KASPERSKY DDoS PROTECTION

Protéger votre entreprise contre les pertes financières et préserver sa réputation avec Kaspersky DDoS Protection

Une attaque par déni de service distribué (DDoS) est l'une des armes les plus populaires figurant dans l'arsenal des cyber-criminels. Elle a pour but d'empêcher les utilisateurs ordinaires d'accéder normalement aux systèmes d'information, tels que les sites Web ou les bases de données. Les attaques DDoS peuvent avoir différents mobiles. Elles peuvent être liées au houliganisme informatique, à des pratiques de concurrence déloyales ou à des projets d'arnaque.

Les DDoS sont fondées sur une structure à plusieurs couches. Elles font appel à ceux qui demandent les attaques, aux créateurs de botnets proposant leurs ressources, aux intermédiaires qui organisent les attaques et s'adressent aux clients, et à ceux qui versent les paiements pour les services fournis. Un nœud de réseau disponible sur Internet peut devenir une cible, qu'il s'agisse d'un serveur spécifique, d'un périphérique de réseau ou d'une adresse mise hors service dans le sous-réseau de la victime.

Il existe deux cas de figure courants pour lancer des attaques DDoS, à savoir l'envoi de demandes directement à la ressource attaquée à partir d'un grand nombre de bots, et le lancement d'une attaque par amplification DDoS par le biais de serveurs publiquement disponibles contenant des vulnérabilités logicielles. Dans le premier cas, les cyber-criminels transforment tout un tas d'ordinateurs en « zombies » contrôlés à distance, qui suivent alors les ordres de leur maître et envoient simultanément des demandes au système informatique de la victime (déployant ainsi une « attaque distribuée »). Il arrive parfois qu'un groupe d'utilisateurs soit recruté par des « hacktivistes », reçoive un logiciel spécial conçu pour lancer des attaques DDoS et soit invité à attaquer une cible précise.

Dans le deuxième cas, c'est-à-dire l'attaque par amplification, des serveurs provenant d'un centre de données peuvent être utilisés à la place des bots. En général, des serveurs publics souffrant de vulnérabilités logicielles servent à l'amplification. À l'heure actuelle, les serveurs DNS (système de nom de domaine) et les serveurs NTP (protocole de temps de réseau) peuvent être employés. Une attaque est amplifiée en falsifiant les adresses IP de retour et en envoyant une demande courte à un serveur qui nécessite beaucoup plus de temps pour répondre. La réponse reçue est envoyée à l'adresse IP falsifiée appartenant à la victime.

Cas de figure d'attaque DDoS

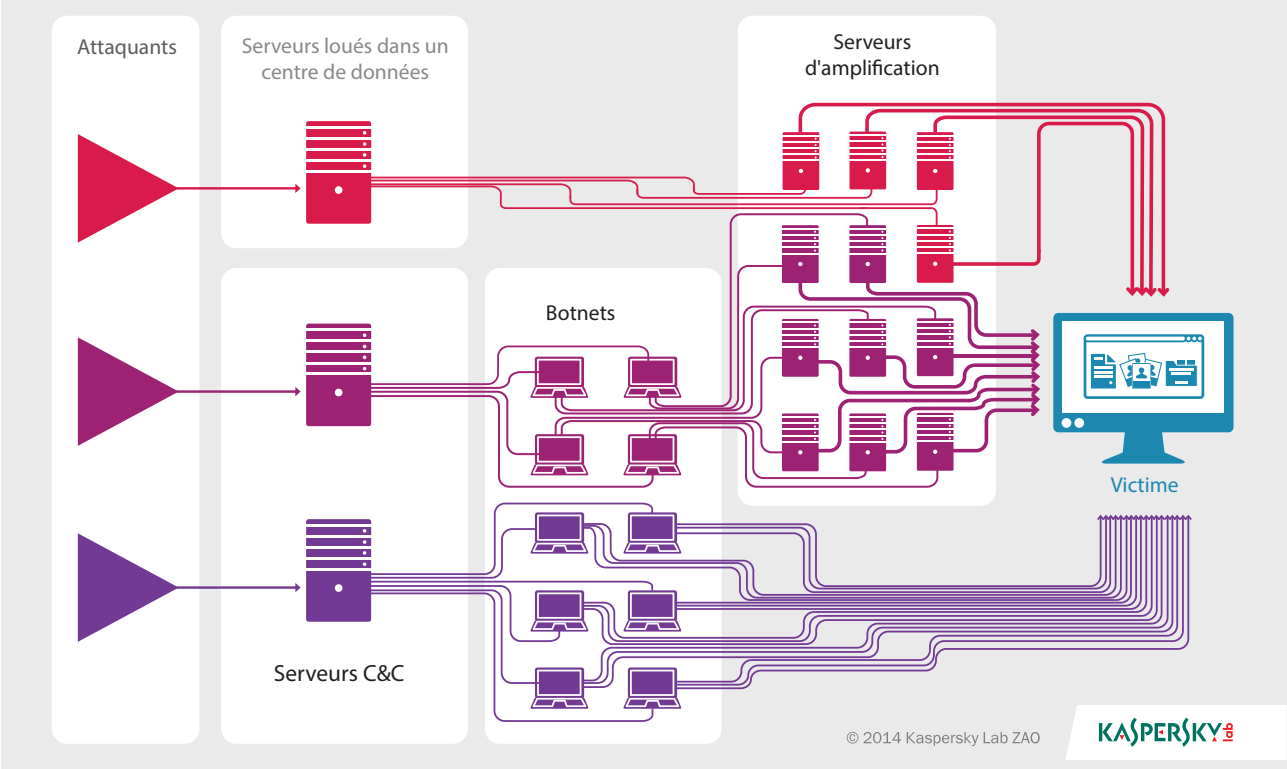

Schéma 1. Diagramme des versions les plus populaires des attaques DDoS

Il existe un autre facteur aggravant la situation encore davantage. Compte tenu de la présence répandue des programmes malveillants et du grand nombre de botnets créés par des cyber-criminels, pratiquement n'importe qui peut lancer ce genre d'attaque. Les cyber-criminels proposent leurs services en annonçant que n'importe qui peut désactiver un site spécifique pour seulement 50 USD par jour. Les paiements sont généralement versés en crypto-monnaie et il est pratiquement impossible de suivre ces flux d'argent.

Les prix étant peu élevés, n'importe quelle ressource en ligne peut être ciblée par une attaque DDoS. Ce ne sont pas seulement les ressources en ligne de grandes et célèbres organisations qui sont visées. Il est plus difficile d'endommager les ressources en ligne appartenant à de grandes entreprises, mais en cas d'indisponibilité de ces dernières, le coût lié aux temps d'arrêt provoqués n'en serait que plus élevé. Hormis les pertes directes issues des opportunités commerciales manquées (p. ex. pour les ventes électroniques), les sociétés peuvent être passibles de sanctions monétaires si elles n'ont pas rempli leurs obligations contractuelles, ou encourir des frais supplémentaires liés aux mesures associées à prendre pour éviter toute autre attaque. Enfin, la réputation d'une société peut être ternie, ce qui peut lui faire perdre des clients actuels ou futurs.

Le coût total dépend de la taille de l'entreprise, du segment sur lequel elle opère et du type de service attaqué. D'après les calculs de la société d'analyse IDC, une seule heure de temps d'arrêt pour un service en ligne peut coûter de 10 000 à 50 000 dollars USD à une société.

Méthodes de prévention des attaques DDoS

Il existe des dizaines de sociétés qui proposent des services de protection contre les attaques DDoS. Certaines d'entre elles installent des équipements dans l'infrastructure d'information du client, d'autres utilisent les fonctionnalités disponibles chez les fournisseurs ISP, et d'autres encore font passer le trafic par des centres de nettoyage dédiés. Cependant, toutes ces approches suivent le même principe : le trafic indésirable, c'est-à-dire le trafic créé par les cyber-criminels, est filtré, puis éliminé.

L'installation d'équipements de filtrage côté client est considéré comme la méthode la moins efficace. En premier lieu, la société doit avoir des employés spécialement formés pour maintenir les équipements et les régler, ce qui génère des frais supplémentaires. En deuxième lieu, cette méthode est efficace seulement pour contrer les attaques visant le service et est impuissante pour prévenir les attaques visant à asphyxier le canal Internet. Un service opérationnel n'a aucune utilité s'il est impossible d'y accéder en ligne. Les attaques DDoS étant de plus en plus populaires, il est désormais bien plus facile de surcharger un canal de connexion.

Si le filtre est installé du côté fournisseur, le trafic devient plus fiable car le canal Internet est plus large et il est bien moins aisé de le boucher. En revanche, les fournisseurs ne se spécialisent pas dans les services de sécurité et, comme ils détectent seulement le trafic notoirement indésirable, ils ignorent souvent les attaques plus subtiles. Pour mettre en œuvre une analyse approfondie suivie d'une réponse rapide, il est nécessaire d'avoir le savoir-faire et l'expérience nécessaires. Par ailleurs, ce genre de protection crée un lien de dépendance entre le client et un fournisseur spécifique, ce qui complique les choses si le client doit utiliser un canal de sauvegarde de données ou s'il souhaite changer de fournisseur.

C'est pour cette raison qu'il convient de considérer les centres de traitement spécialisés qui mettent en œuvre diverses méthodes de filtrage de trafic comme la méthode la plus efficace pour neutraliser les attaques DDoS.

Kaspersky Lab DDoS Protection

Kaspersky DDoS Protection est une solution qui vous protège contre tous les types d'attaques DDoS à l'aide d'une infrastructure distribuée de centres de nettoyage de données. La solution fait appel à différentes méthodes combinées, notamment le filtrage du trafic côté fournisseur, l'installation d'un appareil contrôlé à distance pour analyser le trafic près de l'infrastructure du client et l'utilisation de centres de nettoyage spécialisés disposant de filtres flexibles. En outre, les experts de Kaspersky Lab surveillent en permanence le travail réalisé par la solution, ce qui leur permet de détecter une attaque le plus tôt possible et de modifier les filtres en conséquence.

Kaspersky DDoS Protection en mode actif

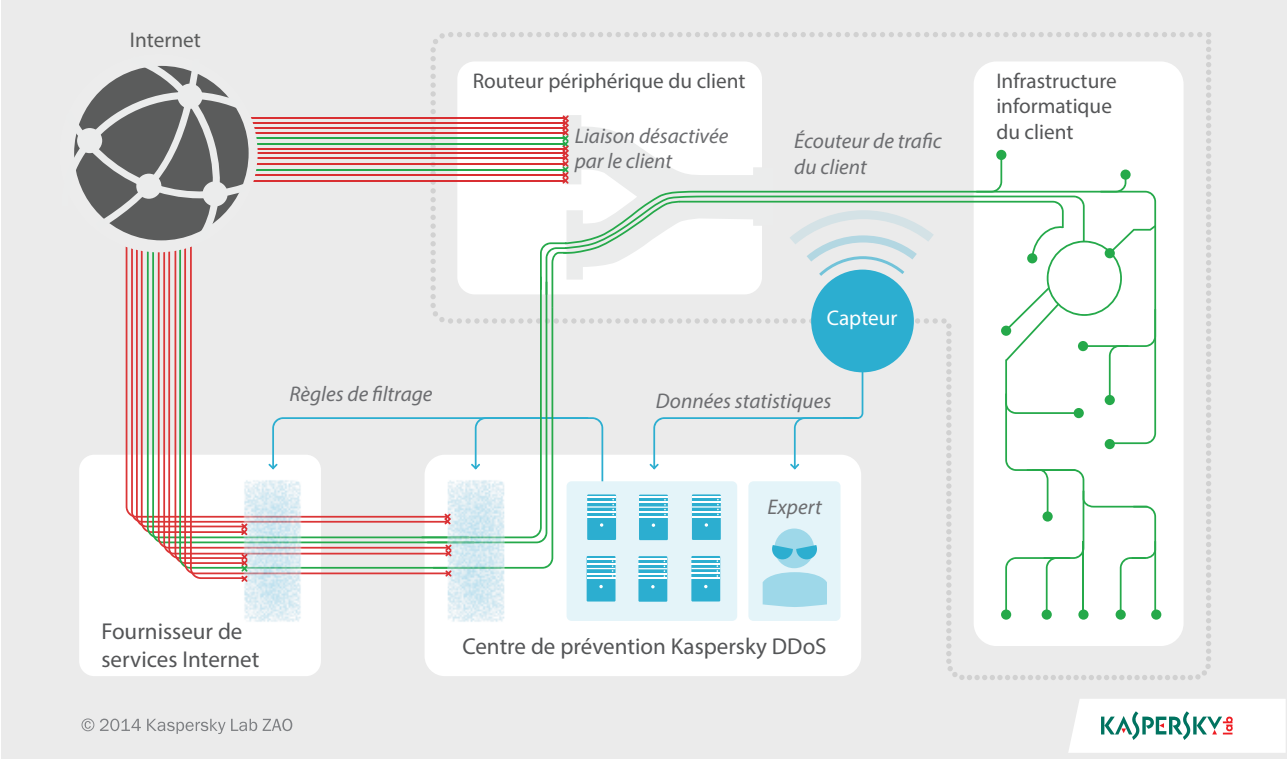

Schéma 2. Kaspersky DDoS Protection : diagramme de fonctionnement

L'arsenal de Kaspersky Lab

Cela fait plus de dix ans que Kaspersky Lab combat toutes sortes de menaces en ligne. Pendant cette période, les analystes de Kaspersky Lab ont acquis un niveau d'expertise inégalé et ils ont obtenu une compréhension approfondie du mode de fonctionnement des attaques DDoS. Les experts de la société sont à l'affût des tous derniers développements en cours sur Internet, analysent les dernières méthodes utilisées pour lancer les cyber-attaques, et améliorent les outils de protection existants. Grâce à ce savoir-faire, il est possible d'identifier une attaque DDoS dès qu'elle se produit et avant qu'elle n'ait envahi la ressource en ligne ciblée.

Le deuxième élément de la technologie de Kaspersky DDoS Protection est le capteur installé près de l'infrastructure informatique du client. Le capteur est un élément logiciel exécuté sur le système d'exploitation Ubuntu et nécessitant un serveur x86 standard. Il analyse les types de protocoles utilisés, le nombre d'octets et de paquets de données envoyés, le comportement du client sur le site Web, notamment au niveau des métadonnées ou des informations sur les données envoyées. Il ne redirige pas le trafic, ne modifie pas et n'analyse pas le contenu des messages. Les statistiques sont alors transmises à l'infrastructure de Kaspersky DDoS Protection dans le cloud, qui crée un profil à partir de ces statistiques pour chaque client en fonction des métadonnées recueillies. En réalité, ces profils sont des registres des tendances d'échange d'informations pour chaque client. Les changements des temps d'utilisation habituels sont enregistrés. Le trafic est ensuite analysé et, quand le comportement du trafic diffère du profil basé sur les statistiques, la présence potentielle d'une attaque est identifiée.

Les centres de nettoyage constituent l'élément de base de Kaspersky DDoS Protection. Ils se situent sur les principales lignes dorsales d'Internet, notamment à Francfort et à Amsterdam. Kaspersky Lab utilise simultanément plusieurs centres de nettoyage pour pouvoir diviser ou rediriger le trafic à nettoyer. Les centres de traitement sont unis au sein d'une infrastructure d'informations en commun dans le cloud et les données sont gardées dans ces limites. Par exemple, le trafic en ligne des clients européens ne quitte pas le territoire européen.

Un autre moyen clé de contrôler le trafic des attaques DDoS consiste à le filtrer du côté fournisseur. L'ISP n'est pas seulement un fournisseur de canal Internet, car il fait équipe avec Kaspersky Lab dans le cadre d'un partenariat technologique. De ce fait, Kaspersky DDoS Protection peut éliminer le trafic indésirable le plus couramment utilisé dans les attaques DDoS aussi près de son point d'origine que possible. Cela empêche les différents flux de s'unir en une seule attaque puissante tout en soulageant les centres de nettoyage, qui peuvent alors se concentrer sur le trafic plus sophistiqué.

Outils de redirection du trafic

Pour que la solution de sécurité fonctionne efficacement, il est tout d'abord nécessaire de configurer un canal de connexion entre les centres de nettoyage et l'infrastructure informatique du client. Dans Kaspersky DDoS Protection, ces canaux sont disposés en conformité avec le protocole Encapsulation générique de routage. Ils sont utilisés pour créer un tunnel virtuel entre le centre de nettoyage et les équipements du réseau client. Ce tunnel permet alors de transmettre le trafic nettoyé au client.

La redirection du trafic peut être effectuée selon deux méthodes différentes, soit en annonçant le sous-réseau du client à l'aide d'un protocole de routage dynamique BGP, soit en modifiant le registre DNS en introduisant l'URL du centre de nettoyage. La première méthode est préférable car elle permet de rediriger le trafic bien plus rapidement et garantit une protection contre les attaques ciblant directement une adresse IP spécifique. Cependant, pour faire appel à cette méthode, le client doit avoir une plage d'adresses qui est indépendante du fournisseur, par exemple un bloc d'adresses IP fournies par un bureau d'enregistrement Internet régional.

Les deux méthodes sont très semblables sur le plan de la procédure de redirection. Si la première méthode est utilisée, les routeurs BPG côté client et dans le centre de nettoyage créent une connexion permanente par le biais du tunnel virtuel et, en cas d'attaque, un nouveau passage entre le centre de nettoyage et le client est créé. Quand la deuxième méthode est employée, le client reçoit une adresse IP puisée dans la réserve d'adresses du centre de nettoyage. En cas d'attaque, le client remplace l'adresse IP dans le registre-A DNS par l'adresse IP qui lui a été attribuée par le centre de nettoyage. Après cela, tout le trafic arrivant à l'adresse du client est tout d'abord envoyé au centre de nettoyage. Cependant, pour mettre un terme à l'attaque contre l'ancienne adresse IP, le fournisseur doit bloquer tout le trafic entrant, à l'exception des données provenant du centre de nettoyage.

Mode opératoire

Dans une situation normale, tout le trafic provenant d'Internet arrive directement chez le client. Les actions de protection sont activées dès qu'un signal est reçu du capteur. Dans certains cas, les analystes de Kaspersky Lab peuvent identifier une attaque dès le début et informer le client de la situation. En pareil cas, il est possible de prendre des mesures préventives à l'avance. L'expert des attaques DDoS disponible chez Kaspersky Lab reçoit un signal lui indiquant que le trafic arrivant chez le client ne correspond pas au profil statistique. Si l'attaque est confirmée, le client en est informé et doit donner l'ordre de rediriger le trafic vers les centres de nettoyage (dans certains cas, il est possible de se mettre d'accord avec le client à l'avance pour que la redirection soit automatique).

Dès que les technologies de Kaspersky Lab déterminent la nature de l'attaque, des règles de nettoyage spécifique sont appliquées pour ce type d'attaque et la ressource Web spécifique. Certaines de ces règles, qui sont conçues pour parer les attaques les plus grossières, sont communiquées à l'infrastructure du fournisseur et sont appliquées aux routeurs appartenant au fournisseur. Le reste du trafic est envoyé aux serveurs du centre de nettoyage et filtré selon un certain nombre de signes caractéristiques, tels que les adresses IP, les données géographiques, les informations des en-têtes HTTP, l'exactitude des protocoles et l'échange de paquets SYN, etc.

Le capteur continue à surveiller le trafic arrivant chez le client. S'il reçoit toujours les signes d'une attaque DDoS, le capteur alerte le centre de nettoyage et le trafic fait l'objet d'une analyse approfondie du comportement et des signatures. Ces méthodes permettent de filtrer et d'éliminer le trafic malveillant selon les signatures et, de cette façon un type de trafic spécifique peut être bloqué ou des adresses IP peuvent être bloquées selon certains critères précis observés. Il est ainsi possible de filtrer les attaques les plus sophistiquées, notamment les attaques par flooding HTTP. Ces attaques consistent à imiter un utilisateur accédant à un site Web alors que l'activité est en réalité chaotique, anormalement rapide et en provenance d'une foule d'ordinateurs zombies.

Les experts de Kaspersky Lab surveillent l'ensemble du processus à partir d'une interface dédiée. Si une attaque est particulièrement compliquée ou inhabituelle, l'expert peut intervenir, modifier les règles de filtrage et réorganiser les processus. Les clients peuvent aussi observer le fonctionnement de la solution et le comportement du trafic à partir de leur propre interface.

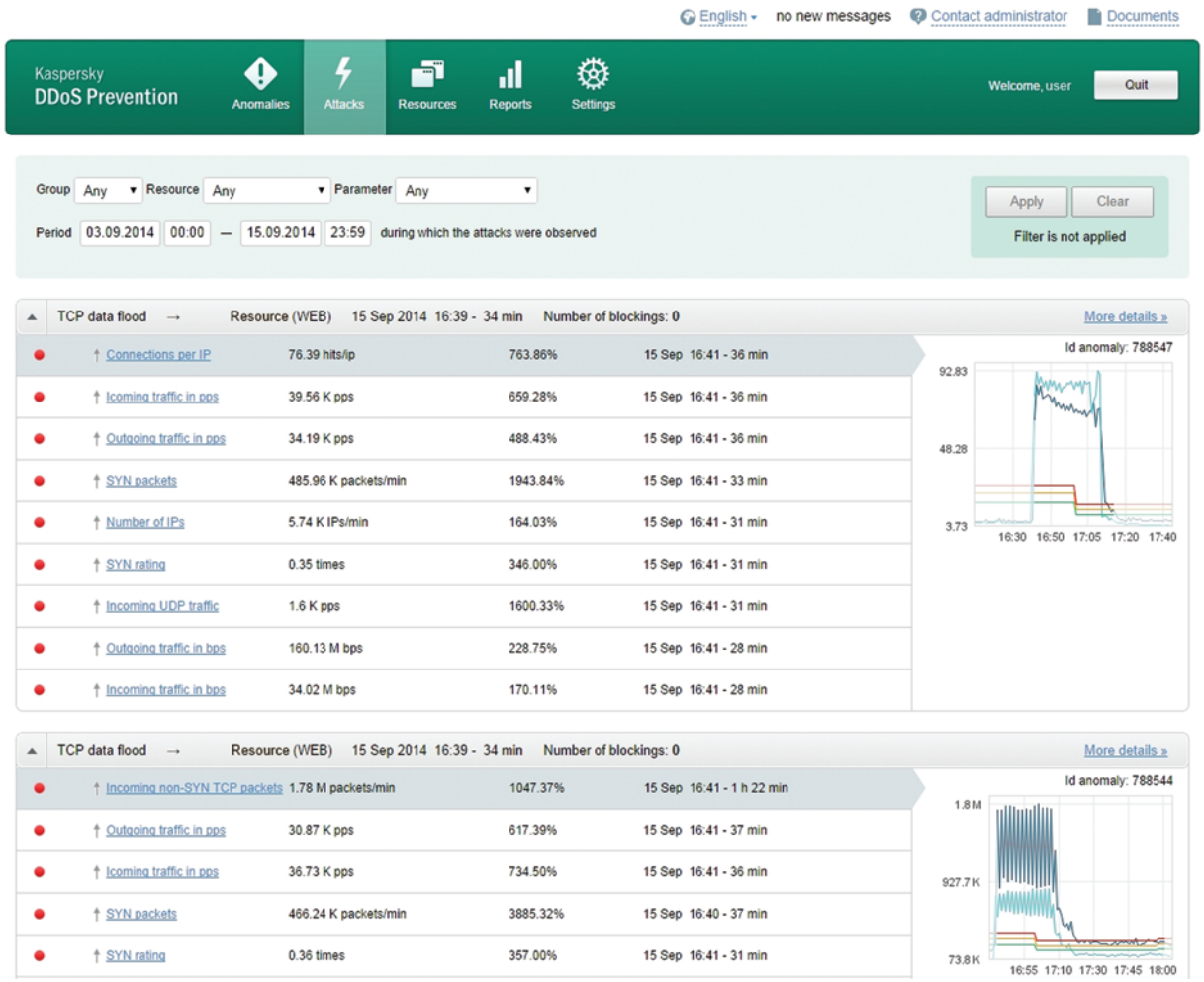

Schéma 3. Capture d'écran de l'interface du client

Quand l'attaque prend fin, le trafic est redirigé vers les serveurs du client. Kaspersky DDoS Protection repasse en mode veille et le client reçoit un rapport détaillé sur l'attaque, qui explique notamment la façon dont elle s'est développée et présente des paramètres mesurables, ainsi que la distribution géographique des sources de l'attaque.

Avantages de l'approche adoptée par Kaspersky Lab

- L'envoi du trafic vers les centres de nettoyage de Kaspersky Lab pendant une attaque et le filtrage du trafic côté fournisseur sont déjà des mesures qui permettent de réduire considérablement les frais encourus par le client.
- Des règles de filtrage sont élaborées individuellement pour chaque client en fonction de la nature des services en ligne à protéger.
- Les experts de Kaspersky Lab surveillent le processus et modifient rapidement les règles de filtrage quand cela s'avère nécessaire.
- La collaboration étroite entre les experts de Kaspersky DDoS Protection et les développeurs de Kaspersky Lab permet d'adapter la solution avec souplesse et avec rapidité face à l'évolution de la situation.
- Pour assurer le plus haut niveau possible de fiabilité, Kaspersky Lab utilise seulement des équipements et des fournisseurs de service européens dans les pays européens.
- Kaspersky Lab a accumulé une vaste expérience dans le cadre de l'application de cette technologie en Russie, où il a su protéger des établissements financiers de premier plan, des agences commerciales, des organismes gouvernementaux, des magasins en ligne, etc.

Mars 15/Global

www.kaspersky.com/fr