KASPERSKY DDOS PROTECTION

Découvrez comment Kaspersky Lab défend les entreprises contre les attaques DDoS

▶ LES ENTREPRISES SONT DEVENUES LA CIBLE DES CYBER-CRIMINELS.

Si votre entreprise a déjà subi une attaque en déni de service distribué (DDoS), vous savez déjà que cela peut représenter des coûts considérables, aussi bien en termes financiers qu'en termes de réputation. Même si votre entreprise a eu la chance d'échapper à l'attention des cyber-criminels et des pirates qui lancent ces attaques, les perspectives d'avenir risquent de ne pas être positives.

LE VOLUME ET LA GRAVITÉ DES ATTAQUES NE CESSENT D'AUGMENTER

Malheureusement, depuis quelques années, le coût du lancement d'une attaque DDoS a nettement chuté, ce qui signifie que les attaques sont plus nombreuses que jamais. Dans le même temps, les attaques se font également plus complexes et se situent à une échelle qui risque de faire saturer la bande passante de communications de l'entreprise ciblée en quelques secondes seulement, anéantissant presque instantanément les processus internes vitaux et désactivant totalement la présence en ligne de la victime.

Pour les entreprises de toutes tailles qui comptent sur leur infrastructure informatique et sur leur site Web pour assurer la plupart de leurs processus stratégiques, les interruptions prolongées qui peuvent être occasionnées par les attaques DDoS ne sont pas envisageables. De toute évidence, compte tenu du volume, de l'ampleur et de la gravité des attaques modernes, l'entreprise ne peut plus se permettre d'attendre que son infrastructure soit attaquée pour se protéger des attaques DDoS. En fait, les entreprises - ainsi que les organisations du secteur public - doivent prendre conscience des menaces et veiller à mettre en place des mesures adéquates contre les attaques DDoS.

« UN HOMME AVERTI EN VAUT DEUX »

Chaque entreprise se doit de disposer d'une stratégie anti-DDoS, prête à être mise en action dès qu'une attaque est détectée. Dans ces conditions, en cas d'attaque, l'entreprise sera en mesure d'en atténuer les effets - rapidement - afin de :

- Réduire au minimum les périodes d'inactivité des infrastructures et processus stratégiques
- Permettre aux clients de continuer à accéder aux services en ligne
- Maintenir la productivité des employés
- Minimiser les conséquences pour sa réputation

▶ MÉTHODES D'ATTAQUES DDOS

Les cyber-criminels et les pirates utilisent différentes techniques pour mettre en œuvre des attaques DDoS qui désactivent ou surchargent l'infrastructure informatique de l'entreprise prise pour cible.

ATTAQUES VOLUMÉTRIQUES

Ces attaques sont de plus en plus courantes. En générant des niveaux de trafic considérable, ces attaques saturent la capacité de la connexion Internet de l'entreprise victime et désactivent ou retardent toutes les activités en ligne.

ATTAQUES DE NIVEAU 7 (APPLICATIVE)

Les attaques contre la couche application cherchent à provoquer la panne des serveurs qui exécutent les applications vitales, tels que les serveurs Web dont dépend la présence en ligne de la victime.

ATTAQUES CONTRE LES RESSOURCES (INFRASTRUCTURE)

Les attaques qui visent à désactiver l'équipement réseau et / ou les systèmes d'exploitation des serveurs risquent d'interrompre le fonctionnement des processus essentiels de l'entreprise.

ATTAQUES HYBRIDES

Les cyber-criminels lancent également des attaques complexes qui combinent plusieurs méthodes, notamment des techniques volumétriques, contre la couche d'application et contre l'infrastructure.

▶ LA SOLUTION LA PLUS COMPLETE DE DÉFENSE ET D'ATTÉNUATION

Kaspersky DDoS Protection apporte une solution de protection et d'atténuation complète et intégrée contre les attaques DDoS, qui tient compte de chaque étape nécessaire pour défendre votre entreprise. De l'analyse continue de tout votre trafic en ligne aux alertes signalant la présence possible d'une attaque, puis de la réception de votre trafic redirigé au nettoyage de votre trafic et à la restitution d'un trafic « propre », Kaspersky Protection DDoS vous offre tout ce dont votre entreprise a besoin pour se défendre et atténuer les effets de tous les types d'attaques DDoS.

KASPERSKY DDOS PROTECTION COMPREND :

- La sonde d'analyse Kaspersky Lab, qui fonctionne au sein de votre infrastructure informatique
- Les services de notre réseau mondial de « centres de nettoyage » du trafic de données
- L'assistance de notre Centre des opérations de sécurité et d'experts de la protection contre les attaques DDoS
- Des analyses et rapports détaillés post-attaque

▶ COMMENT FONCTIONNE KASPERSKY DDOS PROTECTION

La sonde d'analyse Kaspersky Lab collecte des informations concernant l'ensemble de votre trafic de communications – 24 heures sur 24, 7 jours sur 7 et 365 jours par an. La sonde est installée aussi près que possible de la ressource que vous souhaitez protéger, et elle recueille constamment des données concernant votre trafic, notamment :

- Données d'en-tête
- Types de protocole
- Nombre d'octets envoyés et reçus
- Nombre de paquets envoyés et reçus
- Activités et comportements de chaque visiteur de votre site Web
- Toutes les métadonnées concernant votre trafic

Toute ces informations sont envoyées aux serveurs de Kaspersky Lab dans le cloud, où elles sont analysées afin de nous permettre de créer des profils de comportement des visiteurs et des profils de votre trafic typique, sans oublier la manière dont ce trafic peut varier selon l'heure du jour et le jour de la semaine, et les conséquences que peuvent avoir des événements spéciaux sur vos modèles de trafic. Une fois qu'ils disposent de cette compréhension détaillée de vos « conditions normales de trafic » et du « comportement normal de vos visiteurs », nos serveurs basés dans le cloud sont à même d'analyser vos conditions de trafic en direct - en temps réel - et d'identifier rapidement les anomalies qui peuvent indiquer qu'une attaque a été lancée contre votre entreprise.

En outre, nos experts de la surveillance des menaces observent en permanence le paysage des menaces DDoS, afin d'identifier les nouvelles attaques. Cette veille spécialisée contribue à garantir aux clients de Kaspersky Lab qu'ils bénéficieront d'une réponse rapide dès le lancement d'une attaque.

ÉVITER LES FAUSSES ALARMES… PUIS NETTOYER VOTRE TRAFIC

Dès qu'une attaque potentielle contre votre entreprise est identifiée par nos serveurs ou nos experts de la surveillance, le Centre d'opérations de sécurité de Kaspersky Lab reçoit une alerte. Pour contribuer à éviter les fausses alarmes - et les perturbations inutiles pour votre entreprise - les ingénieurs de Kaspersky Lab vérifient que l'anomalie du trafic ou le comportement suspect résulte d'une attaque DDoS. Ensuite, nos ingénieurs contactent immédiatement votre entreprise, afin de vous recommander de rediriger votre trafic vers notre réseau de centres de nettoyage.

Au cours de l'attaque, alors que l'ensemble de votre trafic passe désormais par l'un de nos centres de nettoyage :

- Votre infrastructure n'est plus surchargée par le volume de « trafic indésirable »
- Notre processus de nettoyage élimine l'ensemble du trafic indésirable
- Le trafic légitime vous est renvoyé depuis notre réseau de centres de nettoyage

… et l'ensemble du processus est totalement transparent pour vos employés et vos clients.

LA CONFIGURATION DE LA PROTECTION EST UNE OPÉRATION RAPIDE ET FACILE

Lorsque vous choisissez Kaspersky DDoS Protection, vous avez quelques tâches de configuration à réaliser pour que votre surveillance 24h24, 7 jours sur 7 (et vos canaux de communication concernant les « attaques en direct ») soient mis en place. Kaspersky Lab et ses partenaires peuvent s'occuper de tout ou une partie du processus de configuration, selon vos besoins.

Si vous avez besoin d'une solution clé en main, Kaspersky Lab et ses partenaires peuvent se charger de la grande majorité des procédures de configuration, notamment :

- Installation de la sonde sur votre site
- Configuration de la redirection du trafic vers nos centres de nettoyage
- Mise en place de la livraison d'un trafic « propre » à votre entreprise

... il vous suffit alors de fournir un canal Internet distinct vers la sonde, afin de permettre à Kaspersky DDoS Protection de continuer à recueillir des données lorsque votre canal Internet principal est désactivé par une attaque.

LE CAPTEUR – LA SURVEILLANCE 24H24, 7 JOURS SUR 7

La sonde Kaspersky Lab est fournie avec un système d'exploitation standard Ubuntu Linux. Dans la mesure où la sonde fonctionne sur un serveur x86 standard, ou sur une machine virtuelle*, vous n'avez pas à entretenir de matériel particulier.

Comme la sonde est connectée au port SPAN (Switched Port Analyzer), elle bénéficie de la meilleure vue possible sur le trafic qui entre et sort de la ressource qu'elle protège.

Dès que la sonde est connectée à votre infrastructure, elle commence à recueillir les données sur votre trafic entrant et sortant. Elle analyse chaque paquet d'en-têtes et envoie les informations aux serveurs Kaspersky DDoS Protection dans le cloud, où nous élaborons des profils statistiques du « comportement normal du trafic » et du « comportement normal des visiteurs » dans votre entreprise.

Afin de préserver la confidentialité de vos communications et de vous aider à respecter vos engagements de conformité, la sonde ne capture pas le contenu des messages dans votre trafic de communications. La sonde recueille uniquement des données concernant votre trafic : ainsi, la confidentialité de vos messages n'est jamais compromise par les processus de Kaspersky DDoS Protection.

* La machine virtuelle doit satisfaire ou dépasser les exigences de performance minimales spécifiées par Kaspersky Lab.

REDIRECTION DU TRAFIC

Dans des conditions de fonctionnement normales, tandis que les serveurs Kaspersky DDoS Protection basés dans le cloud recherchent le moindre signe d'une attaque DDoS, votre trafic est orienté directement vers le réseau de votre entreprise. Votre trafic n'est redirigé vers notre réseau mondial de centres de nettoyage que lorsqu'une attaque a été détectée et que votre entreprise a confirmé son souhait de rediriger son trafic.

Kaspersky DDoS Protection vous offre le choix entre plusieurs méthodes de redirection :

- Le protocole BGP (Border Gateway Protocol)
- Domain Name System (DNS)

LES TUNNELS GRE (GENERIC ROUTING ENCAPSULATION, OU ENCAPSULATION GÉNÉRIQUE DE ROUTAGE)

Quelle que soit la méthode de redirection la mieux adaptée à votre entreprise, les tunnels GRE permettent d'activer la communication entre votre passerelle de frontière (ou votre routeur) et chaque centre de nettoyage Kaspersky DDoS Protection.

En cas d'attaque DDoS lancée contre votre entreprise, l'ensemble de votre trafic peut être redirigé vers l'un de nos centres de nettoyage. Les tunnels GRE sont ensuite utilisés pour renvoyer le trafic nettoyé de nos centres de nettoyage vers votre entreprise.

CHOIX ENTRE BGP ET DNS

Le choix de configurer la redirection de votre trafic via BGP ou DNS dépendra en grande partie de la nature de l'infrastructure informatique et de communications de votre entreprise :

- Pour le protocole BGP, vous devez disposer des éléments suivants :
  - Un réseau indépendant de fournisseurs, contenant les ressources que vous souhaitez protéger
  - Un système autonome

  … la plupart des grandes entreprises sont en mesure de satisfaire à ces critères.

- Pour le DNS, vous devrez être capable de :
  - Gérer votre propre zone de domaine pour les ressources que vous cherchez à protéger
  - Définir la durée de vie (TTL) des enregistrements DNS sur 5 minutes

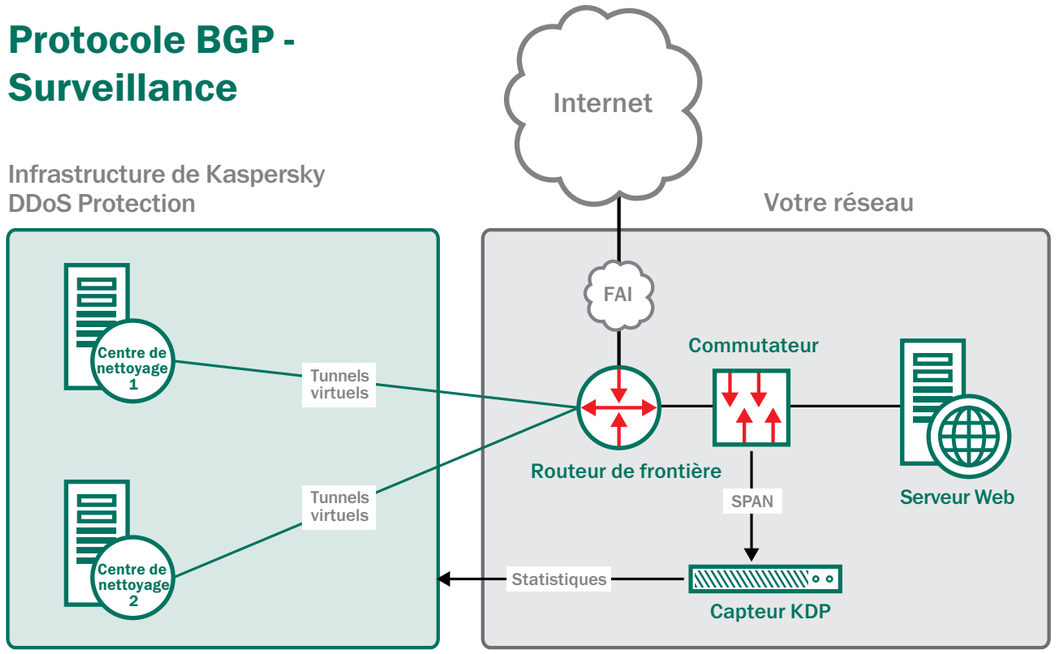
Généralement, lors d'une attaque, la méthode BGP est celle qui redirige le trafic le plus rapidement. C'est la raison pour laquelle la solution BGP est souvent privilégiée par la plupart des entreprises.

▶ COMMENT FONCTIONNE LA REDIRECTION BGP

SURVEILLANCE

En mode surveillance, l'ensemble de votre trafic est envoyé directement à votre entreprise. Toutefois, les tunnels GRE fonctionnent « en direct » : nos routeurs et nos routeurs BGP échangeant fréquemment des informations d'état... ainsi, les centres Kaspersky DDoS Protection sont prêts à recevoir votre trafic redirigé chaque fois que cela est nécessaire.

Protocole BGP - Surveillance

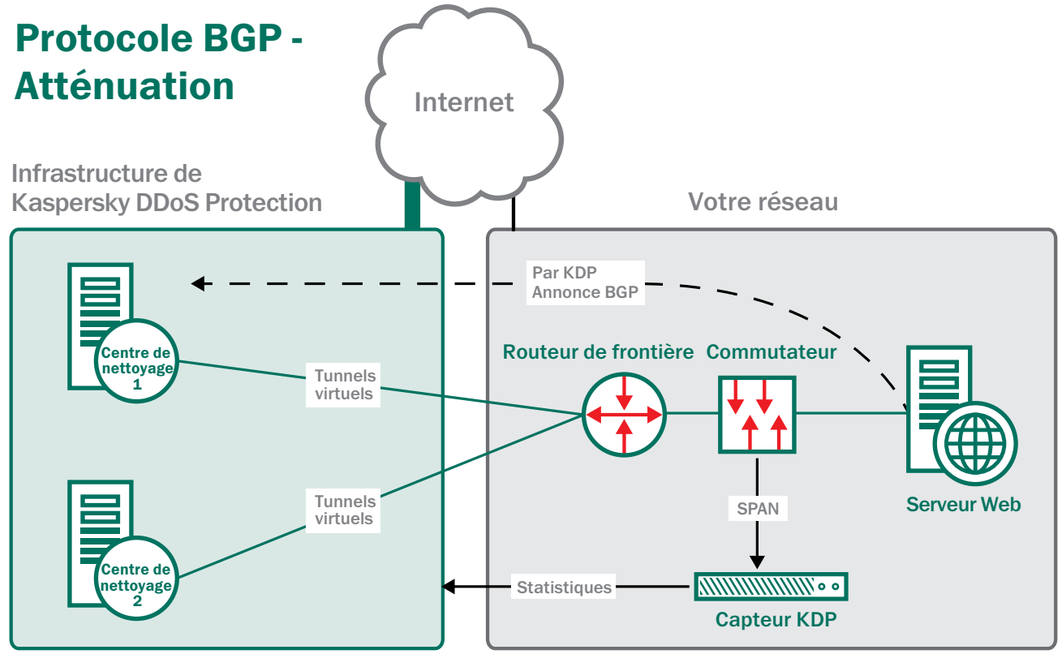


AU COURS D'UNE ATTAQUE

Lorsqu'une anomalie de trafic est identifiée par la sonde Kaspersky Lab, et que le début de l'attaque est confirmé par les ingénieurs de Kaspersky Lab, vous pouvez choisir de rediriger l'ensemble de votre trafic vers un centre de nettoyage Kaspersky DDoS Protection.

Tout au long de l'attaque, la sonde Kaspersky Lab continuera à recueillir des informations et à les envoyer pour analyse aux serveurs Kaspersky DDoS Protection basés dans le cloud.

Protocole BGP - Atténuation



APRÈS UNE ATTAQUE

Une fois que l'attaque a cessé, votre trafic est à nouveau envoyé directement vers votre entreprise. La sonde continue de recueillir des données à propos de votre trafic, et transmet constamment ces données à nos serveurs basés dans le cloud, ce qui nous permet d'affiner continuellement nos profils de comportements dans vos conditions de trafic normales.

Les tunnels restent actifs, échangeant des informations d'état entre vos routeurs et ceux de Kaspersky Lab, afin de permettre à Kaspersky DDoS Protection d'être prêt à intervenir si une autre attaque est lancée contre votre entreprise et que vous choisissez à nouveau de rediriger votre trafic.

Les experts de Kaspersky Lab vous fourniront également une analyse détaillée post-attaque et vous expliqueront avec précision :

- Ce qui s'est passé au cours de l'attaque
- Combien de temps l'attaque a duré
- Comment la solution Kaspersky DDoS Protection a traité l'attaque

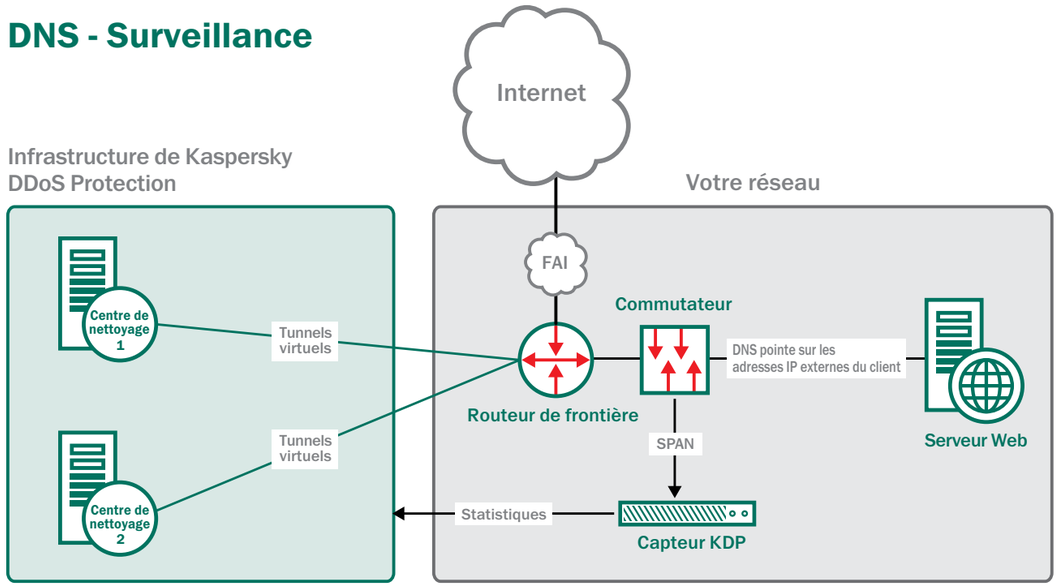
▶ COMMENT FONCTIONNE LA REDIRECTION DNS

SURVEILLANCE

Lors de la configuration initiale, Kaspersky Lab alloue l'une des adresses IP de son pool Kaspersky DDoS Protection à votre entreprise. Cette adresse sera utilisée en cas d'attaque.

En mode surveillance, l'ensemble de votre trafic est envoyé directement à votre entreprise, via son ou ses adresse(s) IP normale(s). Toutefois, les tunnels GRE fonctionnent « en direct » : vos routeurs et nos routeurs échangeant fréquemment des informations d'état… ainsi, les centres Kaspersky DDoS Protection sont prêts à recevoir votre trafic redirigé chaque fois que cela est nécessaire.

DNS - Surveillance

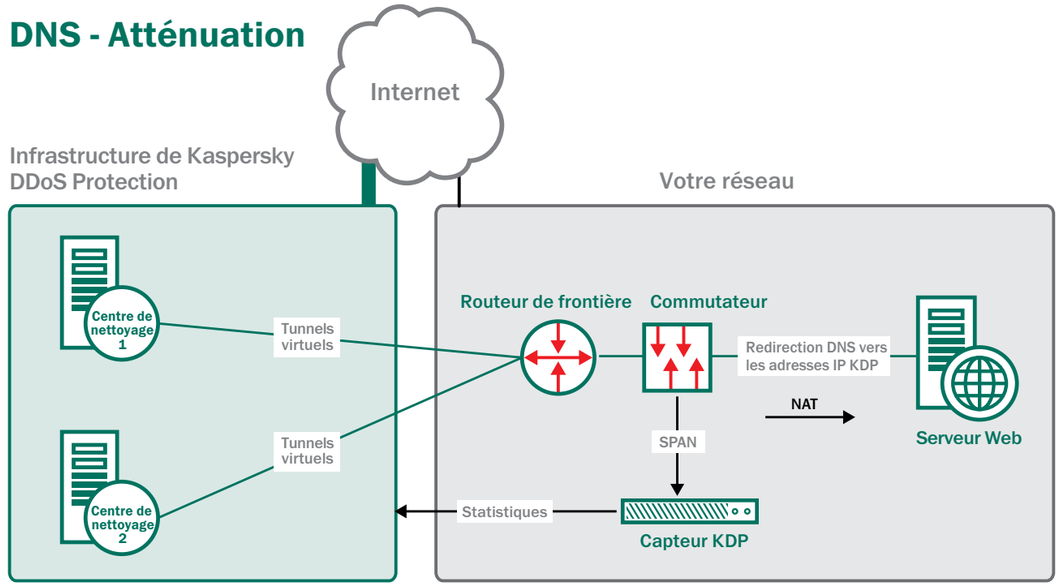


AU COURS D'UNE ATTAQUE

Lorsqu'une anomalie trafic est identifiée par la sonde Kaspersky Lab, et que le début d'une attaque est confirmé par les ingénieurs de Kaspersky Lab, vous modifiez simplement l'adresse IP dans l'enregistrement A de DNS… afin que votre entreprise utilise désormais l'adresse IP de Kaspersky DDoS Protection qui vous a été allouée lors de la configuration initiale. En même temps, comme les pirates peuvent attaquer directement votre adresse IP, votre FAI doit bloquer l'ensemble du trafic orienté vers votre adresse IP d'origine, à l'exception des communications avec l'infrastructure de DDoS Protection de Kaspersky Lab.

Une fois que vous avez modifié votre adresse IP, l'ensemble de votre trafic est réacheminé vers les centres de nettoyage de Kaspersky Lab. Le trafic « propre » est ensuite renvoyé vers votre entreprise, depuis nos centres de nettoyage, via les tunnels GRE.

DNS - Atténuation



APRÈS UNE ATTAQUE

Une fois que l'attaque a cessé, vous pouvez débloquer votre adresse IP initiale et modifier l'enregistrement A du DNS afin que votre trafic soit à nouveau envoyé directement vers votre entreprise.

La sonde Kaspersky Lab continue de recueillir des données sur votre trafic, et les transmet constamment à nos serveurs basés dans le cloud, afin de nous permettre d'affiner constamment nos profils de comportement en fonction de vos conditions de trafic normales.

Les tunnels restent actifs, échangeant des informations d'état entre vos routeurs et les routeurs de Kaspersky Lab, afin de permettre à Kaspersky DDoS Protection d'être prêt à intervenir si une autre attaque est lancée contre votre entreprise et que vous choisissez à nouveau de rediriger votre trafic.

Les experts de Kaspersky Lab vous fourniront également une analyse détaillée post-attaque et vous expliqueront avec précision :

- Ce qui s'est passé au cours de l'attaque
- Combien de temps l'attaque a duré
- Comment la solution Kaspersky DDoS Protection a traité l'attaque

SURVEILLANCE DES MENACES, POUR UNE DÉFENSE ENCORE PLUS ROBUSTE

Kaspersky DDoS Protection comporte un autre composant de défense important... un composant avec lequel les autres fournisseurs ne peuvent pas rivaliser.

Kaspersky Lab est le seul fournisseur de solutions anti-malware à proposer une solution de protection contre les attaques DDoS, ce qui signifie qu'aucun autre fournisseur de protection anti-DDoS ne peut rivaliser avec l'expertise et l'efficacité du service et de l'infrastructure de notre service de veille stratégique.

Nos experts observent en permanence le paysage des cyber-menaces, afin d'identifier les nouveaux logiciels malveillants et les menaces émergentes sur Internet. Les mêmes experts - et les mêmes méthodes d'avant-garde - sont également utilisés pour surveiller le paysage des menaces DDoS. Cette surveillance spécialisée nous aide à détecter plus précocement les attaques DDoS... afin de permettre à votre entreprise de bénéficier d'une protection plus rapide.

PROTECTION MULTI-NIVEAUX

Grâce à une combinaison unique de surveillance du trafic en continu, d'analyse statistique et d'analyse du comportement, sans oublier notre veille spécialisée et proactive portant sur les attaques DDoS, nous proposons une solution plus rigoureuse de protection contre les attaques DDoS.

DataSheet_DDoS/OCTOBRE2014/FR