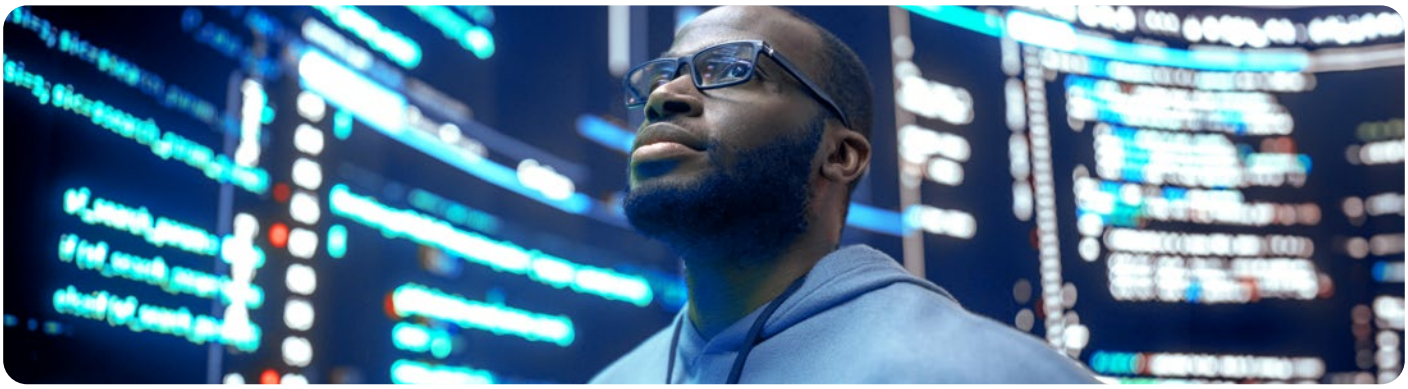
L'heure juste sur les attaques par déni de service distribué

Sept faits qui exposent votre entreprise à des risques



Le paysage des cybermenaces évolue rapidement et les organisations font l'expérience d'attaques plus complexes que jamais. Les attaques par déni de service distribué sont parmi les plus agressives tant du point de vue de leur nature que de leur volume, le nombre d'attaques ayant augmenté de plus de 150 % en 2022[1]. Malgré cette réalité, de nombreuses organisations croient que les attaques par déni de service distribué sont un problème facile à résoudre. Vous trouverez ci-dessous sept faits qui montrent que les attaques par déni de service distribué sont des menaces sérieuses.

Fait 1 : tous les secteurs peuvent faire l'objet d'une attaque; personne n'est à l'abri

Bien que certains secteurs d'activité soient plus susceptibles d'être victimes d'une telle attaque, n'importe quel secteur peut être visé. La facilité d'accès et le faible coût d'exécution des attaques font en sorte que les pirates informatiques peuvent très facilement lancer des attaques contre n'importe quelle entreprise ou personne, dans n'importe quel secteur d'activité. Les attaques par application Web et API ont connu une croissance exponentielle tout au long de 2022. Cela a élargi le paysage des menaces, augmentant le risque pour tous les secteurs.

Fait 2 : les attaques par déni de service distribué ne se limitent pas à la dégradation des sites Web

Les attaques par déni de service distribué sont souvent une diversion pour des attaques plus graves. Pendant que le centre de gestion de la sécurité est occupé à répondre à l'attaque par déni de service distribué, les pirates informatiques peuvent utiliser d'autres tactiques pour voler des données ou naviguer (latéralisation) dans le système du client. Par conséquent, il est essentiel de réduire ce qui est souvent perçu comme du bruit afin de permettre à votre centre de gestion de la sécurité de faire son véritable travail, c.-à-d. de détecter des menaces importantes.

Fait 3 : les coupe-feu seuls n'offrent pas une protection suffisante

Les coupe-feu et les IPS ont parfois des fonctions de protection contre les attaques par déni de service distribué utiles pour détecter certaines adresses IP malveillantes. Cependant, elles ne sont pas efficaces contre les attaques massives ou les attaques de couche 7. Il est conseillé de disposer d'un coupe-feu d'applications Web pour détecter les attaques OWASP 10, les exploitations de couche 7, en conjonction avec une protection contre les attaques par déni de service distribué.

Fait 4 : les attaques par déni de service distribué ne se limitent pas aux attaques massives

Bien que le nombre d'attaques massives au niveau de la couche réseau soit plus élevé, le nombre d'attaques lentes au niveau de la couche application est aussi en augmentation. Les attaques utilisant plusieurs vecteurs deviennent de plus en plus courantes; celles-ci combinent des attaques massives au niveau de la couche réseau à des attaques sophistiquées au niveau de la couche application. Les attaques par application Web et API ont augmenté de 128 % de 2021 à 2022[1].

Fait 5 : les répercussions d'une attaque par déni de service distribué vont au-delà de votre site Web

N'importe quel actif connecté à Internet peut être touché : la chaîne d'approvisionnement, les points de vente, le traitement des transactions, les dossiers des patients et le service à la clientèle, pour ne nommer que ceux-là. Tous les systèmes communiquant avec l'extérieur ont besoin de protection, peu importe où ils sont gérés. L'accès à vos systèmes en ligne peut même être bloqué si vos serveurs de noms de domaine sont attaqués.

Fait 6 : les organisations de toutes tailles sont sujets aux attaques

Les attaques par déni de service distribué peuvent toucher n'importe quelle entreprise, peu importe sa taille. Avec l'émergence du déni de service distribué avec demande de rançon, les entreprises plus petites deviennent des proies plus faciles, car elles ont des ressources TI limitées pour contrer ces attaques.

Fait 7 : les solutions de protection contre les attaques par déni de service distribué doivent être au cœur de votre planification budgétaire en matière de cybersécurité

Compte tenu du nombre croissant d'attaques et du degré de sophistication, l'impact sur les entreprises est bien plus qu'une perte de revenus. L'atteinte à la réputation, le désabonnement des clients et des conséquences juridiques sont tout autant de risques considérables. Quelle que soit la fréquence, la durée ou la taille de l'attaque, les organisations non protégées ont subi une perte moyenne de 200 000 $ par attaque par déni de service distribué[2], sans parler des attaques associées aux rançongiciels. En 2020, le coût moyen des attaques par rançongiciel au Canada était de près de deux millions de dollars[3].

Protégez votre réseau et assurez la sécurité de votre entreprise avec Bell

En tant que plus grand exploitant de réseau au Canada, Bell possède un avantage unique sur le paysage des menaces de déni de service distribué, et peut fournir la protection pour détecter, atténuer et filtrer les attaques de déni de service distribué.

Pour obtenir une évaluation et déterminer si votre entreprise est à risque, demandez qu'un de Bell vous vous rappelle.

Pour en savoir plus sur les attaques par déni de service distribué et la sécurité du réseau, visitez bell.ca/securiteDDoS

[1] Rapport d'analyse des menaces mondiales 2022 – Radware
[2] Financial Post : Attaques de déni de service distribué au H1 2023 en hausse de 200 % par rapport à 2022 selon les nouvelles données de Zayo
[3] Rapport 2020 sur la défense contre les cybermenaces (CD