# Liste de contrôle de la lutte contre l'extorsion DDoS

Êtes-vous prêt à faire face à la hausse des attaques par déni de service distribué (DDoS) ? Les entreprises qui ne disposent pas d'une stratégie de protection contre les attaques DDoS se retrouvent face à deux options : payer la rançon ou risquer de subir des interruptions imprévues. Suivez ces étapes pour limiter le risque d'attaque DDoS à des fins d'extorsion contre votre entreprise.

## 1. Ne cédez pas aux menaces (imaginaires ou autres)

Akamai recommande de ne pas payer de rançon ni céder aux tentatives d'extorsion : il n'y a aucune garantie que le pirate mette ses menaces à exécution ni que le paiement vous protège d'une attaque DDoS. Les cybercriminels tentent de tirer profit de « la peur de l'inconnu » pour gagner rapidement de l'argent avant de passer à la cible suivante.

## 2. Faites appel aux experts de la protection

Déterminez si les ressources stratégiques et l'infrastructure dorsale sont protégées. Si vous ne disposez pas de contrôles de protection contre les attaques DDoS, engagez des fournisseurs basés sur le cloud qui peuvent rapidement activer des services d'urgence (contactez le support DDoS d'Akamai) pour réduire les risques. Nos spécialistes SOCC dans le monde luttent avec succès contre les attaques DDoS depuis plus de 20 ans.

## 3. Que les jeux DDoS commencent

Si vous disposez du bon partenaire de protection et de contrôles de sécurité adaptés, les pirates n'ont aucune chance. Pour Akamai, presque toutes les attaques DDoS associées à cette campagne ont été bloquées de manière proactive avec notre accord de niveau de service (SLA) immédiat ; seul un faible pourcentage a nécessité une protection active par notre SOCC mondial. En effet, environ 70 % de toutes les attaques que nous avons bloquées en 2020 ont été totalement stoppées avec l'accord de niveau de service (SLA) immédiat de Prolexic.

## 4. Changez de stratégie de sécurité

Il suffit d'une attaque pour savoir que le système de défense contre les attaques DDoS est indispensable dans le contexte de menaces actuel. Évaluez votre tolérance au risque pour déterminer si une solution de protection à la demande ou de protection permanente basée sur le cloud vous convient le mieux pour garantir la protection de votre présence sur Internet.

## 5. Repensez votre guide DDoS

Si ce n'est pas déjà le cas, faites en sorte que vos équipes chargées de l'informatique, des opérations, de la sécurité et de la communication avec les clients travaillent main dans la main pour vous assurer que vous êtes préparé et saurez réagir en cas d'attaque. Chez Akamai, nous créons des guides de défense personnalisés avec chaque client et réalisons divers exercices de préparation aux attaques afin de garantir que les processus, les personnes et les procédures appropriés sont en place pour optimiser la réponse aux incidents.

Pour garantir l'opérationnalité de leurs ressources commerciales stratégiques actuelles, les entreprises, qu'elles soient grandes ou petites, ont besoin d'un accès à des contrôles de protection de haute qualité, à l'échelle de leur plateforme, ainsi que de l'expertise nécessaire pour stopper les campagnes d'attaques DDoS dans leur élan. Visitez akamai.com/ddos-briefing pour demander votre rapport personnalisé sur les menaces DDoS et bénéficier des informations qui vous aideront à protéger votre entreprise.