Akamai

Les attaques DDoS peuvent-elles être interrompues instantanément ?

DÉFINISSONS CLAIREMENT CE QU'EST LE TEMPS DE RÉPONSE

Le temps de réponse devrait être limité, non ? Il s'agit du délai entre le début d'une attaque DDoS et la mise en œuvre effective de la protection de vos ressources ou applications.

Mais ce n'est pas ce que proposent réellement les accords de niveau de service (SLA) de tous les fournisseurs. Vous devez comprendre exactement quand l'attaque commence et quand elle s'arrête.

MÉFIEZ-VOUS DE CES SITUATIONS COURANTES AVEC CERTAINS FOURNISSEURS

FOURNISSEUR A

0:10 = 05:10

Les contrôles du fournisseur A doivent identifier un pic de trafic pendant plus de 5 minutes avant de confirmer qu'il s'agit d'une attaque DDoS.

L'accord de niveau de service avec temps de réponse garanti de 10 secondes ne démarre qu'après la confirmation de l'attaque.

FOURNISSEUR B

TTM = TEMPS DE RÉPONSE

Les conditions générales du fournisseur B définissent le temps de réponse comme le délai nécessaire pour déployer un contrôle de défense.

Aucun accord de niveau de service n'est garanti pour arrêter l'attaque.

FOURNISSEUR C

AUTOMATISATION ≠ GARANTIE

Le fournisseur C s'engage à fournir une détection et une protection automatisées dans son accord de niveau de service avec temps de réponse garanti.

Des techniques de défense manuelles et personnalisées visant à neutraliser les attaques sophistiquées ne font pas partie de cet accord de niveau de service.

COMPRENDRE LES CONDITIONS GÉNÉRALES

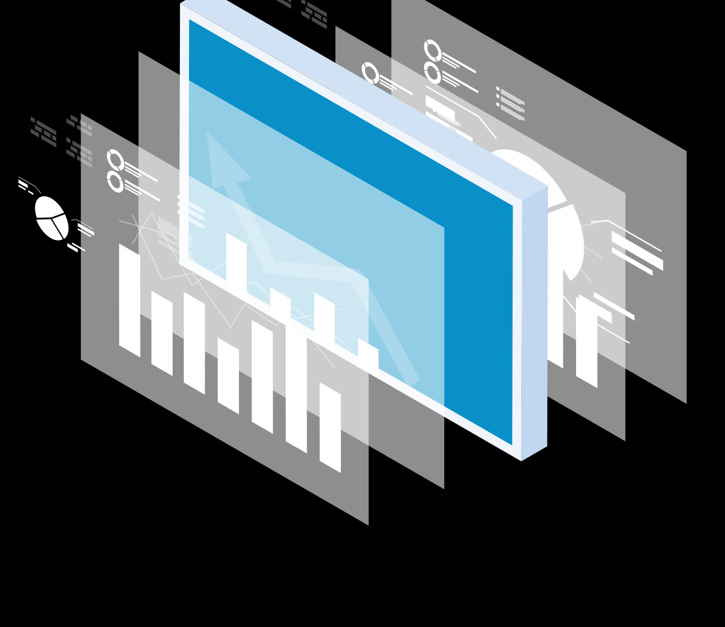
Soyez **méfiant** lorsque vous rencontrez des formulations de type :

… temps de réponse …

En cas d'attaque DDoS prolongée …

… après détection …

LE TEMPS DE RÉPONSE D'AKAMAI



Lorsque **immédiat signifie zéro** seconde

Nos contrôles de protection proactifs sont conçus pour bloquer les attaques DDoS et vous protéger avant même que vous ne vous rendiez compte que vous avez été ciblé par une attaque. C'est la puissance de l'Akamai Intelligent Edge Platform.

TEMPS DE **détection de l'attaque** + TEMPS **d'application des contrôles d'atténuation** + TEMPS DE **blocage de l'attaque** = **Le meilleur temps de réponse de sa catégorie**

LES 8 ÉTAPES DE LA PROTECTION CONTRE LES ATTAQUES DDOS

Akamai dispose du temps de réponse le plus rapide du secteur grâce à une collaboration efficace entre ses chercheurs experts en menaces, ses gestionnaires d'incidents, ses architectes de sécurité et ses technologies de défense de pointe. Le centre de commande des opérations de sécurité (SOCC) d'Akamai effectue les étapes suivantes :

1. **Détection** rapide de l'attaque grâce à la surveillance DDoS permanente.
2. **Alerte** du client en suivant le protocole établi.
3. **Gestion** du trafic client avec un routage permanent facilité.
4. **Analyse** du trafic et identification des vecteurs pour l'application de la protection.
5. **Ajustement** des protections appliquées pour minimiser le nombre de faux positifs et faux négatifs.
6. **Identification** des nouveaux vecteurs d'attaque.
7. **Analyse** du trafic et identification des vecteurs émergents pour appliquer des mesures de protection en continu.
8. **Optimisation** des protections appliquées pour neutraliser les attaques changeantes.

LES RISQUES D'UN TEMPS DE RÉPONSE RETARDÉ

Quelles sont les **conséquences** des temps d'arrêt ?

0:01 — Après 1 seconde, vos ressources ou applications Web deviennent indisponibles.

0:10 — Après 10 secondes, l'expérience des clients devient moins fluide et la productivité des employés diminue.

5:00 — Après 5 minutes, la réputation de votre marque est dégradée et votre chiffre d'affaires est affecté.

ÉVALUEZ VOTRE STRATÉGIE DE SÉCURITÉ FACE AUX ATTAQUES DDOS

En combien de temps votre fournisseur peut-il détecter une attaque ?

Vos applications les plus importantes seraient-elles toujours disponibles ?

Pourriez-vous subir des dommages collatéraux ?

Vos utilisateurs légitimes seraient-ils affectés ?

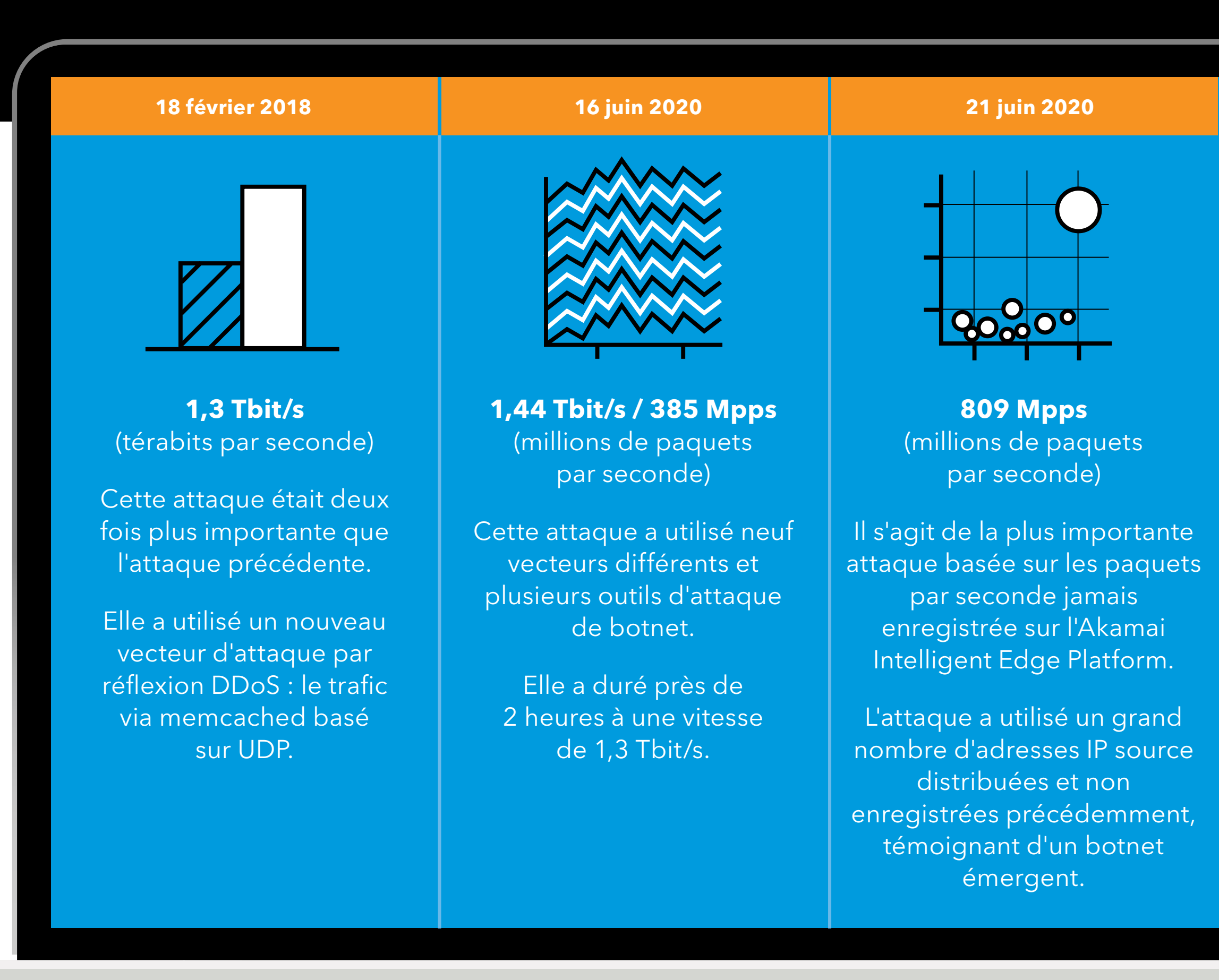
En combien de temps votre fournisseur peut-il appliquer des contre-mesures de protection ?

En combien de temps votre fournisseur peut-il commencer à analyser le trafic ?

L'EXPERTISE D'AKAMAI EN MATIÈRE DE MENACES

Plus importantes, plus **complexes** et plus **dangereuses**

L'ampleur des attaques DDoS évolue comme jamais auparavant. En 2020, nous avons observé une activité DDoS de plus en plus importante et complexe. Le nombre de vecteurs d'attaque et leurs combinaisons sont sans précédent.



18 février 2018	16 juin 2020	21 juin 2020
1,3 Tbit/s (térabits par seconde) Cette attaque était deux fois plus importante que l'attaque précédente. Elle a utilisé un nouveau vecteur d'attaque par réflexion DDoS : le trafic via memcached basé sur UDP.	**1,44 Tbit/s / 385 Mpps** (millions de paquets par seconde) Cette attaque a utilisé neuf vecteurs différents et plusieurs outils d'attaque de botnet. Elle a duré près de 2 heures à une vitesse de 1,3 Tbit/s.	**809 Mpps** (millions de paquets par seconde) Il s'agit de la plus importante attaque basée sur les paquets par seconde jamais enregistrée sur l'Akamai Intelligent Edge Platform. L'attaque a utilisé un grand nombre d'adresses IP source distribuées et non enregistrées précédemment, témoignant d'un botnet émergent.

Une défense efficace associe une plateforme éprouvée, des professionnels expérimentés et des techniques et des processus sophistiqués.

Le **temps de réponse** doit correspondre au temps nécessaire à l'identification et au blocage du trafic malveillant, sans affecter le trafic et les utilisateurs légitimes.

Une attaque n'est bloquée avec succès que si vos applications stratégiques, votre infrastructure et la réputation de votre marque sont parfaitement protégées.

RENFORCEZ VOTRE PROTECTION CONTRE LES ATTAQUES DDOS DÈS AUJOURD'HUI

Découvrez comment Akamai peut vous aider à bénéficier d'une protection instantanée.

En savoir plus

Akamai

Akamai sécurise et diffuse des expériences digitales pour les plus grandes entreprises du monde entier. L'Intelligent Edge Platform d'Akamai englobe tout, de l'entreprise au cloud, afin d'offrir rapidité, agilité et sécurité à ses clients et à leurs entreprises. Les plus grandes marques mondiales comptent sur Akamai pour les aider à concrétiser leur avantage concurrentiel grâce à des solutions agiles qui développent la puissance de leurs architectures multiclouds. Akamai place les décisions, les applications et les expériences au plus près des utilisateurs, et au plus loin des attaques et des menaces. Les solutions de sécurité en bordure de l'Internet, de performances Web et sur mobile, d'accès professionnel et de diffusion vidéo du portefeuille d'Akamai s'appuient également sur un service client exceptionnel, des analyses et une surveillance 24 h/24 et 7 j/7, 365 jours par an. Pour savoir pourquoi les plus grandes marques mondiales font confiance à Akamai, rendez-vous sur les pages www.akamai.com et blogs.akamai.com ou suivez @Akamai sur Twitter. Nos coordonnées dans le monde entier sont disponibles à l'adresse www.akamai.com/locations.

Publication : 11/20