2021, les restrictions COVID-19 se sont assouplies et les citoyens ont commencé à retourner dans leurs bureaux physiques et leurs salles de classe.

Ce retour progressif à la vie pré-pandémique a coïncidé avec une diminution du nombre d'attaques par déni de service distribuées (DDoS), tant en France qu'au niveau mondial. En effet, un million d'attaques DDoS en moins ont été perpétrées entre le premier semestre 2021 (5,4 millions) et le second (4,4 millions).

Pour sa part, la France a enregistré une baisse de 6 % de la fréquence des attaques DDoS au second semestre 2021, contre 46 % chez ses voisins allemands et britanniques sur la même période.

Pour Philippe Alcoy, spécialiste de la sécurité chez NETSCOUT, s'il est tentant de considérer la diminution du nombre total d'attaques comme un signe que les cybercriminels pourraient se reposer sur leurs lauriers, il n'en est rien.

En réalité, ce ralentissement témoigne surtout d'innovations constantes et de recherches de nouvelles techniques d'attaque pour renforcer et monétiser leur comportement malveillant.

« Les cybercriminels ont adopté une nouvelle approche, et lancent davantage d'attaques DDoS par voie directe (sans spoofing) à l'aide de botnets et d'inondations basées sur le protocole TCP.

Pour preuve, en France les attaques basées sur le protocole TCP représentent quatre des cinq principaux types de vecteurs d'attaque ayant touché le pays. Leur augmentation s'est faite au détriment des attaques par amplification DNS, qui restent malgré tout le deuxième vecteur d'attaque utilisé en France sur le second semestre 2021 ; cela témoigne de la popularité de cette méthode d'attaque.

Toutefois, cette accalmie peut être trompeuse. Bien que le nombre d'attaques DDoS qui ont eu lieu à la fois dans le monde et en France ait diminué sur la période, cela représente toujours une augmentation de l'activité d'attaque par rapport aux niveaux pré-pandémiques. Il est donc vital que les organisations restent vigilantes et anticipent les attaques DDoS.

Pour ce faire, investir dans des systèmes de protection DDoS robustes et efficaces les aidera à atténuer les menaces DDoS, empêchant ainsi les attaques de causer des dommages importants. Une approche proactive plutôt que réactive sera également plus efficace pour protéger leurs infrastructures.

De plus, elles peuvent faire appel à un spécialiste des attaques DDoS pour les aider à s'orienter dans le paysage peu familier et en constante évolution de la cybersécurité.

Enfin, les organisations doivent tester périodiquement leurs systèmes de protection afin d'identifier les changements dans la méthodologie des attaques et évaluer leurs niveaux de vulnérabilités et les résoudre.

Une combinaison des meilleures pratiques actuelles et des mesures efficaces d'atténuation des attaques permettra aux entreprises françaises de protéger leurs ressources digitales contre les attaques DDoS. Elles prendront ainsi véritablement en charge leur cybersécurité pour prolonger la continuité de leurs activités et rester compétitives et performantes. »