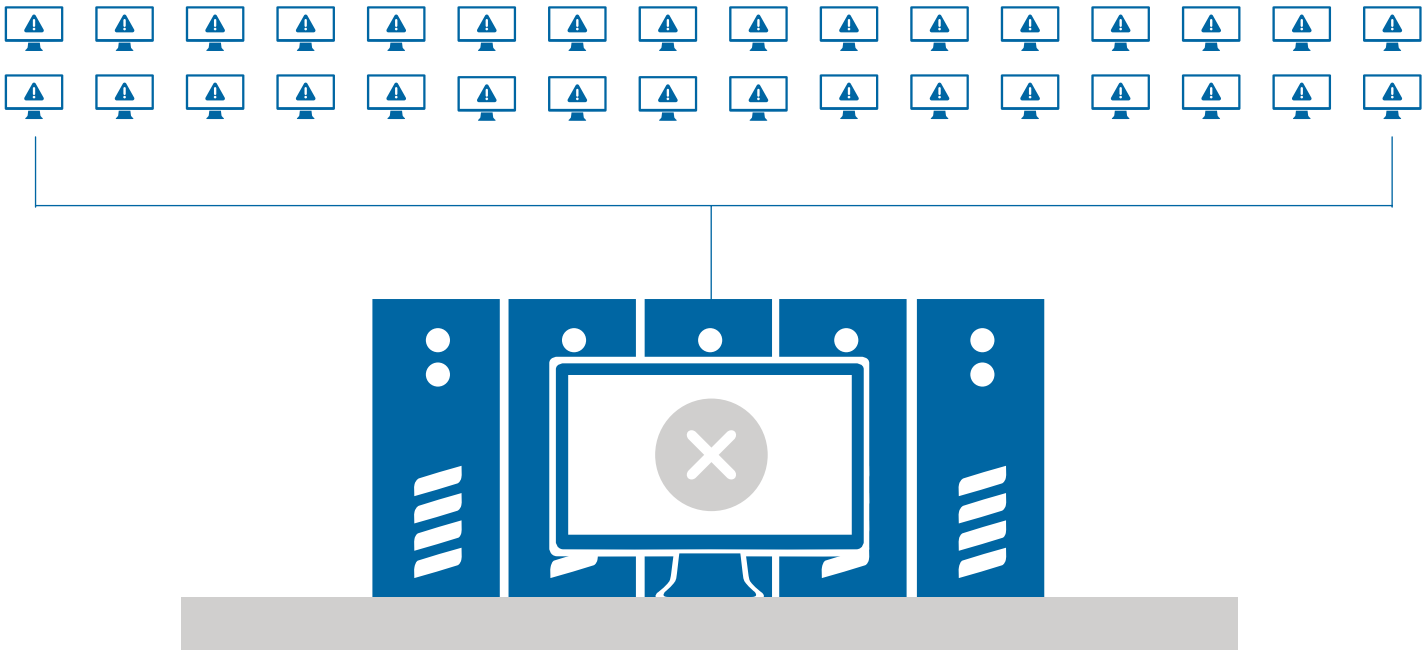

# Introduction aux attaques DDoS

## Guide des causes, coûts et conséquences des attaques par déni de service distribué (DDoS)

Un livre blanc de Bell

# Sommaire

La moitié de toutes les organisations considèrent maintenant les attaques par déni de service distribué (DDoS) comme la cybermenace qui causera le plus de tort à leurs activités commerciales. Comme ces attaques deviennent plus répandues (et de plus en plus perfectionnées), la première étape pour protéger votre organisation consiste à savoir exactement ce à quoi vous êtes confronté.

Ce livre blanc fait le point sur la manière dont fonctionnent les attaques par déni de service distribué (DDoS), pourquoi elles deviennent plus courantes, et les coûts et conséquences qu'elles peuvent entraîner pour la rentabilité et la réputation de la marque de votre organisation.

## Table Des Matières

Une menace croissante ..... 1

Comment fonctionnent les attaques DDoS ..... 1

Comment une attaque DDoS nuit à vos activités commerciales ..... 5

Conclusion ..... 7

À propos de Bell ..... 8

# Une menace croissante

Il se peut que les vols de numéros de carte de crédit et les violations de la confidentialité de données d'entreprise fassent les gros titres, mais les attaques par déni de service distribué (DDoS) causeront fort probablement tout autant de nuits blanches à un grand nombre de chefs de l'information. En fait, la moitié de toutes les organisations considèrent maintenant les DDoS comme la cybermenace qui infligera le plus de dommages à leurs activités commerciales[1].

Les attaques DDoS sont de plus en plus prédominantes et peuvent avoir des effets dévastateurs sur les organisations de toutes tailles. À l'échelon le plus élevé, leur objectif est simple : empêcher le trafic d'utilisateurs légitimes d'accéder aux services et ressources en ligne d'une organisation. Les cybercriminels s'y prennent en mettant les sites Web hors ligne et en ralentissant considérablement les serveurs, ce qui limite gravement l'aptitude de l'organisation à exercer ses activités commerciales et met en péril l'expérience client.

Dans le cadre d'un récent sondage mené par Radware auprès de plus de 300 entreprises à l'échelle mondiale, 90 % des répondants ont déclaré qu'ils ont subi un type quelconque de cyberattaque en 2015, et plus de la moitié, soit 51 %, ont signalé avoir essuyé une attaque DDoS[2]. Et si les plus récentes tendances servent d'indicateur, ce chiffre grimpera encore davantage à court terme. Entre les 3e et 4e trimestres de 2015, le nombre d'attaques DDoS signalées a bondi de 39,9 %; si on compare le 4e trimestre de 2014 au même trimestre de 2015, le nombre a monté en flèche au rythme stupéfiant de 148,9 %[3].

**90%** **des répondants ont déclaré qu'ils ont subi un type quelconque de cyberattaque en 2015, et plus de la moitié des répondants ont signalé avoir essuyé une attaque DDoS[2].**

La bonne nouvelle, c'est qu'il existe de solides défenses contre les attaques DDoS. Toutefois, pour comprendre comment et pourquoi elles sont efficaces, il est important de savoir ce qui se produit au cours d'une attaque DDoS.

# Comment fonctionnent les attaques DDoS

## Cibles multiples, chemins multiples

La plupart des attaques DDoS prennent l'une de deux formes principales:

### Attaques massives

Également connues sous le nom d'inondation de réseau, ces attaques utilisent des milliers de demandes d'information simultanées afin d'encombrer la liaison Internet cible d'une entreprise, de congestionner son réseau et de rendre son site Web largement inaccessible. C'est essentiellement comme un engorgement en ligne monstre qui force plusieurs voies de trafic utilisateur à converger en une seule. Si vous tentez d'accéder au site Web visé, il vous faudra beaucoup de temps pour l'atteindre (si jamais vous l'atteignez).

### Attaques lentes de faible intensité

Ces attaques reposent sur de plus petits volumes de demandes d'information soigneusement élaborées formulées sur une plus longue période, ce qui les rend plus difficiles à détecter. Elles ont pour but d'occuper toute la mémoire ou la puissance de traitement disponible d'une application ou d'un serveur afin d'épuiser petit à petit les ressources informatiques des équilibreurs de charge, des serveurs et des coupe-feu. Quasi immobilisée par ce trafic illégitime, l'infrastructure des TI se bat pour traiter les véritables demandes d'utilisateur, ce qui la force à fonctionner de manière inefficace ou même à s'arrêter totalement.

---

[1] Radware. *2015-2016 Global Application and Network Security Report*. Extrait de https://www.radware.com/ert-report-2015/.
[2] Radware. *2015-2016 Global Application and Network Security Report.* Extrait de https://www.radware.com/ert-report-2015/.
[3] Akamai. *Q4 2015 State of the Internet - Security Report*. Extrait de https://content.akamai.com/PG5795-Q4-2015-SOTI-Security-LandingPage.

Qu'elles adoptent une approche massive ou lente de faible intensité, les attaques DDoS ciblent ordinairement deux volets essentiels de l'infrastructure de TI d'une organisation : son réseau et ses applications[4].

### Attaques de la couche réseau

Les attaques contre la couche réseau (appelées aussi « attaques des couches 3 et 4 ») visent à surcharger les connexions au réseau en gonflant le volume du trafic et en occupant d'énormes quantités de bande passante. Bien que l'attaque la plus volumineuse puisse occuper autant que 200 gigabits de bande passante par seconde (Gbit/s), seulement 40 Gbit/s suffiront à mettre la plupart des réseaux en panne. Ce type d'attaque peut bloquer l'accès aux serveurs et entraîner d'énormes frais d'utilisation excédentaire de données et de bande passante pour la victime. Les auteurs de l'attaque ciblent le réseau en exploitant les vulnérabilités sur des plans comme le protocole de datagramme utilisateur (UDP), le protocole de synchronisation de réseau (NTP) et le système de noms de domaine (DNS). Les attaques de la couche réseau comptent actuellement pour 97 % de toute l'activité DDoS et ne montrent aucun signe de ralentissement, comme en témoigne la hausse de 42,4 % du nombre d'attaques signalées du 3e au 4e trimestre de 2015[5].

### Attaques contre la couche application

Les attaques contre la couche application (appelées aussi « attaques de la couche 7 ») sont conçues pour surcharger un serveur en lui envoyant une énorme quantité de demandes qui exigent la manipulation et le traitement d'un grand nombre de ressources. Il suffit habituellement de 50 à 100 demandes par seconde pour ralentir énormément ou mettre à l'arrêt un site Web moyen. Ce type d'attaque cible les protocoles d'application qui recèlent des faiblesses exploitables, comme le protocole de transfert hypertexte (HTTP), le protocole de transfert de courrier simple (SMTP), le protocole de transfert de fichiers (FTP) et le langage d'interrogation structuré (SQL). Le nombre d'attaques contre la couche application qui ont été signalées est également en plein essor et a augmenté de 28,2 % du 3e au 4e trimestre de 2015[6].

Étant donné qu'elles sont les cibles d'attaque les plus répandues, rien de surprenant que les couches réseau et application bénéficient de la plus grande proportion d'investissement en sécurité des TI. Ces deux couches ont reçu respectivement 30 % et 19 % du financement de sécurité des TI budgété, réservé ou affecté en 2015[7].

## Une armée de zombies

Les attaques DDoS sont qualifiées de « distribuées » parce que les demandes proviennent de centaines voire de milliers de sources à la fois, plutôt que d'un seul ordinateur (comme c'est le cas d'une attaque par déni de service traditionnelle). Cette approche mise d'ordinaire sur un « réseau de zombies », c'est-à-dire un réseau d'ordinateurs infectés par des maliciels, pour attaquer de façon coordonnée une cible bien précise.

La plupart des réseaux de zombies font l'objet de création à l'aide d'un maliciel spécialement conçu, que l'on propage au plus grand nombre d'ordinateurs possible par l'intermédiaire de fichiers joints, scripts Web et autres outils malveillants. Tout ordinateur qui exécute le maliciel par inadvertance s'intègre au réseau de zombies et devient relié au serveur de commande et de contrôle de ce réseau, en attente de nouvelles instructions.

Comme le maliciel ne s'active qu'au signal du serveur de commande et de contrôle, la plupart des gens ignorent que leur ordinateur fait partie d'un réseau de zombies et que celui-ci le mettra à profit à tout moment à des fins malicieuses. Selon les estimations du Federal Bureau of Investigation des États-Unis, quelque 500 millions d'ordinateurs dans le monde sont infectés chaque année, et 18 nouveaux zombies naissent chaque seconde[8].

**500 millions d'ordinateurs dans le monde se font infecter chaque année, et 18 nouveaux zombies naissent chaque seconde[8].**

---

[4] Incapsula. *Denial of Service Attacks*. Extrait de https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html.

[5] Akamai. *Q4 2015 State of the Internet - Security Report.* Extrait de https://content.akamai.com/PG5795-Q4-2015-SOTI-Security-LandingPage.html.

[6] Akamai. *Q4 2015 State of the Internet - Security Report.* Extrait de https://content.akamai.com/PG5795-Q4-2015-SOTI-Security-LandingPage.html.

[7] Ponemon Institute. *2015 Cost of Cyber Crime Study: Global*. Extrait de http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf.

[8] Federal Bureau of Investigation. (2014). *Taking Down Botnets*. Extrait de https://www.fbi.gov/news/testimony/taking-down-botnets.

## Aucune expérience nécessaire

Les attaques DDoS sont en plein essor, notamment parce que les outils requis pour les lancer sont devenus plus accessibles et moins dispendieux que jamais auparavant. Tout comme n'importe qui peut maintenant acheter un logiciel-service ou une infrastructure-service, il en va de même pour les attaques DDoS. Il s'ensuit que des personnes qui n'auraient d'habitude aucune idée de la façon de créer ou de distribuer le maliciel nécessaire pour assembler un réseau de zombies peuvent maintenant se procurer aisément ce dont ils ont besoin, ou engager les services de quelqu'un d'autre qui le fera pour eux.

Plusieurs services de DDoS pour compte d'autrui (également connus sous les noms de « stresseur » et de « botteur ») ont vu le jour depuis quelques années. Ces services permettent à des cybercriminels potentiels de louer des infrastructures de réseau de zombies existantes ou même de payer quelqu'un pour lancer une attaque de bout en bout en leur nom à l'endroit d'une cible de leur choix.

Les coûts associés au « DDoS-service » sont étonnamment bas. Par exemple, un groupe de piratage offre huit différents forfaits d'abonnement au DDoS, dont le plus abordable commence à seulement 6 $ par mois. Cette option fournit l'accès à un réseau de zombies qui peut mettre un site Web en panne durant 100 secondes. Ceux qui paient 130 $ par mois peuvent mettre un site Web hors ligne durant plus de huit heures[9]. Et lorsque les abonnés paient ces services par voie de systèmes de paiement substitutifs comme Bitcoin, il devient extrêmement difficile de retracer une attaque particulière et de l'imputer à une personne quelconque[10].

**Ceux qui paient 130$ par mois peuvent mettre un site Web hors ligne durant plus de huit heures[9].**

Compte tenu de la faiblesse des obstacles, toute personne munie d'une carte de crédit et d'un motif quelconque peut rapidement et facilement amorcer une attaque DDoS. Prenez par exemple le cas de cet adolescent de 17 ans dans l'Idaho qui a payé un fournisseur externe de services de DDoS afin de lancer de multiples attaques à l'endroit du plus grand district scolaire de l'État. L'attaque a interrompu la connectivité Internet à l'échelle de 52 écoles pendant plus d'une semaine, causant la perte de résultats d'examens, rendant des cours et documents en ligne inaccessibles, et portant atteinte aux systèmes d'administration et de paie[11].

## Quel est le motif?

Étant donnée la facilité de lancer des attaques DDoS à faible coût avec très peu de préparation, il est devenu clair que toute organisation court le risque de subir une attaque à tout moment. Mais qu'est-ce qui peut motiver l'auteur d'une attaque? Voici quelques-unes des raisons[12, 13] :

### Cyberactivisme

Le DDoS sert souvent de forme de protestation contre les gouvernements et les sociétés dont les actions sont considérées comme « incorrectes » ou « mauvaises » par l'attaquant. Le cyberactivisme peut s'étendre du politique et de l'éthique (p. ex. : des attaques par des groupes comme Anonymous contre des organisations telles que l'État islamique et le FBI) au personnel et au mesquin (p. ex. : des serveurs de jeux informatiques en ligne mis en panne par des joueurs irrités au sujet de changements récents apportés au jeu).

### Vandalisme

Parfois des attaquants mettent un site Web en panne simplement pour prouver qu'il est possible de le faire, ou pour nulle autre raison que de « se faire remarquer » par une communauté d'utilisateurs en ligne. On attribue ces types d'attaques à ce qu'il est convenu d'appeler des « pirates adolescents », en raison de la puérilité des motifs; ils le font purement et simplement pour sentir une montée d'adrénaline ou attirer l'attention de leurs pairs.

---

[9] PCMag. (2014). *Lizard Squad Offers $6 DDoS Attack Tool.* Extrait de https://www.pcmag.com/article2/0,2817,2474386,00.asp.

[10] National Crime Agency. (2015). *Operation Vivarium Targets Users of Lizard Squad's Website Attack Tool.* Extrait de https://www.nationalcrimeagency.gov.uk/news/691-operation-vivarium-targets-users-of-lizard-squad-s-website-attack-tool.

[11] KTVB. (2015). *Student Accused of Cyber Attack on West Ada District.* Extrait de http://www.ktvb.com/news/crime/student-accused-of-cyber-attack-on-west-ada-district/175763447.

[12] Incapsula. *Denial of Service Attacks.* Extrait de https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html.

[13] Brain Stuff. (2014). *Why Do People Perform DDoS Attacks?* Extrait de http://www.brainstuffshow.com/blogs/why-do-people-perform-ddos-attacks.html.

### Concurrence

Si le site Web d'une entreprise donnée tombe en panne, c'est une bonne nouvelle pour ses concurrents. L'entreprise touchée perdra non seulement des ventes, mais sa réputation en prendra également un coup… et ses clients pourront affluer vers la concurrence à la place. Ces types d'attaques semblent monnaie courante dans des secteurs hautement concurrentiels comme les jeux de hasard en ligne.

### Extorsion

Sachant à quel point une attaque DDoS peut endommager une entreprise, le cybercriminel peut se servir de la simple menace d'une attaque pour extorquer de l'argent à une victime. À moins qu'on paie la rançon, l'attaque ira de l'avant tel que l'attaquant l'avait planifiée (ou si elle est déjà en cours, il ne l'arrêtera pas tant qu'il n'a pas reçu l'argent).

### Diversion

Le DDoS peut également servir de « rideau de fumée » pour dissimuler la véritable cible d'une cyberattaque. Pendant que les équipes de TI s'activent à régler une panne de site Web ou de serveur qui les a détournées de leur attention sur leur vrai travail, il devient plus facile de s'infiltrer furtivement dans le réseau interne de l'entreprise pour lui voler des données financières ou sur ses clients.

## De simple à perfectionné

Les attaques DDoS ne deviennent pas seulement plus répandues et plus accessibles. Elles sont aussi en train de devenir plus complexes, de sorte que les professionnels de la sécurité informatique ont de plus en plus de difficulté à les détecter, à les prévenir et à les repousser.

Tandis que les attaques DDoS traditionnelles reposaient sur un seul vecteur d'attaque, les attaques multivectorielles qui utilisent une combinaison d'attaques massives, lentes de faible intensité, de la couche réseau et contre la couche application deviennent rapidement la norme.

**56%** **de toutes les attaques DDoS qui ont eu lieu au cours du quatrième trimestre de 2015 ont utilisé plusieurs vecteurs d'attaque à la fois[14].**

L'approche multivectorielle donne aux attaquants une plus grande chance de succès. En effet, ils peuvent cibler différentes ressources simultanément ou même utiliser un type d'attaque en guise de leurre pour en dissimuler un autre. Lorsque les professionnels de la sécurité informatique ne savent pas d'où les attaques proviendront ni ce qu'elles cibleront, la prévision, la gestion et l'atténuation des attaques deviennent beaucoup plus difficiles.

Qui plus est, les attaquants rehaussent davantage leur probabilité de succès en changeant leur méthode de lancement des attaques DDoS. Plutôt que de centrer leurs efforts sur les attaques de grande envergure traditionnelles qui se déroulent de manière persistante sur une très longue période de temps, certains cybercriminels se tournent maintenant vers des attaques de type « rafales » ou « raids éclair ». Ces attaques produisent d'énormes volumes de trafic pendant une courte période, durent juste assez longtemps pour mettre un serveur ou un site Web en panne (entre 20 minutes et une heure), puis se répètent plusieurs fois pendant des jours, voire des semaines.

Ce genre d'attaque a été mis au point dans le but précis de contrer les mesures de sécurité de TI traditionnelles ciblant les attaques persistantes et prolongées. Au moment où les systèmes et protocoles anti-DDoS sont déclenchés manuellement, l'attaque en rafale ou le raid éclair a déjà fait toute son œuvre en gaspillant du temps et des ressources de TI tout en perturbant l'ensemble de l'organisation[15].

[14] Akamai. *Q4 2015 State of the Internet – Security Report*. Extrait de https://content.akamai.com/PG5795-Q4-2015-SOTI-Security-LandingPage.html.
[15] Incapsula. (2013). *Hit and Run DDoS Attack.* Extrait de https://www.incapsula.com/blog/hit-and-run-ddos-attack.html.

# Comment une attaque DDoS nuit à vos activités commerciales

## Un effet immédiat sur votre rentabilité

Le but ultime d'une attaque DDoS consiste à porter préjudice à l'expérience client d'une organisation:

- En mettant son site Web complètement hors ligne de sorte qu'aucun trafic légitime ne peut y accéder.
- En rendant son serveur si lent et léthargique que même si les clients peuvent accéder au site, ils ne peuvent rien y accomplir.

Toute entreprise de commerce électronique dont le site Web se paralyse jusqu'à la panne totale subira des conséquences immédiates sous la forme de ventes perdues. Pensez au cas d'Amazon en août 2013 : lorsque son site Web est tombé en panne seulement 40 minutes, l'entreprise a perdu environ 5 millions $ en ventes[16].

Même les organisations qui ne vendent aucun produit en ligne peuvent encaisser d'énormes contrecoups si leur site Web est une source cruciale de renseignements ou de services. Lorsque le réseau ou les serveurs sont sous le coup d'une attaque, les clients ne peuvent plus obtenir le soutien dont ils ont besoin. Cela peut engendrer un déluge d'appels ou de messages de courriel reçus, et ainsi surcharger et bloquer les lignes de communication, qui pourraient autrement servir à des fins plus productives.

## Le coût élevé des mesures correctives

Selon la nature et le moment de l'attaque, remettre sur pied et en fonctionnement un site Web ou un serveur tombé en panne pourrait nécessiter des heures, voire des jours de travail. Dans le cadre d'un sondage Forrester Research mené auprès de décideurs canadiens contribuant directement aux systèmes de contact client, 35 % d'entre eux ont précisé qu'il en coûterait entre 10 000 $ et 100 000 $ pour régler une attaque DDoS. Une autre tranche de 25 % d'entre eux ont indiqué qu'il en coûterait entre 100 000 $ et 1 million $[17]. Mais ceci n'est qu'une goutte d'eau dans l'océan en comparaison de ce que Sony a dû absorber en 2011 : lorsque son réseau PlayStation a encaissé une série d'attaques DDoS et de violations de confidentialité de données, on a rapporté que le géant de l'électronique a dépensé plus de 250 millions $ en deux ans pour corriger et régler les répercussions immédiates des attaques et des violations et renforcer ses défenses[18].

Selon la nature et le moment de l'attaque, remettre sur pied et en fonctionnement un site Web ou un serveur tombé en panne pourrait nécessiter des heures, voire des jours de travail.

**Certaines estimations évaluent qu'il faut jusqu'à 90 jours pour se remettre complètement d'une attaque DDoS moyenne[18].**

---

[16] VentureBeat. (2013). *Amazon Website Goes Down for 40 Minutes, Costing the Company $5 Million.* Extrait de https://venturebeat.com/2013/08/19/amazon-website-down/#YrOqv7cqKgylGzWm.99.

[17] Ponemon Institute. *2015 Cost of Cyber Crime Study: Global.* Extrait de http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf

[18] Ponemon Institute. *2015 Cost of Cyber Crime Study: Global.* Extrait de http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf

Dans le cadre d'un sondage Forrester Research mené auprès de décideurs canadiens contribuant directement aux systèmes de contact client, 35 % d'entre eux ont précisé qu'il en coûterait entre 10 000 $ et 100 000 $ pour régler une attaque DDoS. Une autre tranche de 25 % d'entre eux ont indiqué qu'il en coûterait entre 100 000 $ et 1 million $[19]. Mais ceci n'est qu'une goutte d'eau dans l'océan en comparaison de ce que Sony a dû absorber en 2011 : lorsque son réseau PlayStation a encaissé une série d'attaques DDoS et de violations de confidentialité de données, on a rapporté que le géant de l'électronique a dépensé plus de 250 millions $ en deux ans pour corriger et régler les répercussions immédiates des attaques et des violations et renforcer ses défenses[20].

## Une atteinte directe à votre réputation

Les chiffres indiqués ci-dessus ne tiennent pas compte des coûts associés aux dommages éventuels à la réputation de l'entreprise, ou encore à la fidélisation ou à l'acquisition de clients. Si votre site Web est votre produit, ou si le rendement de votre produit dépend de la disponibilité de votre serveur, vos clients pourraient n'avoir aucun accès à des services pour lesquels ils ont déjà payé. Cela peut susciter de la colère et de la frustration, ce qui pourrait avoir un effet négatif sur votre image de marque. Les clients qui ont vécu une mauvaise expérience risquent fort de répandre la nouvelle, surtout dans les médias sociaux. Ainsi, même une fois l'attaque DDoS résolue, l'effet produit sur votre réputation peut nuire à vos ventes des semaines, voire des mois durant.

Dans le cadre du sondage Forrester Research auprès de décideurs en matière de TI susmentionné, les entreprises canadiennes ont classé les incidences indirectes de la perte de leur site Web durant une heure ou plus comme suit[21] :


**67%**

des répondants affirment que la satisfaction de la clientèle en souffre

**56%**

des répondants pensent que cela influe de façon déterminante sur la marque

**52%**

des répondants affirment que l'acquistion de clients est compromise

**55%**

des répondants sont préoccupés par les effets négatifs sur la fidélisation de la clientèle

## Chaque secteur est en danger

Aucun secteur n'est immunisé contre la possibilité d'une attaque DDoS. Toutefois, certains types d'organisation sont plus susceptibles d'être ciblés, comme les ministères, les entreprises de jeux ludiques et de jeux de hasard en ligne, et les fournisseurs de services Internet. Le secteur des jeux en ligne, frappé particulièrement durement au cours du 4e trimestre de 2015, a compté pour 54 % de toutes les attaques DDoS pendant cette période. Si on examine précisément les attaques contre la couche application, le secteur de la vente au détail demeure la cible la plus fréquente, visé par 59 % de toutes les attaques de ce type durant ce même trimestre[22].

---

[19] 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.

[20] Fortune. (2014). *Why Sony Didn't Learn from Its 2011 Hack*. Extrait de http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack.

[21] 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.

[22] Akamai. *Q4 2015 State of the Internet - Security Report*. Extrait de https://content.akamai.com/PG5795-Q4-2015-SOTI-Security-LandingPage.

Toutefois, de nombreux autres types d'organisation s'exposent à d'importants risques, notamment dans les secteurs de la finance, de l'éducation, des soins de santé, de l'énergie, des services publics et des services juridiques. En fait, 2015 a connu une telle augmentation du nombre d'attaques contre des écoles et d'autres sites Web relatifs à l'enseignement que cela a incité Radware à changer le classement du niveau de risque de ces organisations de moyen à élevé[23].

Bien que les attaques DDoS fassent les manchettes seulement lorsqu'elles ciblent les gouvernements, les banques ou les sociétés multinationales, la réalité démontre que les organisations de toutes tailles sont visées. Dans le secteur financier, par exemple, des caisses d'économie et des maisons de courtage de petite taille ont été également la cible d'attaques DDoS[24].

# Conclusion

Même si elles sont en danger, de nombreuses organisations pensent qu'elles n'ont pas la taille ou la présence en ligne suffisante pour être la cible d'une attaque. Par conséquent, elles sont moins susceptibles d'investir dans une protection avancée contre les attaques DDoS, ce qui les rend vulnérables aux yeux d'éventuels cybercriminels. Surtout dans le cas d'organisations de plus petite taille ou moins visibles en ligne, même une seule panne prolongée peut entraîner une perte irréversible de ventes ou de confiance des clients.

L'une des clés de la protection de votre organisation consiste à pouvoir reconnaître une attaque DDoS avant qu'elle n'intervienne. Mais même si une pointe soudaine de l'utilisation de la bande passante constitue généralement le premier signe avertisseur d'une attaque DDoS, ce n'est pas toutes les organisations qui sont en mesure de détecter de tels changements en temps réel.

**Dans un sondage auprès de professionnels des TI, 21 pour cent des répondants ont indiqué que les plaintes des clients constituaient le principal indicateur d'une attaque, et près de la moitié des répondants ont admis qu'ils ne pouvaient réagir que de manière réactive à une attaque : leurs efforts pour reconnaître et bloquer une attaque n'ont lieu que bien après que les dommages ont été subis[25].**

Ces chiffres soulignent l'importance d'utiliser un service de sécurité des TI proactif et toujours en garde. De nombreux services de ce type existent, y compris des solutions sur place, des solutions en nuage, et des combinaisons des deux. Et la bonne nouvelle, c'est qu'il n'est pas nécessaire d'être une organisation d'envergure mondiale dotée d'une équipe TI gigantesque pour mettre ces solutions en place. Par exemple, notre service Sécurité du réseau contre les attaques DDoS Bell, un service abordable entièrement géré, détecte, atténue et filtre automatiquement les attaques DDoS avant qu'elles atteignent le réseau de votre entreprise, et empêche ainsi le trafic malveillant d'interrompre votre exploitation.

Visitez notre site Web pour obtenir de plus amples renseignements sur le service Sécurité du réseau contre les attaques DDoS Bell. Pour en savoir plus sur la manière dont Bell peut protéger votre organisation contre toutes sortes de cyberattaques, veuillez communiquer avec votre conseiller de Bell. Nous vous aiderons à trouver la solution de sécurité la mieux adaptée à vos besoins commerciaux.

---

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

[24] Credit Union Times. (2014). *DDoS Takes Aim at Vulnerable Credit Unions*. Extrait de http://www.cutimes.com/2014/10/03/ddos-takes-aim-at-vulnerable-credit-unions?page=1.

[25] Corero Network Security. (2015). *Corero Network Security Finds Degradation of Customer Confidence and Lost Revenues are the Most Damaging Ramifications of DDoS Attacks*. Extrait de https://www.corero.com/company/newsroom/press-releases/corero-network-security-survey-finds-degradation-of-customer-confidence-and-lost-revenues-are-the-most-damaging-ramifications-of-ddos-attacks-/.

# À propos de Bell

Les entreprises qui exigent une infrastructure de TI fiable et hautement sécurisée choisissent Bell. Bell fait partie intégrante de l'infrastructure névralgique du Canada, et elle offre une expertise d'avant-garde en matière de détection, d'atténuation et de prévention des menaces.

À titre de propriétaire et exploitant du plus important réseau de voix et de données au pays, Bell voit très bien les menaces qui peuvent peser sur votre entreprise. Nous pouvons agréger d'énormes quantités de données et établir des corrélations entre différentes structures de trafic pour détecter le trafic malveillant de manière proactive et l'atténuer, et réduire les délais d'intervention lorsque surviennent des incidents. De plus, avec une équipe de plus de 300 professionnels de la sécurité détenant des certifications de sécurité avancées comme CIPPIC, CISA, CISM, CISSP et OSSTMM, nous avons l'expérience et l'information nécessaires pour vous aider à planifier, à concevoir, à réaliser et à gérer la solution de sécurité complète qui convient à votre entreprise.