

Attaques DDoS : quand on cherche à faire tomber votre site

Saturer un service pour le rendre indisponible : qui fait ça, pourquoi, et comment une PME s'en protège sans budget de banque.

7 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/attaque-ddos

L'attaque par déni de service distribué (DDoS) ne vole rien : elle sature — des milliers de machines (souvent des objets connectés piratés) bombardent votre site ou votre connexion jusqu'à l'asphyxie. Longtemps réservée aux grandes cibles, elle s'est démocratisée : quelques dizaines d'euros « louent » une attaque. Motifs : extorsion, concurrence déloyale, vengeance, ou simple dommage collatéral. La protection, elle aussi, s'est démocratisée.

1. Comprendre l'attaque

- Le principe : plus de requêtes que le service ne peut en traiter — le site rame puis tombe, les vrais visiteurs ne passent plus
- Les variantes : saturation brute de la connexion (volumétrique), épuisement du serveur (requêtes applicatives coûteuses), ou attaques ciblant des fonctions précises (recherche, panier)
- La durée : de quelques minutes (démonstration, écran de fumée pendant une autre attaque) à des jours (extorsion)
- Le DDoS d'extorsion : « payez ou nous continuons » — même famille que le ransomware, même réponse : on ne paie pas, on se protège

2. Se protéger : déléguer à ceux qui encaissent

- La protection DDoS est une affaire d'échelle : elle se délègue à des infrastructures qui absorbent — pas à votre serveur
- Pour un site web : un CDN/proxy de protection (Cloudflare et équivalents — offres gratuites incluses) place un bouclier mondial devant le site ; c'est la mesure reine, souvent gratuite pour une PME
- Vérifier ce que votre hébergeur inclut : les hébergeurs sérieux (OVHcloud et autres) intègrent une protection volumétrique de base
- Le e-commerce et les services critiques justifient les offres de protection supérieures — à mettre en regard du coût d'une journée de vente perdue (voir notre guide e-commerce)
- Cacher l'adresse IP d'origine du serveur derrière le bouclier : un bouclier contournable par l'adresse directe ne protège rien — point technique à faire vérifier

BON À SAVOIR

L'essentiel pour 90 % des PME tient en une phrase : votre site derrière un CDN avec protection (souvent gratuit), votre hébergeur choisi avec protection incluse, et votre supervision qui alerte en cas d'indisponibilité. Trois décisions prises une fois, zéro maintenance — et l'attaque à 50 € louée par un concurrent aigri s'écrase sans que vous la remarquiez.

3. Pendant l'attaque

- La supervision vous alerte avant les clients : site lent/down + trafic anormal = suspicion
- Contacter l'hébergeur/le prestataire : ils voient la nature de l'attaque et activent les mitigations supérieures
- Activer le mode « sous attaque » du CDN le cas échéant (défi automatique aux visiteurs) — prévu pour
- Ne pas payer en cas de demande de rançon ; documenter (captures, heures, messages) et déposer plainte — le DDoS est un délit
- Communiquer sobrement si l'indisponibilité se voit : « incident technique en cours de résolution » suffit publiquement

4. Et votre connexion de bureau ?

- Le DDoS peut viser la connexion de l'entreprise elle-même (rare mais handicapant : plus d'Internet au bureau)
- La parade est la même que pour les pannes : la connexion de secours 4G/5G maintient l'essentiel
- Éviter d'exposer l'adresse du bureau inutilement : pas de services auto-hébergés publics sans nécessité, et le VPN plutôt que des ports ouverts
- Signalement à l'opérateur : les FAI professionnels ont des procédures de mitigation

L'essentiel à retenir

- 01 Placer le site derrière un CDN avec protection DDoS
- 02 Vérifier la protection incluse chez l'hébergeur
- 03 Masquer l'adresse d'origine du serveur derrière le bouclier
- 04 Superviser la disponibilité avec alertes
- 05 Prévoir la connexion de secours pour le bureau
- 06 En cas d'attaque : mitigation, documentation, plainte — jamais de rançon

Questions fréquentes

Qui attaquerait une PME comme la nôtre ?

Les cas réels observés : le concurrent indélicat (les boutiques en ligne pendant les périodes clés), l'ex-salarié ou le client furieux (l'attaque se loue sans compétence), l'extorsion opportuniste, et le dommage collatéral (votre hébergement mutualisé voisin d'une cible). La motivation importe peu : la protection de base étant quasi gratuite, la question « qui ? » ne conditionne plus la réponse « se protéger ».

Mon site est tombé : DDoS ou simple panne ?

La panne est dix fois plus fréquente : hébergement défaillant, pic de trafic légitime (passage TV, promo), mise à jour ratée. Les indices du DDoS : trafic massif depuis des sources innombrables et improbables, motifs de requêtes répétitifs, courrier de rançon. L'hébergeur ou le CDN tranche en regardant les courbes — d'où l'intérêt d'être chez des acteurs outillés.

Le CDN gratuit type Cloudflare a-t-il des contreparties ?

Votre trafic transite par un tiers (américain pour les leaders — question à intégrer à votre analyse RGPD selon vos données), et les fonctionnalités fines sont payantes. Pour un site vitrine, le rapport protection/coût reste imbattable ; des alternatives européennes existent pour les contextes exigeants. L'important : décider en connaissance, pas par défaut.

Pour aller plus loin

ANSSI — comprendre et prévenir les DDoS — cyber.gouv.fr/publications/comprendre-et-anticiper-les-attaques-ddos

Cybermalveillance.gouv.fr — l'attaque en déni de service — www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/attaque-en-deni-de-service-ddos

Un doute, une urgence, un incident ?

Cyberionis évalue votre exposition, prépare vos défenses et vous épaulé pour réagir vite en cas d'attaque.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr