Akamai

LIVRE BLANC

Éviter le chaos

grâce à une protection adaptée contre les attaques DDoS au niveau de la couche applicative

Que représentent les attaques DDoS au niveau de la couche applicative pour nous aujourd'hui ?

Une attaque DDoS, ou par déni de service distribué, est un type de cyberattaque qui tente de rendre un site Web ou une ressource réseau indisponible en l'inondant de trafic malveillant, afin de l'empêcher de fonctionner. Les experts en sécurité du monde entier connaissent malheureusement bien ce procédé. Les attaques DDoS constituent toujours la technique d'attaque la plus courante des acteurs malveillants et ont connu une augmentation au cours des cinq dernières années. Par exemple, l'une des attaques les plus récentes (en termes de paquets par seconde [PPS]) a culminé à 809 MPPS en près de deux minutes.

Dans cette augmentation des attaques, nous avons observé une tendance à la multiplication des cas d'attaques DDoS au niveau de la couche applicative. Également connues sous le nom d'attaques DDoS de couche 7, ces attaques ciblent et perturbent des applications Web spécifiques, et non des réseaux entiers. Bien qu'il soit difficile de prévenir et d'atténuer les risques de ces attaques, l'adoption massive de technologies telles que l'automatisation et les services cloud a permis aux pirates d'accéder facilement aux outils nécessaires pour les lancer. Par conséquent, il n'a jamais été aussi facile de compromettre la couche applicative.

En réalité, les requêtes utilisées dans ce type d'attaque ressemblent à des requêtes normales de l'utilisateur final. Il n'existe donc pas de moyen simple d'évaluer la sophistication d'une attaque. Si une attaque affecte à la fois le serveur ciblé et le réseau de manière efficace, cela signifie qu'elle crée plus de dégâts avec moins de bande passante totale. En résumé, les attaques au niveau de la couche applicative sont faciles à mettre en œuvre, difficiles à ralentir ou à arrêter, et spécifiques à une cible.

Afin de comprendre comment les attaques DDoS au niveau de la couche applicative affectent nos organisations de manière inédite, nous devons savoir comment elles nous touchent dans toutes les catégories. Comparons les catégories d'attaques DDoS avec des pièges susceptibles de faire dégénérer une fête que vous avez organisée chez vous. Lorsque vous organisez une fête pour une occasion spéciale ou pour vous amuser le week-end, vous laissez entrer des invités dans votre maison. Cependant, quelques scénarios indésirables peuvent se produire :

Types d'attaque DDoS

Scénario 1
Attaque volumétrique

Enthousiastes à propos de votre fête, vos invités partagent un peu trop d'informations à son sujet (notamment sur les réseaux sociaux). Les gens finissent par apprendre que votre fête est l'événement à ne pas manquer. Ainsi, le jour J, des personnes que vous ne connaissez pas arrivent en masse. Voilà l'analogie qu'on peut faire avec une attaque DDoS volumétrique : toutes vos ressources sont consommées par des personnes que vous n'aviez pas prévues.

Scénario 2
Attaque de protocole

Un invité à qui vous pensiez pouvoir faire confiance a été corrompu ! Les gens qui veulent être invités à votre fête (et qui n'ont pas reçu d'invitation) harcèlent cet invité de questions pour connaître les détails de l'événement. L'invité cède et de nombreuses personnes que vous n'aviez pas invitées viennent à votre fête. Voilà l'analogie que l'on peut faire avec une attaque DDoS de protocole : quelqu'un qui était censé assurer la confidentialité des informations a failli dans son rôle.

Scénario 3
Attaque d'application

Une personne malveillante entend parler de votre fête et décide de se faire passer pour un invité, afin d'entrer dans votre maison et de voler vos effets personnels. Voilà l'analogie qu'on peut faire avec une attaque DDoS d'application : une personne se fait passer pour un visiteur légitime afin de mieux vous nuire.

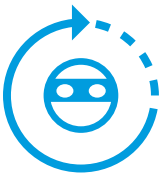
Dans tous ces scénarios, il existe une vulnérabilité commune : vous avez ouvert votre maison pour un événement. Il s'agit de la vulnérabilité inévitable que les attaques DDoS au niveau de la couche applicative exploitent, car il s'agit de la couche dans laquelle votre entreprise interagit avec l'utilisateur. De plus, comme il s'agit d'une couche sur laquelle vous avez moins de contrôle, puisqu'elle sert directement les utilisateurs, il peut être plus difficile d'atténuer les risques d'attaques DDoS au niveau de cette couche.

De plus, si l'un de ces problèmes se produit, cela vous coûtera des frais supplémentaires. Si on reprend l'analogie de la fête, vous risquez de faire face à des dépenses liées à la consommation de plus grandes quantités de nourriture et de boissons que prévu, à la découverte par des inconnus de renseignements personnels vous concernant ou aux retombées d'une attaque contre votre maison. Une mauvaise organisation peut donc coûter cher.

De nombreuses solutions de sécurité promettent de plus en plus de protéger vos systèmes, vos ressources et vos informations sensibles contre les attaques DDoS au niveau de la couche applicative, qui sont désormais plus courantes et parmi les plus difficiles à contrer. Vous leur avez accordé votre confiance pour protéger ce que vous avez à offrir. En fin de compte, la qualité de votre protection contre les attaques DDoS dépend de celle de la plateforme à laquelle vous la confiez. Examinons les derniers changements et tendances à prendre en compte lorsque vous recherchez la plateforme de protection contre les attaques DDoS au niveau de la couche applicative.

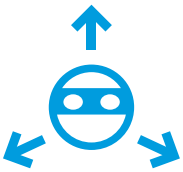
Les tendances et les changements

Comme toujours, lorsque nous élaborons des solutions contre une attaque spécifique, les pirates adaptent leurs stratégies en conséquence pour les contourner. Nous avons surveillé leurs agissements, et voici les quatre tendances et changements que nous observons actuellement :



1. Passage à des attaques répétées et de courte durée

Les attaques DDoS portent de moins en moins sur la durée et davantage sur l'envergure et la fréquence. Akamai a constaté des attaques complexes avec plus de neuf vecteurs d'attaque différents combinant ARMS, SYN flood, réflexion UDP (DNS, WS-Discovery, etc.), HTTP flood, et bien plus encore.

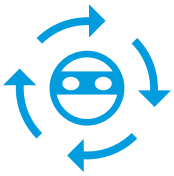


2. Utilisation plus fréquente d'attaques multivectorielles

Plus de 20 % des pirates ont recours à des attaques DDoS multivectorielles, combinant différentes méthodes d'attaque DDoS en une attaque courte, qui se répète peu de temps après. Selon Link11, le plus grand nombre de vecteurs concurrents observés était de 18, soit une augmentation de 50 % par rapport à 2021.

3. Contournement plus fréquent des mesures de détection et donc d'atténuation

La distinction entre le trafic d'attaque et le trafic normal est difficile, en particulier dans le cas d'une couche applicative. Par exemple, lorsqu'un botnet exécute une attaque HTTP flood contre le serveur d'une victime. Comme chaque bot dans un botnet fait des requêtes réseau apparemment légitimes, le trafic n'est pas usurpé et peut sembler « normal ».



4. Automatisation d'abord, adaptation des tactiques ensuite

Avec la prévalence des plateformes cloud et des IaaS/PaaS, les pirates ont facilement accès à l'automatisation et à la puissance de calcul. Il leur est donc facile d'automatiser les attaques et de lancer une attaque rapidement et à grande échelle. Ces attaques ne sont donc pas seulement importantes en termes de volume. Leur distribution est plus grande, elles sont intelligemment conçues et plus aléatoires (randomisation des paramètres dans les requêtes, etc.).

Comme indiqué dans le scénario de la fête, votre maison peut être compromise de trois façons : par la consommation de ressources, un invité corruptible ou un acteur malveillant déguisé. Avec les tendances et les changements dans les attaques au niveau de la couche applicative, votre maison (ou plutôt entreprise) pourrait se retrouver confrontée à un chaos conçu pour passer sous votre radar. En effet, dans ces trois techniques, tout est orchestré pour favoriser la furtivité, par exemple, en vérifiant au préalable le nombre d'entrées de votre maison, en se renseignant à l'avance sur le code vestimentaire de la fête ou en créant de faux profils sur les réseaux sociaux, afin d'en savoir plus sur vous et faire passer les acteurs malveillants pour vos amis proches aux yeux de tous les autres invités.

En raison de la complexité croissante des attaques DDoS au niveau de la couche applicative, il est utile d'avoir une stratégie de protection plus holistique que par le passé. Auparavant, toute solution de protection des applications Web et des API (WAAP) pouvait couvrir vos besoins, même celles conçues en interne. Désormais, votre solution WAAP doit dépasser la complexité des attaques au niveau de la couche applicative qui se produisent aujourd'hui.

Une approche holistique de la protection contre les attaques DDoS au niveau de la couche applicative

Ce qui rend les attaques DDoS au niveau de la couche applicative difficiles à détecter, c'est que même lorsque les attaques multivectorielles contiennent des schémas évidents, un pirate motivé surveillera la réponse à l'attaque et la modifiera pour esquiver un défenseur déterminé. Pour relever ce défi de manière plus cohérente et plus précise, vous devez améliorer vos capacités WAAP en matière de détection, d'atténuation et de fonctions en libre-service.

En dernière instance, vous ne voulez pas que votre WAAP surveille uniquement la porte d'entrée de votre maison. Vous voulez que la protection soit aussi capable de défendre chaque point d'entrée, de comprendre comment identifier les acteurs malveillants déguisés en invités et qu'elle soit évolutive, si vous êtes confronté à plusieurs attaques à la fois. Il y a une bonne nouvelle : il est possible d'adopter la bonne plateforme pour atténuer le chaos des attaques DDoS au niveau de la couche applicative et poursuivre ses activités comme d'habitude. Votre stratégie de lutte contre les attaques DDoS doit devenir plus globale et se concentrer sur les points suivants :

L'évolutivité de votre plateforme

Peu importe le fonctionnement quotidien de votre WAAP, si elle ne peut pas évoluer pour absorber une attaque volumétrique, elle sera vite dépassée. C'est pourquoi la plateforme qui chapeaute la WAAP est tout aussi importante que la WAAP elle-même. Vous voulez également savoir où la plateforme fonctionne. Par exemple, Akamai dispose de sites en périphérie, dans le monde entier, souvent dans les régions d'origine des attaques. Il est beaucoup plus facile d'arrêter une attaque DDoS si elle peut être atténuée à l'endroit même où elle a commencé. De plus, l'évolutivité facilitera grandement les opérations à enjeux, comme la limitation de débit et les règles personnalisées.

Les ressources de données et les résultats qui alimentent vos protections

Bien que n'importe quelle solution WAAP puisse surveiller le trafic et produire des rapports sur les données que vous générez, envisagez une solution capable d'agréger les données d'un point de vue global. Lorsque votre fournisseur de solutions dispose d'une visibilité sur le trafic dans des milliers d'entreprises, les données que vous générez peuvent être contextualisées parmi les organisations confrontées aux mêmes menaces et peuvent mieux renseigner les systèmes d'apprentissage automatique en place dans votre solution. Ensuite, vos propres équipes internes peuvent obtenir ces données et les utiliser pour itérer et personnaliser votre solution.

La visibilité et la précision de votre solution

Certaines méthodes de détection peuvent être proposées par défaut, notamment les détections d'anomalies ou de comportements, qui ne se limitent pas au trafic client entrant, mais s'intéressent au débit de la connexion d'origine et aux paramètres de performance du serveur. Cependant, lorsque vous disposez d'une solution évolutive basée sur un ensemble de données robuste, votre WAAP sera beaucoup plus ciblée et précise. De plus, vous aurez une compréhension plus détaillée de ce qui se passe sur votre trafic, car la solution est adaptative et capable de comprendre s'il y a une attaque cachée (comme les attaques qui se cachent derrière un proxy ouvert sur Internet). Tout cela aidera à s'assurer que les bonnes personnes sont informées tout en réduisant considérablement les faux positifs.

Si vous deviez organiser une fête, vous voudriez que votre maison soit suffisamment grande (évolutive) pour accueillir des invités supplémentaires qui n'auraient peut-être pas été conviés, afin d'éviter d'être débordé. Vous voudriez parler à d'autres personnes qui ont connu de mauvaises expériences lors de fêtes (ressources de données), afin de savoir à l'avance quelles mesures de protection mettre en place. Et vous voudriez partager la liste des invités à l'avance et saluer tous les invités avant qu'ils entrent dans votre maison (visibilité et précision), pour vous assurer que tout le monde est en sécurité.

Et si vous ne voulez pas faire tout ce travail vous-même, vous pouvez embaucher des renforts de confiance qui s'en chargeront pour vous. Les services gérés peuvent permettre de surveiller tous les signaux auxquels vous devez être très attentif, afin de distinguer un invité régulier d'un invité malveillant. De plus, vous éliminez le stress de devoir consacrer le temps et l'expertise de votre personnel à prévenir 24 heures sur 24 ces attaques de plus en plus courantes et difficiles à détecter.

Le sujet des attaques DDoS au niveau de la couche applicative est rempli de variables et de vulnérabilités qui font naturellement partie de la couche applicative. Et c'est un sujet essentiel, car les attaques DDoS au niveau de la couche applicative peuvent être les plus préjudiciables à votre organisation. Cependant, la défense contre ce type d'attaque ne doit pas être compliquée ou chaotique. Tout ce dont vous avez besoin, c'est d'une solution stratégique, évolutive et axée sur les données — et ensuite vous aurez l'esprit libre (et pourrez faire la fête).

Découvrez comment Akamai peut vous aider à vous protéger contre les attaques DDoS de couche 7.