# Évaluation du risque d'attaques par DDoS

## Un guide pour évaluer votre vulnérabilité aux attaques par déni de service distribué (DDoS)

Un guide d'auto-évaluation de Bell

# Déterminez votre profil de risque d'attaques par DDoS

Les attaques par déni de service distribué (DDoS) étant de plus en plus courantes, il est essentiel que vous ayez une stratégie en place pour protéger vos actifs et votre infrastructure numériques. Mais il faut que ce soit la bonne stratégie, adaptée aux besoins et aux risques de sécurité TI propres à votre entreprise.

En fait, les entreprises ne sont pas toutes tenues d'investir dans un système de protection complet et ultrarobuste pour se protéger contre les attaques par DDoS. Avant d'investir dans une solution de sécurité TI, prenez quelques minutes pour répondre aux questions de cette évaluation. Cet exercice vous aidera à avoir une conversation éclairée sur votre profil de risque face aux attaques par DDoS et le niveau de protection dont vous avez besoin, ce qui vous mettra en bien meilleure position pour trouver la bonne solution – et le bon fournisseur de services de sécurité – pour votre entreprise.

---

## Quelle est la visibilité de votre organisation en ligne?

- Avez-vous une présence en ligne importante?
- Êtes-vous une marque réputée à l'échelle nationale ou internationale?

Si c'est le cas, vous êtes plus susceptible de figurer sur la liste des cibles potentielles d'un attaquant – et d'avoir ainsi besoin d'une solution de sécurité robuste contre les attaques par DDoS.

Certains pirates sont motivés par l'appât du gain (par extorsion ou rançonnement); d'autres sont tout simplement à la recherche de gloire et de notoriété. Provoquer la panne du site Web d'une agence de presse, d'un studio de cinéma, d'un détaillant en ligne, d'un éditeur de jeux vidéo, d'un service gouvernemental ou d'une autre organisation à grande visibilité est un moyen facile pour les attaquants de générer de la publicité et de retenir l'attention de leurs pairs.

## Appartenez-vous à un secteur d'activité à haut risque?

- Est-ce que les gens comptent sur les services en ligne de votre organisation?
- Êtes-vous dans un secteur d'activité vulnérable aux échos négatifs?

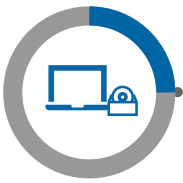
Vos besoins de sécurité face aux attaques par DDoS dépendent grandement du secteur d'activité dans lequel vous évoluez. Même si aucun secteur n'est à l'abri d'une attaque par DDoS, certains types d'organisations sont plus susceptibles d'être ciblées que d'autres – et ont ainsi besoin d'un niveau de protection plus grand. Le graphique suivant montre les secteurs qui sont le plus souvent ciblés par les attaques par DDoS et les facteurs qui en font des cibles potentielles.

# Secteurs les plus ciblés par les attaques par DDoS[1]

## 1. Jeux

- La tendance dans ce secteur est aux jeux multijoueurs en ligne où la moindre interruption peut perturber l'expérience utilisateur
- De nombreux jeux doivent demeurer en ligne en tout temps, ce qui crée un point de défaillance unique que les attaquants peuvent exploiter
- Certaines attaques sont lancées pour protester contre des changements apportés à un jeu et d'autres tout simplement pour la notoriété

## 2. Logiciels et technologie



- De plus en plus de solutions dépendent maintenant de technologies en nuage, comme le logiciel-service, et toute interruption peut avoir un fort impact sur les utilisateurs
- La distribution centralisée des logiciels constitue un point de défaillance unique que les attaquants peuvent exploiter
- Le plus souvent, les attaquants vont cibler ce secteur d'activité au moyen d'attaques visant les applications Web[1]

## 3. Médias et divertissement

- Les agences de presse et les studios de cinéma sont souvent ciblés en raison de leur grande visibilité
- Les « hacktivistes » pourraient paralyser un site de nouvelles pour protester contre le genre d'articles qu'il publie

## 4. Internet et télécoms

- Les attaquants frappent généralement un fournisseur de services Internet afin de bloquer les services qu'il offre à leurs véritables cibles
- Les FSI qui hébergent un grand nombre de sites (ou des sites réputés) sont plus exposés au risque

## 5. Services financiers

- Les banques, les compagnies d'assurance et les fournisseurs de services de paiement – et même les petites coopératives d'épargne et de crédit et les maisons de courtage – présentent une occasion d'extraire de l'information financière monnayable
- Pendant que l'équipe de sécurité s'affaire à régler la panne du site Web, l'attaquant peut en profiter pour pénétrer dans le réseau interne, y installer un logiciel malveillant et voler des données sur les clients
- Le plus souvent, les attaquants vont cibler ce secteur d'activité au moyen d'attaques visant les applications Web[1]

## 6. Éducation

- Parmi les cibles courantes, on compte les serveurs de courriel ou les services en ligne utilisés pour soumettre des travaux, saisir les notes et gérer les admissions
- Les services d'« attaque DDoS sur commande » étant en plein essor, tout étudiant mécontent qui possède une carte de crédit peut rapidement et facilement lancer une attaque

## 7. Gouvernement

- Les attaquants n'ont pas tous une motivation politique : certains veulent publiquement humilier le gouvernement en exposant au grand jour les défaillances de son système de sécurité en ligne, tandis que d'autres sont à la recherche de notoriété[2]

## 8. Vente au détail

- Toute interruption d'une boutique de commerce électronique a un impact direct sur ses revenus et sa réputation
- Les cyberattaques peuvent servir à détourner l'attention d'autres attaques – p. ex. attaques de rançonnement ou importants vols de données
- Les renseignements sur les clients qui se trouvent dans les bases de données des détaillants constituent une cible attrayante
- Ce secteur est le plus frappé par des attaques visant les applications Web[1]

---

[1] Akamai. *Q1 2016 State of the Internet - Security Report*. Extrait de https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q1-2016-state-of-the-internet-security-report.pdf.

[2] Radware. *2015-2016 Global Application and Network Security Report.* Extrait de https://www.radware.com/ert-report-2015/.

# Quelle est l'importance de votre présence Web pour votre entreprise?

- Réalisez-vous des opérations financières en temps réel et d'autres transactions clients sur votre infrastructure Web?
- Le succès de votre entreprise dépend-il de votre capacité d'offrir une expérience en ligne fiable et uniforme à vos clients?

Si vous avez répondu « oui » à l'une de ces questions, la protection contre les attaques par DDoS est fortement recommandée – même si vous n'êtes pas une grande marque nationale – parce que les interruptions de service coûtent cher.

En fait, si vous êtes une plus petite organisation qui compte énormément sur Internet pour le commerce en ligne ou d'autres transactions avec les clients, il vous sera encore plus difficile de vous remettre des pertes de revenus et de la perception négative des clients qui découlent d'une attaque par DDoS prolongée.

# Quel serait l'impact d'une attaque sur votre entreprise?

- Quel serait le coût d'une panne de serveur ou de site Web, peu importe sa durée?
- Quel serait le coût de reprise des activités après une attaque?
- Quels seraient les effets d'une attaque sur votre marque et votre réputation?

Si votre site de commerce en ligne est paralysé, vous en subirez immédiatement les conséquences sous forme de ventes perdues. Et plus il faut de temps à votre équipe TI pour relancer vos applications et vos serveurs, plus les occasions qui vous filent entre les doigts sont nombreuses. La reprise complète de vos activités pourrait exiger des heures, voire des jours. Votre entreprise est-elle en mesure de traverser cette tempête?

En tenant compte des pertes de revenus et des coûts de la main-d'œuvre TI, 35 % des décideurs du monde de la sécurité TI en Amérique du Nord disent qu'il en coûterait entre 10 000 $ et 100 000 $ pour reprendre les activités après une attaque par DDoS, et 31 % parlent de plus de 100 000 $[3]. Et ces coûts ne comprennent pas les dommages potentiels à votre image de marque et à votre réputation. Dans un monde où les médias sociaux sont omniprésents, de mauvaises expériences clients pourraient miner votre capacité d'attirer et de fidéliser les clients longtemps après la reprise de vos activités.

# Communiquez avec Bell

Bell offre plusieurs services de sécurité gérés et professionnels qui peuvent vous aider à évaluer plus en profondeur vos besoins en matière de sécurité, à planifier votre stratégie et à mettre en œuvre la solution DDoS qui convient à votre organisation.

Communiquez avec votre conseiller Bell pour découvrir comment nos experts peuvent vous aider à protéger votre réseau et votre entreprise.

---

[3] Forrester Research. (2014). *Comment protéger votre entreprise contre les attaques par déni de service distribué (DDoS) – livre blanc*. Extrait de https://entreprise.bell.ca/magasiner/entreprise/livre-blanc-securite-services-geres-attaques-ddos-forrester.