PROTÉGEZ VOTRE ENTREPRISE CONTRE LES ATTAQUES DDOS

Janvier 2016

- Tendances et menaces actuelles
- Méthodes et motivations
- Impact, coût et danger caché
- Atténuation des attaques

Livre blanc

cogeco PEER 1

TABLE DES MATIÈRES

1. Synthèse

Les attaques par déni de service distribué (DDoS) font partie des plus anciennes menaces existant dans le domaine de la sécurité informatique. Elles peuvent être utilisées pour perturber des services commerciaux connectés à Internet et provoquer la panique d'une entreprise et de son personnel de sécurité informatique.

Même si elles puisent leurs racines dans le passé, les attaques DDoS continuent de faire des ravages de nos jours, ce qui accentue la nécessité de mettre en place une solution spécifique d'atténuation de l'impact des attaques afin de lutter plus que jamais auparavant contre cette menace.

Comme leur nom le suggère, les attaques par déni de service (DoS) sont conçues pour refuser aux utilisateurs légitimes l'accès à des sites Web et des services en les surchargeant de connexions, requêtes et trafics illégitimes. Une attaque par déni de service distribué (DDoS) survient lorsque des attaques DoS sont lancées par des entités multiples essayant d'attaquer simultanément une même source, que ce soit des pirates en chair et en os ou une seule entité utilisant son réseau de bots. Alors que les technologies actuelles permettent d'atténuer la plupart des attaques DoS isolées, elles ne peuvent pas faire grand-chose contre une attaque DDoS à grande échelle si des mesures adéquates d'atténuation des attaques n'ont pas été mises en place depuis le début.

Les attaques DDoS sont difficiles à tracer et à empêcher, faciles à exécuter, et disponibles à des coûts de plus en plus abordables. Cela explique pourquoi elles représentent une des méthodes d'attaque les plus utilisées par les extorqueurs, les activistes politiques (hacktivistes) et les groupes/individus mécontents.

Contrairement aux vecteurs d'attaques plus traditionnels, qui tentent de s'infiltrer dans des réseaux sans être détectés, les attaques DDoS sont beaucoup plus subtiles ou sournoises : leur principal objectif est de perturber sensiblement un système.

Ce livre blanc de Cogeco Peer 1 s'intéresse tout d'abord au paysage actuel des menaces DDoS et aux différentes tendances de lutte contre les DDoS émergeant dans le secteur de la sécurité. Il se penche ensuite sur les différents types d'attaques DDoS constatés aujourd'hui, et les raisons qui motivent ces actes.

Finalement, ce livre blanc examine également l'impact des attaques DDoS sur les entreprises et les coûts afférents, ainsi que le danger potentiel caché pouvant survenir lors de telles attaques. En guise de conclusion, ce document esquisse une stratégie en sept points pour mettre en place une meilleure défense organisationnelle contre les DDoS.

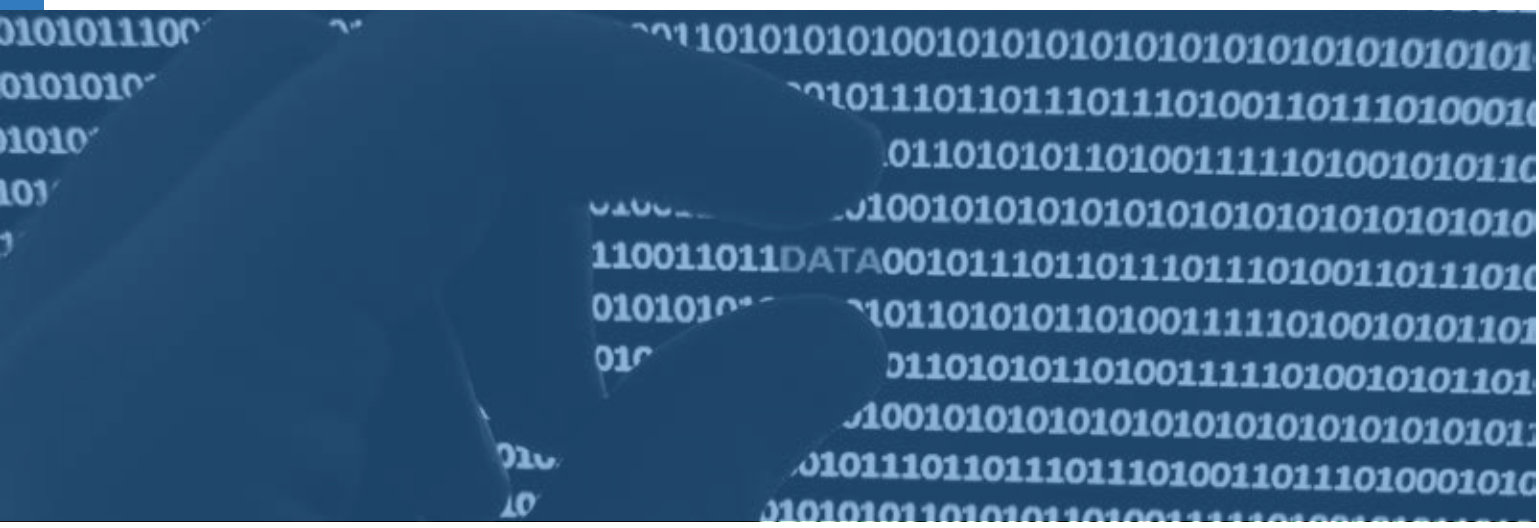
2. DDoS : dernières tendances et paysage actuel des menaces

Selon le rapport d'Akamai intitulé *État des lieux de l'Internet au 2e trimestre 2015 - Rapport sur la sécurité (State of the Internet - Q2 2015 Security Report*), le nombre d'attaques DDoS enregistré au deuxième trimestre 2015 a atteint un niveau record. En effet, le nombre d'attaques DDoS a augmenté de 7 % par rapport au 1er trimestre 2015, ce qui est assez préoccupant. Plus inquiétant encore, le nombre d'attaques DDoS au 2e trimestre 2015 a vertigineusement augmenté de 132 % en termes interannuels.

Pire encore, le rapport d'Akamai répertorie 12 attaques ayant enregistré des pics à plus de 100 gigabits par seconde (Gbps) et 5 attaques à plus de 50 millions de paquets par seconde (Mpps) comme des « méga-attaques ». Ces gigantesques menaces, dont une a atteint les 240 Gbps et a duré plus de 13 heures, sont précisément le type d'attaque qui ferait s'écrouler la majorité des réseaux sous sa pression.

Malgré l'augmentation de la fréquence et de la magnitude des attaques DDoS, un facteur est constamment resté le même : l'origine de la majorité des attaques. Selon le rapport d'Incapsula sur le paysage mondial des menaces DDoS au 3e trimestre 2015 *(Global DDoS Threat Landscape Q3 2015)*, la Chine comptait pour 37,5 % de la totalité des attaques dans le monde, ce qui en fait la principale source du trafic de DDoS. En effet, Incapsula a révélé que le trafic DDoS provenant de Chine avait en fait augmenté de 152 % par rapport au trimestre précédent.

Le rapport d'Incapsula souligne également que les États-Unis étaient la principale cible des attaques DDoS dans le monde, 45,8 % du trafic DDoS ciblant des sites Web hébergés aux États-Unis.



L'aspect le plus inquiétant des attaques DDoS est peut-être qu'elles peuvent toucher n'importe quel type d'entreprise, quel que soit son secteur d'activité. Par exemple, le secteur des jeux en ligne a été très sévèrement touché au 2e trimestre 2015 : selon le rapport d'Akamai, il a été visé par 35 % des attaques DDoS. Toutefois, tout cela n'est pas nouveau. En effet, les jeux en ligne représentent le secteur le plus visé depuis le 2e trimestre 2014.

En résumé, si vous fournissez des services de jeux en ligne pour les propriétaires de Xbox et PlayStation, la menace posée par les attaques DDoS est très réelle et très grave, tout comme leur impact potentiel.

Les secteurs des logiciels et de la technologie (27,74 %), d'Internet et des télécommunications (12,9 %), des médias et des divertissements (9,41 %) et des services financiers (8,19 %) viennent compléter le tableau des cinq secteurs les plus visés par les attaques DDoS au 2e trimestre 2015, certaines des attaques de très grande envergure ayant entraîné des fuites substantielles de données dans ces secteurs.

Une des nouvelles tendances des attaques DDoS qui se développe très rapidement est celle du « botnet à louer » (botnet-for-hire). Ces services de DDoS à louer étant largement disponibles, même des individus et des groupes lambdas pourraient exécuter – ou plutôt faire exécuter pour eux — des attaques DDoS à grande échelle, parfois pour à peine 5 dollars par tentative.

Ces services à louer sont à la base de l'augmentation récente du nombre d'attaques multi-vectorielles. De nos jours, les attaquants DDoS ont accès à plus d'outils, à des dispositifs vulnérables et à un cadre rémunérateur, ce qui permet de faire des DDoS à louer une activité lucrative.

Alors que le concept de tirer parti de botnets personnalisés pour mener des attaques DDoS angoissera inévitablement les directeurs de la sécurité informatique, ces attaques sont généralement plus courtes et plus rudimentaires. Néanmoins, ces attaques continuent de représenter une menace significative pour les réseaux sous-protégés lorsque l'on sait que certains services de DDoS à louer prometteur des volumes d'attaque de plus de 200 Gbps.

Dans son rapport sur les DDoS au 3e trimestre 2015 *(DDoS Intelligence Report Q3 2015)*, Kaspersky Lab accorde une attention particulière à l'augmentation des attaques visant les institutions financières au cours de la période concernée par le rapport. Des organisations bancaires importantes ont été visées dans plusieurs pays, les hackers menaçant de mettre leurs services hors ligne si elles ne payaient pas la rançon demandée.

Kaspersky n'est pas le seul à avoir remarqué cette augmentation des attaques visant les institutions financières. Une étude de cas séparée publiée en septembre 2015 par Akamai a également mis en exergue l'essor d'une stratégie d'attaque menée par un groupe connu sous le nom DDoS-for-Bitcoin (DD4BC), qui veut soutirer des bitcoins aux organisations financières.

L'étude de cas d'Akamai sur le groupe DD4BC intitulée *Case Study: Summary of Operation DD4BC*, qui vient compléter le principal rapport

De nos jours, les attaquants DDoS ont accès à plus d'outils, à des dispositifs vulnérables et à un cadre rémunérateur, ce qui permet de faire des DDoS à louer une activité lucrative.

sur l'état des lieux de l'Internet d'Akamai, révèle que les entreprises travaillant dans le secteur des services financiers américains et canadiens sont de plus en plus visées par le groupe extorqueur de bitcoins.

Depuis avril, Akamai estime que DD4BC a, à lui seul, lancé 114 attaques, la plupart ciblant initialement des organisations en Amérique du Nord et en Asie. Cependant, des entreprises en Corée, en Chine, en Australie et en Nouvelle-Zélande sont désormais également visées, ce qui montre avec quelle rapidité les attaquants peuvent changer de cible.

Le rapport de Kaspersky Lab souligne également ce qu'il nomme un « scénario d'attaque DDoS inhabituel », lors duquel le site d'un des clients de CloudFlare a été victime d'une attaque dont la puissance globale a atteint 275 000 requêtes HTTP par seconde. Le rapport indique qu'un iFrame contenant une publicité malveillante a été lancé dans les navigateurs de nombreux utilisateurs et suite à cela, les postes de travail des utilisateurs ont commencé à envoyer des requêtes XHR à la victime.

La situation à propos des DDoS est devenue tellement grave, avec des attaques désormais plus puissantes et fréquentes que jamais, que le Pentagone a récemment annoncé des projets de financement d'outils et de chercheurs afin d'essayer d'aider les entreprises et organisations à se défendre contre les risques continuellement plus élevés d'attaques DDoS.

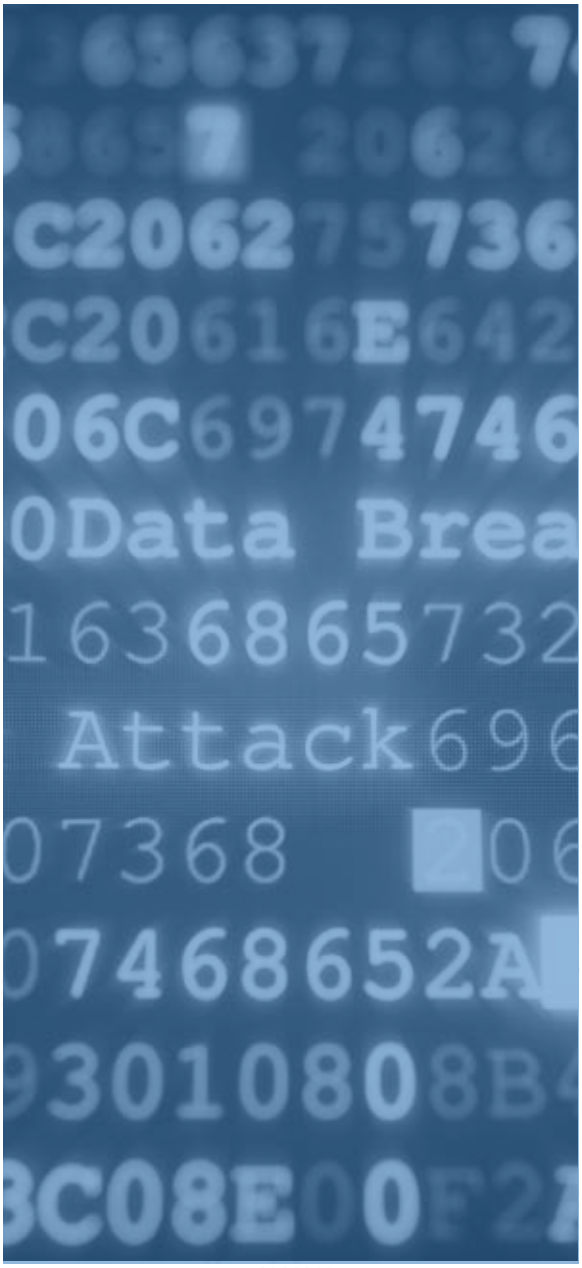
Connue sous le nom de XD3 (Extreme DDoS Defense), l'initiative du Pentagone chargera des chercheurs financés par l'armée de créer de nouveaux outils qui permettront aux organisations touchées de se remettre d'attaques DDoS en 10 secondes.

Le lancement provisoire de ce projet de trois ans est programmé au 1er avril 2016 et les chercheurs seront choisis par la DARPA (Defense Advanced Research Projects Agency).

Le programme XD3 suivra une approche en trois volets : disperser les biens informatiques hautement consolidés, qui présentent une large cible pour les attaquants, modifier le comportement prévisible de nombreux services en ligne afin de duper les hackers, et concevoir des techniques d'atténuation adaptables au niveau des points d'extrémité.

Le fait que la DARPA mène proactivement la lutte contre les hackers apportera du réconfort à de nombreuses entreprises, mais la menace reste imminente et omniprésente, raison pour laquelle les entreprises doivent dans un premier temps mettre en place leurs systèmes de défense contre les attaques DDoS.

Les acteurs malveillants modifient souvent les règles du jeu DDoS en changeant fréquemment de tactiques, en cherchant continuellement de nouvelles vulnérabilités et même en recourant à de vieilles techniques alors considérées comme obsolètes.



3. DDoS : méthodes et motivations

Types d'attaques DDoS

Même si elles font partie des plus anciennes menaces existant sur Internet – elles ont littéralement plusieurs dizaines d'années –, les attaques DDoS ne sont pas simplement occasionnelles, elles sont abondantes. Elles sont massivement utilisées principalement parce qu'elles sont faciles à exécuter, difficiles à empêcher et à tracer, et peu coûteuses, ce qui en fait une stratégie d'attaque à faible risque et à impact élevé.

Le problème, pour les entreprises d'aujourd'hui, est que ces attaques DDoS ont évolué au fil du temps et se sont diversifiées. Par conséquent, il est de plus en plus difficile de se préparer à ces attaques et de les atténuer.

D'une façon générale, on peut classer les attaques DDoS en deux catégories :

- **Avec connexion : requiert une « poignée de main » mutuelle entre un serveur et un client utilisant des protocoles de connexions standards avant le lancement d'une attaque.**
- **Sans connexion : ne requiert pas une connexion/session officiellement établie avant le lancement d'une attaque.**

Contrairement aux attaques par déni de service (DoS) – lors desquelles un seul ordinateur et une seule connexion internet sont utilisés pour frapper une cible avec des paquets de données –, les attaques DDoS passent par l'utilisation de nombreux ordinateurs et de nombreuses connexions Internet, qui sont souvent distribués (d'où le nom déni de service *distribué*) sur un réseau mondial connu sous le nom de botnet (réseau de zombie).

Les attaques DDoS peuvent être sous-divisées en trois catégories principales, en fonction de la partie spécifique de l'infrastructure réseau visée :

Attaques volumétriques

Les attaques volumétriques – aussi connues sous le nom de *Flood* (inondations) – sont généralement menées par le biais de botnets et sont sans connexion. L'objectif principal de ce type d'attaque est de saturer la bande passante de la cible et de provoquer une saturation du site, le rendant de la sorte inaccessible.

Des botnets sont généralement mis à contribution pour générer des volumes de trafic énormes, et la nature des attaques volumétriques (sorte de « ruée en groupe ») les rend très difficiles à atténuer en comparaison avec les attaques provenant d'une source unique.

Il existe de nombreuses sortes d'attaques volumétriques, mais les attaques UDP (User Datagram Protocol) et ICMP (Internet Control Message Protocol) (qui consistent à envoyer de nombreuses requêtes ping) sont les deux plus courantes. Leur magnitude se mesure en bits par seconde (Bps) ou en gigabits par seconde (Gbps).

Selon la 10e étude annuelle d'Arbor Network sur la sécurité des infrastructures IP mondiales (WISR), publiée début 2015, les attaques volumétriques ont représenté 65 % des attaques DDoS signalées en 2014.

Attaques de type « state-exhaustion »

Les attaques de type « state-exhaustion », également appelées attaques par épuisement des tables d'état visent des pare-feu, des serveurs Web et/ou des répartiteurs de charge dans le but spécifique d'épuiser leurs ressources disponibles.

Même des dispositifs haute capacité conçus pour maintenir des millions de connexions simultanées peuvent être renversés par ce type d'attaque.

Une des attaques par épuisement des tables d'état les plus communes, et peut-être même la plus connue, est l'attaque Ping de la mort (Ping of Death). Lors de cette technique, un attaquant défragmente et envoie un paquet de 65 536 bits à une cible aussi vite que possible.

Lorsque le serveur cible réunit les fragments IP pour recomposer le paquet, cela provoque généralement un dépassement de tampon. Cela entraîne le crash de la cible et un déni de service des paquets légitimes.

Les attaques de type « state-exhaustion » sont mesurées en paquets par seconde et selon l'étude WISR d'Arbor Network, elles ont représenté 20 % des attaques DDoS signalées en 2014.

Attaques applicatives

Les attaques applicatives, aussi connues sous le nom d'attaques de la couche 7, ciblent des faiblesses spécifiques au niveau des applications ou des serveurs. Elles tentent d'abord d'établir une connexion avec la ressource ciblée et l'épuisent ensuite en monopolisant les processus et transactions.

Ces attaques comprennent généralement des requêtes qui semblent légitimes et innocentes. Elles peuvent être menées en utilisant un petit nombre de machines, ce qui les rend beaucoup plus difficiles à détecter. La magnitude des attaques applicatives se mesure généralement en requêtes par seconde.

Depuis toujours, les services HTTP et DNS ont été les principales cibles des attaques applicatives, mais les services HTTPS et SMTP sont des cibles de plus en plus populaires.

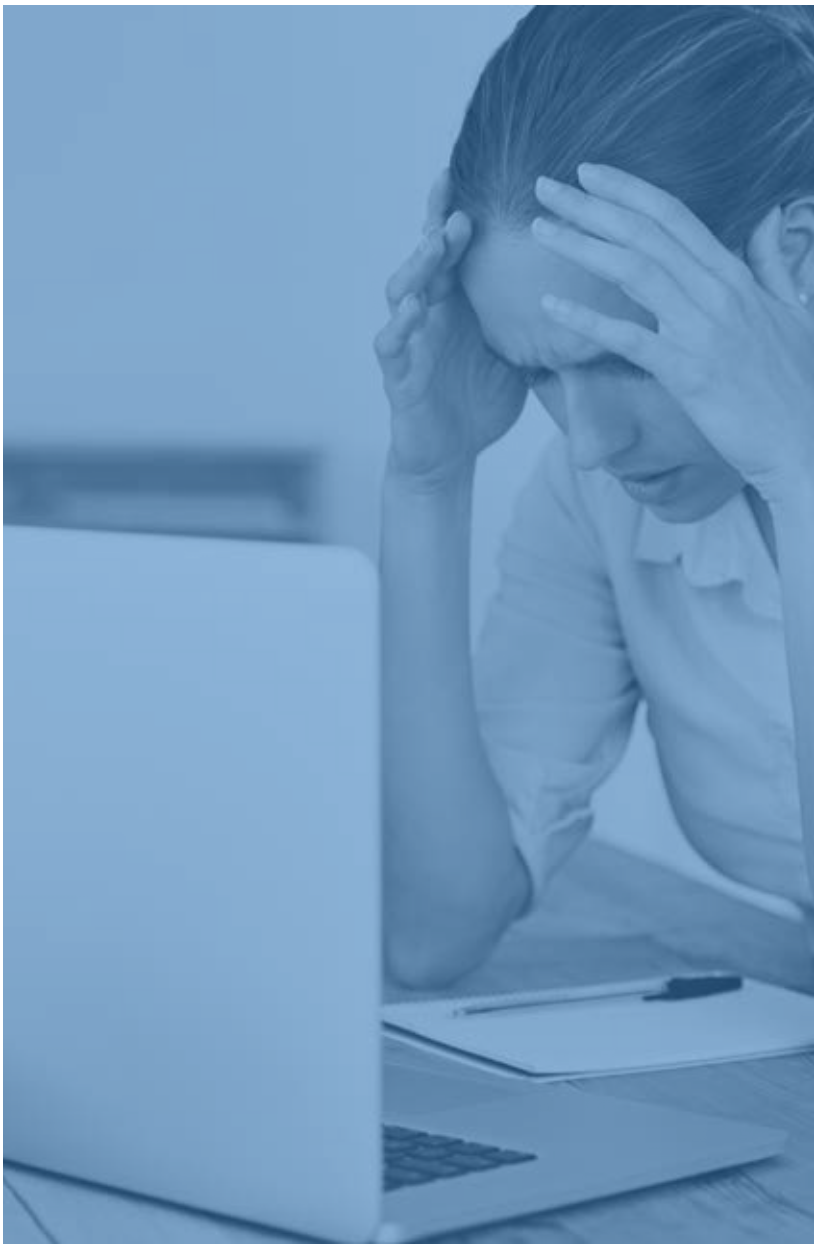
Selon l'étude WISR d'Arbor Network, les attaques applicatives ont représenté 17 % des attaques DDoS signalées en 2014.

Dans des cas extrêmes, les entreprises peuvent être touchées par une combinaison de ces trois types d'attaques, ce qui rend la défense contre les DDoS encore plus délicate.

Attaques DDoS zero-day

Bien qu'elles ne constituent pas un type d'attaque DDoS spécifique, les attaques DDoS zero-day méritent d'être mentionnées, car elles sont souvent citées dans le monde de la sécurité. Elles ont lieux lorsqu'un attaquant exploite une vulnérabilité zero-day, qui est inconnue du fournisseur et n'a pas été corrigée par un patch.

Le terme « zero-day » est bien connu de la communauté des hackers et fait référence au fait que le fournisseur a zéro jour pour corriger la faille (avant que celle-ci ne soit divulguée). Les exploits zero-day sont souvent échangés entre hackers. Par conséquent, une fois découverts, ils se propagent souvent rapidement, ce qui presse encore plus les fournisseurs à créer et à publier des patchs.



Le terme «zero-day» est bien connu de la communauté des hackers et fait référence au fait que le fournisseur a zéro jour pour corriger la faille (avant que celle-ci ne soit divulguée).

Motivations des attaques DDoS

Alors que tous les types d'entreprises et d'organisations peuvent être la cible d'une attaque DDoS – la conséquence la plus évidente d'une attaque réussie étant de rendre une ressource ou un service particulier indisponible ou inutilisable –, les motivations qui sous-tendent ces attaques varient inévitablement.

Extorsion et profit

La motivation la plus facile à comprendre est peut-être l'envie de tirer profit de l'organisation visée. Les pirates savent qu'ils peuvent souvent extorquer une organisation en la menaçant d'une attaque DDoS.

Les attaquants font généralement chanter leurs victimes par e-mails et prouvent parfois leurs intentions en lançant une attaque DDoS à petite échelle sur l'organisation visée. Les cibles privilégiées des tentatives d'extorsion sont les entreprises qui dépendent fortement de leur présence en ligne, comme celles actives dans les secteurs des jeux d'argent en ligne, du commerce électronique et des médias.

Cela peut paraître surprenant, mais souvent les pirates demandent une petite somme d'argent la première fois. Il y a des chances que l'entreprise paie pour éviter les conséquences d'une attaque DDoS, mais dans certains cas, les attaquants montent les enchères et demandent plus d'argent une fois le premier paiement effectué.

Les attaques DDoS motivées par l'envie de tirer profit d'une compagnie sont souvent planifiées pour provoquer un maximum de perturbation et pour frapper une entreprise lors d'un évènement particulier.
Par exemple, les sites de jeux de paris en ligne peuvent être ciblés en plein pendant un grand évènement sportif, ou les boutiques en ligne, pendant les périodes de fêtes.

Cela peut paraître surprenant, mais souvent les pirates demandent une petite somme d'argent la première fois.

Hacktivisme

Le hacktivisme devient de plus en plus populaire et les attaques DDoS sont souvent menées par des groupes qui veulent perturber des organisations et des individus dont ils désapprouvent les croyances politiques, sociales et/ou religieuses.

Les groupes tels que LulzSec et plus récemment Anonymous font régulièrement les gros titres lorsqu'ils menacent des organisations ou des mouvements avec des attaques DDoS. Leurs motivations ne sont pas financières : ils veulent attirer l'attention des médias pour parler de leur cause.

Les groupes de hacktivistes annoncent souvent leurs plans à l'avance afin d'attirer un maximum d'attention publique et médiatique sur l'évènement. La visibilité supplémentaire du groupe lui permet de confirmer ses capacités et de renforcer sa notoriété dans la communauté hacktiviste.

Un exemple probant de ce type de motivation est la cyberattaque lancée contre le site Mumsnet en 2015. Un groupe du nom de Dadsec a revendiqué l'attaque qui a mis le site hors ligne et a déclaré que l'attaque était motivée par les propos à l'encontre des pères tenus selon lui par le site Mumsnet.

Conflits

C'est un malheureux reflet de notre époque, mais de nos jours, les attaques DDoS sont bel et bien utilisées lors de conflits. Les joueurs en ligne en particulier utilisent souvent de courtes attaques DDoS pour perturber leurs adversaires. La cible est rendue dans l'incapacité de jouer ou du moins son service est gravement détérioré, ce qui limite son efficacité.

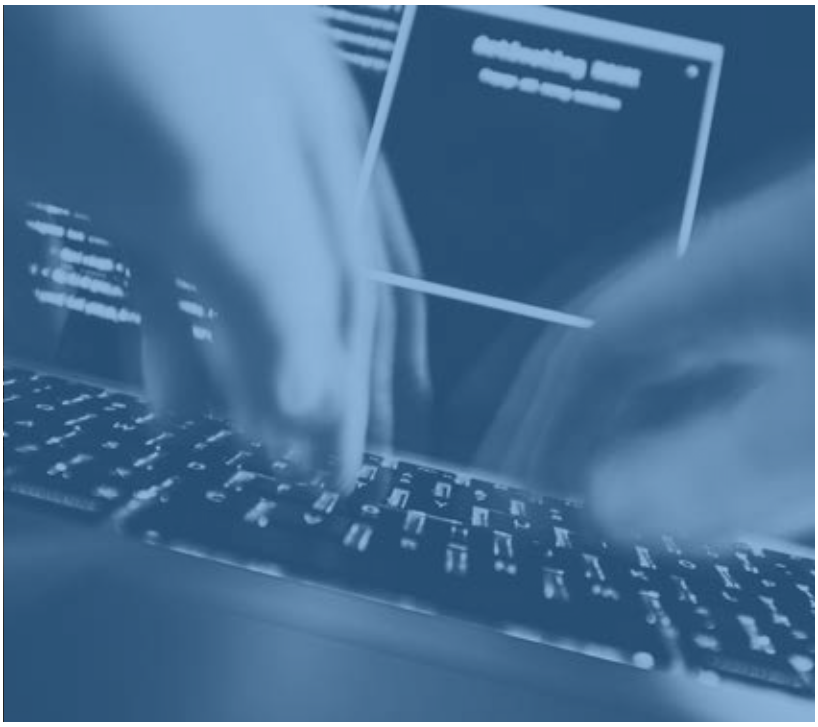
Cependant, les joueurs en ligne ne sont pas les seuls à tirer profit des attaques DDoS. Toute personne ayant de la rancune envers une autre pourrait lancer une attaque DDoS ou payer quelqu'un pour le faire. Par exemple, un client mécontent ou un ancien employé pourrait vouloir se venger d'une entreprise.

Malheureusement, l'essor des services de DDoS à louer donne désormais la possibilité à quiconque disposé à payer de lancer une attaque, et c'est pourquoi ces attaques sont devenues omniprésentes. Il serait tout aussi possible qu'une entreprise engage un hacker pour perturber les opérations en ligne de ses concurrents.

Interruptions involontaires

Même si dans un tel cas on ne peut pas vraiment parler d'une attaque DDoS, les inondations involontaires de trafic sur un site Web peuvent souvent avoir le même effet. Cela se passe parfois lorsqu'une petite entreprise ou organisation apparaît dans les journaux, et que les visiteurs viennent ensuite en masse sur son site Web.

Le site Web s'effondre sous l'afflux de trafic et, en termes d'impact, la pression anormale qu'il subit peut être comparée à une interruption due à une DDoS applicative. Même si personne n'est véritablement responsable du problème, ces types d'interruption soulignent la fragilité de certaines organisations lors d'afflux massifs soudains. Cela met encore plus l'accent sur le besoin d'une protection contre les DDoS.



4. DDoS : impact, coût et danger caché

Impact et coût

Toute interruption ou période d'indisponibilité informatique a un impact sur les résultats d'une entreprise, quelle qu'en soit l'explication. Cela étant dit, au vu de leurs répercussions très graves et de leur durée souvent significative, les attaques DDoS sont particulièrement préjudiciables aux entreprises.

Cependant, les entreprises doivent se préoccuper d'autres facteurs que les implications financières évidentes lorsqu'elles sont touchées par une attaque DDoS. En effet, d'autres répercussions significatives sont également à prendre en compte.

Perte de revenus

Les entreprises dont les revenus reposent uniquement sur leurs applications et services commerciaux connectés à Internet sont sans aucun doute celles qui ont le plus à perdre lors d'une attaque DDoS. Par exemple, si un détaillant travaillant dans l'e-commerce voit son site Web mis hors ligne pendant plusieurs heures, il subira alors une perte directe de revenus étant donné que les clients ne sauront tout simplement pas passer commande.

Tandis qu'il est souvent possible de chiffrer la perte engendrée par une période d'indisponibilité lors d'une journée « normale », l'impact d'une attaque DDoS lancée à un moment de l'année particulièrement chargé – tel que le premier jour des soldes ou les périodes de fêtes – peut être énorme et pratiquement incalculable.

Les clients exigent toujours un service sans faille de leurs détaillants favoris. Vu leurs attentes élevées, ils considèrent généralement comme inacceptable qu'un site Web soit indisponible, a fortiori lorsqu'ils essaient d'obtenir une offre particulière en ligne ou de faire leurs achats de Noël.

Il ressort du rapport sur le coût des attaques par déni de service *(The Cost of Denial-of-Service Attacks)* publié en mars 2015 par l'Institut Ponemon que le coût total moyen annuel des attaques DDoS s'élevait à 1,5 million de dollars pour chaque entreprise touchée. Avec une part du coût total chiffrée à 491 152 $, l'indisponibilité de services Internet orientés clients représente la principale répercussion financière d'une attaque DDoS.

En effet, la partie du *Rapport de l'enquête sur les risques informatiques mondiaux 2014* portant sur les attaques DDoS, publiée début 2015, indique que pour les PME, le coût moyen de chaque période d'arrêt due à une attaque DDoS est de 52 000 $. Les grandes entreprises sont encore plus sévèrement touchées, avec un coût de 444 000 $ par attaque concluante. Ces coûts incluent les pertes commerciales dues à l'indisponibilité ainsi que les dépenses informatiques engagées pour résoudre le problème.

Perte de productivité

Lorsque les systèmes commerciaux d'une entreprise sont hors service, la productivité du personnel chute inévitablement de façon significative. C'est particulièrement le cas pour les membres du personnel dont les tâches et responsabilités s'articulent autour des offres d'e-commerce de l'entreprise.

Mais, toujours selon le rapport de l'Institut Ponemon, les attaques DDoS ont la capacité de toucher une gamme bien plus large de systèmes et de services. En effet, 82 % des personnes interrogées ont déclaré qu'une attaque DDoS avait mis leur centre de données partiellement (48 %) ou totalement (34 %) hors service. Cela signifie que les attaques DDoS peuvent également faire chuter la productivité de départements qui n'opèrent pas en ligne ou dans le commerce électronique.

L'Institut Ponemon a révélé que la perte de productivité des entreprises due à une attaque DDoS s'élevait, en moyenne, à 173 169 $ par an.

Atteinte à la réputation

L'atteinte à la réputation est l'une des conséquences des attaques DDoS les plus difficiles à évaluer en termes de perte financière. L'atteinte à la réputation est l'une des conséquences des attaques DDoS les plus difficiles à évaluer en termes de perte financière. Néanmoins, selon 64 % des personnes interrogées lors de l'étude de l'Institut Ponemon, cela représente la conséquence principale d'une attaque DDoS. Elle l'emporte largement sur la chute de productivité du personnel informatique (35 %) et les pertes de revenus (33 %).

Après tout, une attaque DDoS peut avoir pour conséquence que les clients n'aient plus confiance en l'entreprise et y pensent à deux fois avant d'y refaire des achats à l'avenir. Étant donné que de nos jours, la concurrence en ligne est féroce, les entreprises ne peuvent pas se permettre que leur réputation soit ternie.

Les attaques DDoS à grande échelle qui provoquent des indisponibilités prolongées font presque toujours les gros titres, particulièrement si l'entreprise touchée est une marque très connue. Malheureusement, après ce type de publicité, les entreprises sont cataloguées comme « hackées » et même si l'attaque a uniquement fait tomber le site Web, sans compromettre les données des clients, l'atteinte à la réputation de l'entreprise est déjà chose faite.

Danger caché

Les attaques DDoS sont conçues pour perturber les entreprises, causer des dégâts et faire passer un message. Alors qu'il n'y a rien de secret sur la façon dont elles sont menées, les attaques DDoS sont souvent utilisées comme un écran de fumée pour occuper le personnel informatique d'une entreprise et pour masquer les véritables intentions des pirates.

En août 2015, Carphone Warehouse, l'un des plus grands distributeurs de téléphones portables au Royaume-Uni a été bombardé par une attaque DDoS. À l'époque, l'entreprise s'est démenée pour remettre les services touchés sur pied, mais une fois l'écran de fumée dissipé, Carphone Warehouse s'est rendu compte de l'attaque bien plus sophistiquée qui venait d'avoir lieu.

Pendant l'attaque DDoS, les cyber-criminels se sont infiltrés dans les systèmes de Carphone Warehouse et ont volé les données bancaires et personnelles de 2,4 millions de ses clients. Le vol aurait pu être repéré et empêché si le personnel de sécurité informatique n'avait pas été occupé à résoudre l'attaque DDoS.

Un cas semblable, peut-être le plus célèbre de tous, a eu lieu en 2011, lorsque le réseau PlayStation de Sony est resté hors ligne pendant des semaines après le vol des données personnelles et financières d'environ 77 millions de clients. Dans une lettre adressée à la Chambre des représentants des États-Unis à la suite de la brèche informatique, le président de Sony Computer Entertainment, Kazuo Hirai, a déclaré : « Les équipes de sécurité ont travaillé activement pour nous protéger contre les attaques par déni de service, et il se peut que cela ait rendu plus difficile de détecter rapidement cette intrusion. »

Selon le rapport de Kaspersky Lab publié en septembre 2015, intitulé *Denial of Service: How Businesses Evaluate the Threat of DDoS Attacks* (littéralement, *Déni de service : comment les entreprises évaluent la menace des attaques DDoS*), l'utilisation des attaques DDoS comme écran de fumée devient de plus en plus répandue.

Ce rapport de Kaspersky a révélé que près de trois quarts (74 %) des entreprises qui avaient subi une attaque DDoS avaient également remarqué la perturbation d'autres services, ce qui les amenait à penser que l'attaque avait pour but de masquer une intrusion plus grave.

Selon 45 % des personnes interrogées, les infections par des logiciels malveillants constituent l'effet secondaire principal des attaques DDoS, mais 32 % d'entre elles affirment avoir été victimes d'intrusions réseau ou d'un autre type de piratage. Dans l'ensemble, 26 % des entreprises ayant subi une attaque DDoS ont affirmé que des données sensibles avaient été perdues lors de l'attaque et 31 % d'entre elles ont déclaré que des données non sensibles avaient été volées.

Cette tendance croissante et inquiétante de l'utilisation des DDoS comme leurre rend d'autant plus important de mettre en place un système d'atténuation détectant les comportements suspects en temps réel.

« Les équipes de sécurité ont travaillé activement pour nous protéger contre les attaques par déni de service, et il se peut que cela ait rendu plus difficile de détecter rapidement cette intrusion. »

5. DDoS : atténuation des attaques

Les attaques DDoS deviennent de plus en plus fréquentes, sophistiquées et bon marché, c'est pourquoi il est plus important que jamais de mettre en place un plan précis d'atténuation des attaques. Malheureusement, il ne suffit plus de se dire que « ça n'arrive qu'aux autres ». Les cyber-criminels, les hacktivistes et les personnes mécontentes frappent souvent leurs cibles sans aucune distinction, et cela rend toutes les entreprises et organisations potentiellement vulnérables aux attaques DDoS.

Le plus important pour les entreprises est de contrer la menace posée par les attaques DDoS avant qu'elles ne surviennent. C'est une chose d'être touché par une interruption de service, c'en est une autre de se faire voler des données d'entreprise.

Donc, comment veiller à ce que votre organisation résiste à une attaque DDoS ? Voici une stratégie en sept points pour mettre en place une meilleure défense contre les attaques DDoS :

1. Donnez aux attaques DDoS une place importante dans votre plan de continuité des activités

Les attaques DDoS doivent absolument faire partie de votre plan de continuité des activités. Mais cela implique que les attaques DDoS sont accidentelles ou inattendues, et ce n'est tout simplement pas le cas de nos jours.

Par conséquent, les attaques DDoS devraient être clairement définies et faire partie intégrante du plan de réponse aux incidents de votre entreprise. Cela signifie que les membres clés de votre personnel, vos partenaires stratégiques et les personnes à contacter en cas d'urgence doivent être connus avant l'évènement, de sorte que lors d'une attaque DDoS, l'entreprise sache précisément comment réagir.

Il est recommandé d'effectuer des essais annuels, voire semestriels, de ces plans afin de garantir que tous les aspects ont été pris en compte et que tous les individus concernés comprennent exactement quel est leur rôle. Ces « exercices d'incendie » réguliers permettront à votre organisation d'être mieux préparée en cas d'attaque et répondront également à vos éventuelles obligations de conformité en matière de planification de la continuité des activités.

2. Ne surestimez pas votre infrastructure réseau

Dans des conditions de fonctionnement normales, votre équipement de réseau périphérique s'occupera invariablement de tout, tel que prévu. Cependant, les volumes de trafic que peut produire une attaque DDoS moderne sont suffisants pour faire tomber jusqu'aux équipements de réseau les plus performants.

Les entreprises et organisations qui pensent que leurs pare-feu fournissent une défense adéquate contre une attaque DDoS comprendront bien assez tôt que ce n'est pas le cas. Même la prochaine génération de pare-feu, qui promet une protection accrue contre les DDoS, ne peut pas garantir la sécurité de votre infrastructure essentielle contre tous les types d'attaques DDoS.

3. Fixez des repères afin de détecter plus facilement une attaque DDoS

Étonnamment, de nombreuses entreprises ne connaissent pas la tension subie par leur infrastructure réseau lors de conditions de fonctionnement normales. Par conséquent, elles ont du mal à détecter l'apparition de comportements anormaux. Toutefois, même si elles peuvent constituer des signaux annonciateurs de DDoS, des performances réseau inhabituellement lentes et une indisponibilité du site Web n'indiquent pas nécessairement que votre organisation est attaquée.

En augmentant le contrôle de la sécurité à l'échelle de l'entreprise, de la périphérie jusqu'aux points d'extrémité, vous pouvez augmenter vos chances de détecter une DDoS dès son lancement. De même, si vous gardez à l'esprit les notions de flexibilité et d'adaptabilité lors de la conception de votre réseau – et si savez où se trouvent tous vos « goulots d'étranglement » dès le départ – vous pourrez reconnaître des attaques DDoS de façon plus précise et proactive.

4. Pensez comme un hacker

Ne vous dites pas que les hackers sont imprévisibles et opportunistes. En fait, ils sont souvent extrêmement méthodiques dans leurs approches et ils essayeront de profiter d'autres faiblesses si leurs tentatives d'attaque sont contrecarrées. Les attaques DDoS ne font pas exception à la règle, voilà pourquoi vous pouvez économiser beaucoup d'argent en vous mettant dès maintenant à leur place.

Pensez aux points sur lesquels ils seraient susceptibles de se concentrer et parez tout éventuel type d'attaque. Une seule pièce vulnérable dans votre infrastructure pourrait faire la différence, laissant ainsi votre réseau protégé ou exposé.

5. Connaissez vos clients

La plupart des organisations savent où se situe la majorité de leurs clients, et cela signifie que les origines du trafic réseau peuvent être

analysées et comprises. Bien entendu, de nouveaux clients viendront continuellement s'ajouter, mais si votre entreprise ne s'attend absolument pas à un intérêt venu d'Europe de l'Est ou de Chine, le trafic provenant de ces régions pourrait indiquer quelque chose de suspect.

Alors que le fait de mettre des adresses IP sur liste noire en fonction de leur origine est une tâche ingrate qui n'en finit jamais, il est possible de restreindre l'accès en fonction de la localisation, particulièrement si vous avez choisi une solution de protection DDoS qui vous le permet.

6. Mettez préalablement en place une solution spécifique de protection DDoS

Il existe des solutions d'atténuation d'urgence des DDoS et dans la plupart des cas, elles peuvent être déployées en moins d'une heure. Ces solutions ont tendance à se baser sur un routage du trafic (null-route) et une redirection du trafic sur demande, les coûts associés à chaque évènement étant facturés au client. Mais pourquoi risquer la réputation, la productivité et les résultats de votre entreprise en vous reposant sur une solution d'atténuation qui ne protège pas proactivement votre infrastructure ?

Mettre en place un système spécifique d'atténuation des attaques DDoS détectant les comportements suspects est non seulement plus sûr, mais vous permet également une plus grande tranquillité d'esprit vis-à-vis de vos activités. En bref, ces solutions sont liées à votre flux de données et sont envoyées dans des centres de nettoyage qui filtrent la majorité du trafic suspect et garantissent un trafic authentique en temps réel.

En faisant partie de votre plan de réponse aux incidents, cette protection spécifique contre les attaques DDoS enverra des alertes immédiates afin d'identifier et d'atténuer toute éventuelle attaque.

Mettre en place un système spécifique d'atténuation des attaques DDoS détectant les comportements suspects est non seulement plus sûr, mais vous permet également une plus grande tranquillité d'esprit vis-à-vis de vos activités.

7. Soyez paré à toute éventualité

Votre solution d'atténuation des attaques DDoS devra être testée et validée lors de sa mise en place et ensuite, à un intervalle régulier. Cela vous assurera qu'elle remplit dès le départ les attentes de votre organisation et qu'aucune vulnérabilité n'a été négligée.

Les attaques DDoS ont évolué depuis leur arrivée dans le paysage de la sécurité informatique il y a déjà de nombreuses années et elles continueront inévitablement d'évoluer. Voilà pourquoi votre solution d'atténuation doit également évoluer, sinon votre entreprise pourrait ultérieurement être exposée. Il est également encouragé de mettre en place une relation de travail étroite avec votre fournisseur de solution d'atténuation contre les attaques DDoS afin de veiller à ce que votre réponse face à une attaque soit calme, préparée et efficace.

De nos jours, la menace posée par les attaques DDoS est réelle et leur intensité potentielle – associée aux faibles dépenses nécessaires pour en lancer une – en fait un problème de sécurité de plus en plus inquiétant pour les entreprises.