Barracuda®

Défense contre les attaques DDoS basées sur les applications à l'aide du pare-feu Barracuda Web Application Firewall

Livre blanc

Synthèse

Dans le passé, les attaques DDoS étaient en grande partie basées sur le volume et visaient à submerger le réseau en utilisant un faux trafic UDP, TCP SYN ou ICMP. Divers fournisseurs ont proposé des solutions contre ces attaques, notamment des fournisseurs d'appliances de périphérie et de services tels que les FAI, le cloud et les plateformes de nettoyage CDN. Cependant, les plateformes d'attaque d'aujourd'hui ont évolué et comportent des attaques DDoS de couche application ciblant les serveurs de noms de domaine et de sites Web. Selon Stratecast, les attaques DDoS spécifiques aux applications augmentent chaque année de trois chiffres1 et Gartner estime que les attaques de couche application constitueront 25 % de toutes les attaques DDoS en 2013.2

Cette croissance est due au fait que les organisations sont mal préparées à lutter contre les DDoS d'application. Beaucoup d'entre elles recherchent des solutions à partir de leurs pare-feu de périphérie existants, qui ont une visibilité limitée sur la couche application. De plus, du point de vue de l'attaquant, les attaques DDoS d'application nécessitent beaucoup moins de ressources et peuvent être plus furtives. Ils peuvent rendre les services d'application inaccessibles discrètement, bien que l'infrastructure réseau puisse demeurer réactive.

La visibilité et le contrôle du trafic au niveau de l'application sont des éléments essentiels d'une stratégie de défense en couches pour lutter efficacement contre les attaques DDoS à plusieurs volets. Les solutions de couche réseau ayant évolué avec des attaques volumétriques ne peuvent pas détecter les attaques de couche application. Elles n'ont pas une connaissance approfondie des protocoles d'application. De plus, elles ne terminent pas les sessions d'application, n'en prennent pas le contrôle activement et ne les désinfectent pas. Le pare-feu Barracuda Web Application Firewall fournit une solution de couche application virtualisée sur site combinant des informations situationnelles en temps réel et des informations historiques, afin d'atténuer les DDoS d'application.

Botnets et DDoS de couche application

Les botnets sont des réseaux de machines infectées par des logiciels malveillants, saisies par des serveurs appelés serveurs de commande et de contrôle (C&C). Auparavant, la plupart des PC étaient infectés, mais les appareils mobiles et les machines basées sur le cloud sont également de plus en plus ciblés. Une fois qu'une machine est infectée par le logiciel malveillant, la victime fait partie du botnet. Un logiciel malveillant de botnet sophistiqué, tel que Mebroot, prend le contrôle complet de la machine en remplaçant la zone d'amorçage (MBR), ce qui lui permet de se charger avant le système d'exploitation et d'éviter d'être détecté par les outils antivirus.

La communication avec les serveurs C&C s'effectue sur des canaux secrets à l'aide d'un chiffrement propriétaire, mais en utilisant des ports communs pour traverser les pare-feu. Les serveurs C&C emploient des techniques d'évasion telles que le flux rapide de domaine et l'hébergement P2P pour couvrir leurs traces.

Les criminels exploitant des botnets, connus sous le nom de botmasters, envoient des commandes au botnet via les serveurs C&C, afin d'effectuer leurs tâches néfastes, telles que les campagnes de spam, les attaques DDoS, les fraudes aux clics ou la collecte d'informations personnelles telles que les identifiants bancaires ou les numéros de carte de crédit. Dernièrement, les botnets sont couramment utilisés pour les menaces persistantes avancées et la cyberguerre, comme en témoignent les attaques FLAME, DUQU et autres logiciels malveillants.

Il existe un marché souterrain florissant permettant de louer ou de créer des réseaux de botnets. La capture d'écran suivante du tableau de bord du botnet DIY Zeus affiche la répartition géographique des machines infectées :

[1] Entrée dans la prochaine phase de la défense contre les DDoS, avril, 2012 – Stratecast
[2] Armement des services financiers et du commerce électronique contre les principales menaces informatiques de 2013 (G00237376) – Gartner

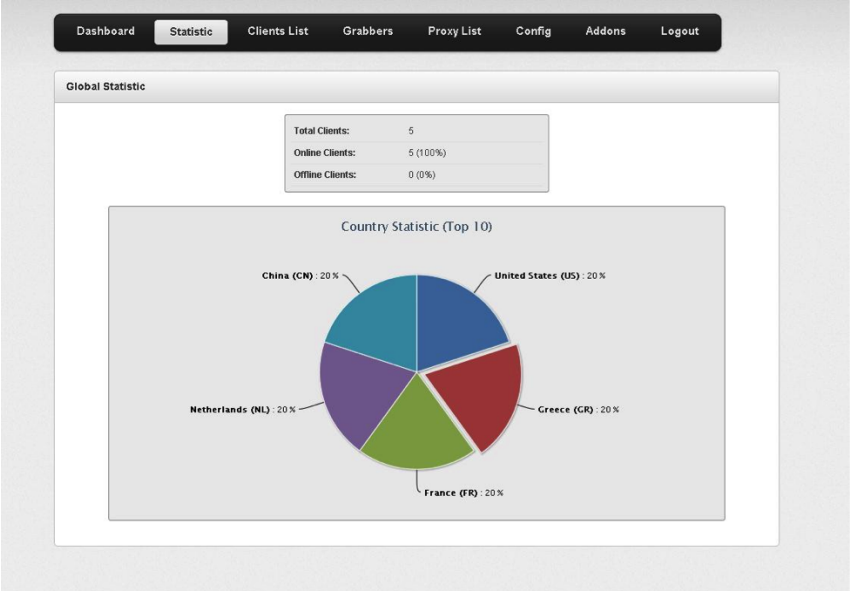


Figure 1 : Capture d'écran du tableau de bord du botnet Zeus

Lutte contre les attaques DDoS de couche application

Les organisations ont également hésité à adopter des systèmes d'atténuation DDoS en raison de préoccupations liées au coût, à l'efficacité et au retour sur investissement. Le pare-feu Barracuda Web Application Firewall est disponible en tant qu'appliance matérielle ou que solution de couche application virtualisée. Il combine des informations situationnelles en temps réel et des informations historiques, afin d'atténuer les DDoS d'application. Il peut atténuer les attaques en fonction des seuils centrés sur l'application, des vérifications de protocole, de l'intégrité de la session, des défis de clients actifs et passifs, des listes noires historiques de réputation des clients, de la géolocalisation et de la détection des temps d'inactivité anormaux. Ceci est intégré dans sa plateforme de pare-feu d'application renforcée, permettant les deux fonctions dans une offre consolidée avec un RSI supérieur et des avantages de conformité. Contrairement aux solutions de fournisseurs de services tarifées en fonction du volume, l'atténuation est indépendante du volume et de la fréquence des attaques, ce qui assure une protection à temps plein à des coûts minimaux.

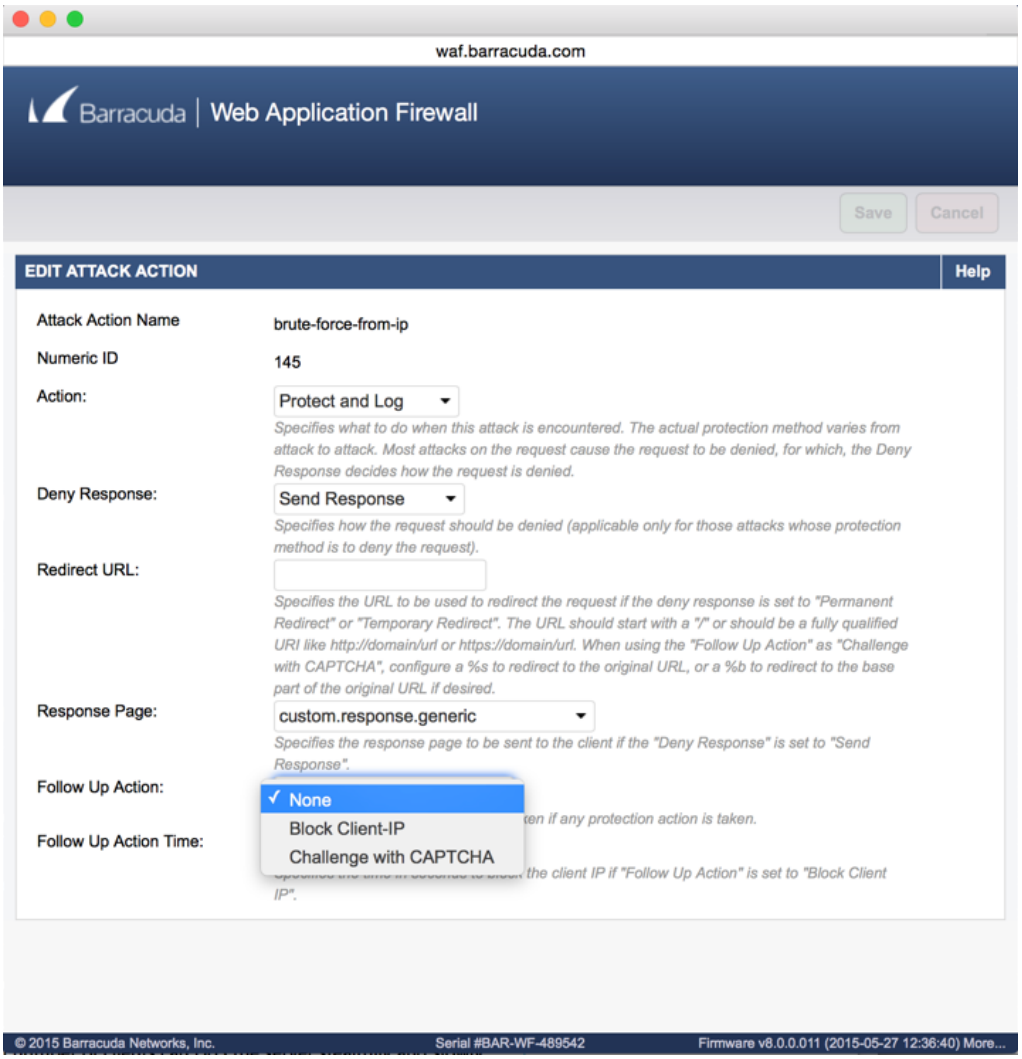
Protection DDoS basée sur les applications du pare-feu Barracuda Web Application Firewall
Détection d'anomalies de protocole pour HTTP
Inondations HTTP GET, POST
« Attaques lentes » HTTP – Slowloris, R-U-Dead-Yet (RUDY), attaque par lecture lente
Protection LOIC, HOIC
Défis JS
Défis CAPTCHA
Contrôles de géolocalisation
Filtrage des proxys anonymes
Inspection SSL sans exporter de clés privées hors site
Flux de réputation IP
Capacité de production excédentaire
Suivi du taux de session
Mises à jour automatiques des signatures et du micrologiciel
Intégration SIEM adaptée au fournisseur

Défense contre les inondations HTTP GET et POST

Les applications comportent souvent plusieurs pages ou interfaces riches en ressources, faisant appel à une base de données, à la mémoire ou à opérations nécessitant beaucoup du processeur, p. ex. des recherches en texte libre. Les botnets ciblent fréquemment ces pages par un flot de demandes afin de faire s'effondrer les applications Web.

La première couche de protection consiste ici à déterminer et à appliquer des seuils de navigation humaine acceptables pour une application particulière. Par exemple, les utilisateurs d'une application Web bancaire cliqueraient sur un maximum de 10 pages par minute.3 De plus, les demandes humaines contiendraient des en-têtes de client valides tels que des cookies et des référents.

Le module de prévention de la force brute du pare-feu Barracuda Web Application Firewall vous permet de définir et d'appliquer de tels seuils. Les clients violant ces seuils peuvent être mis sur liste noire ou mis au défi à l'aide d'un CAPTCHA, afin d'éliminer les faux positifs.



Les attaquants peuvent adapter leurs attaques en réglant les robots individuels de manière à ce qu'ils restent en dessous d'un certain seuil. Cependant, si le nombre de requêtes par bot est réduit de quelques ordres de grandeur (c.-à-d. de 1 000 à 10 requêtes par minute), les attaquants devront augmenter le nombre de bots d'une ampleur similaire. Cette mesure a un effet dissuasif, car elle augmente considérablement le risque de découverte et les coûts économiques du lancement d'une attaque DDoS durable.

[3]Pour obtenir des informations concernant la protection contre les attaques par le canon à ions à orbite basse (LOIC) du groupe Anonymous, veuillez consulter « Défense contre Anonymous à l'aide du pare-feu Barracuda Web Application Firewall »

Défense contre les « attaques lentes » HTTP

Certaines attaques utilisent des clients malveillants s'attardant sur des demandes et des réponses partielles et interagissant au minimum, afin d'empêcher que les délais d'inactivité du serveur n'expirent. Les attaques ralentissent les applications en consommant des ressources système, ce qui empêche finalement de gérer le trafic du serveur. Il s'agit des attaques « faibles et lentes », car un nombre relativement faible de clients peuvent exécuter le serveur de manière furtive et lente, sans consommer de bande passante importante sur le réseau. De telles attaques sont désormais courantes.

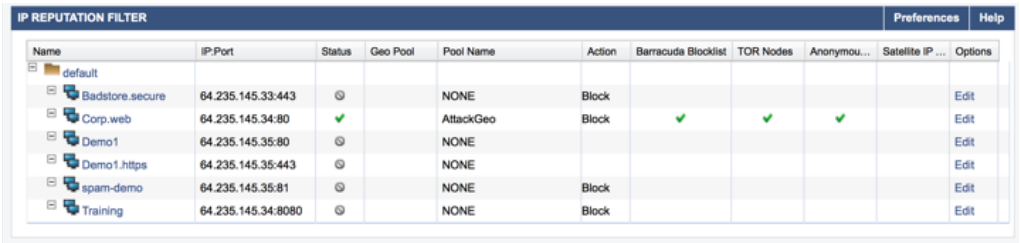
Slowloris est un exemple de client initiant et envoyant des en-têtes HTTP à plusieurs reprises à intervalles réguliers, mais ne terminant jamais complètement leur envoi. Cela empêche de libérer les processus de serveur et les ressources réseau, ce qui conduit finalement à l'effondrement. Du point de vue de la conformité du protocole, il s'agit d'un trafic normal que les appareils basés sur des signatures ou des listes noires ne peuvent pas détecter.

Grâce à son architecture proxy, son protocole et sa connaissance des applications, le pare-feu Barracuda Web Application Firewall peut détecter et bloquer ce trafic anormal. Il utilise un algorithme adaptatif surveillant les seuils de communication incrémentiels et agrégés pour vieillir et fermer les connexions malveillantes de manière agressive, afin de les empêcher de consommer les ressources système.

Filtrage du trafic Botnet basé sur les vérifications d'intégrité côté client

La grande majorité du trafic des applications Web sur les sites Web accessibles sur Internet est accessible par les navigateurs humains, à l'exclusion des indexeurs des moteurs de recherche, tels que Google et Yahoo. La plupart du trafic Web provient d'êtres humains utilisant une plateforme de navigateur commune, telle qu'Internet Explorer, Firefox, Chrome ou Safari. Le trafic provenant des robots se compose souvent de scripts automatisés ne disposant pas des riches capacités de navigation des clients utilisant un navigateur. Par conséquent, il est possible de distinguer le trafic humain du trafic de robots à l'aide de quelques algorithmes heuristiques.

Le pare-feu Barracuda Web Application Firewall fournit deux mécanismes permettant de détecter et de filtrer ces sources de trafic. Premièrement, il détecte les clients suspects en injectant des contrôles côté client, afin d'évaluer le navigateur Web et la session d'application. Il s'agit d'un mécanisme passif de réponse au défi qui n'est pas gênant pour le trafic généré par l'homme, mais qui peut détecter et bloquer le trafic généré par les bots. Le deuxième mécanisme consiste à lancer des défis actifs, des images CAPTCHA pour vérifier les clients humains. Cela peut s'effectuer sans modifier les applications Web côté serveur.

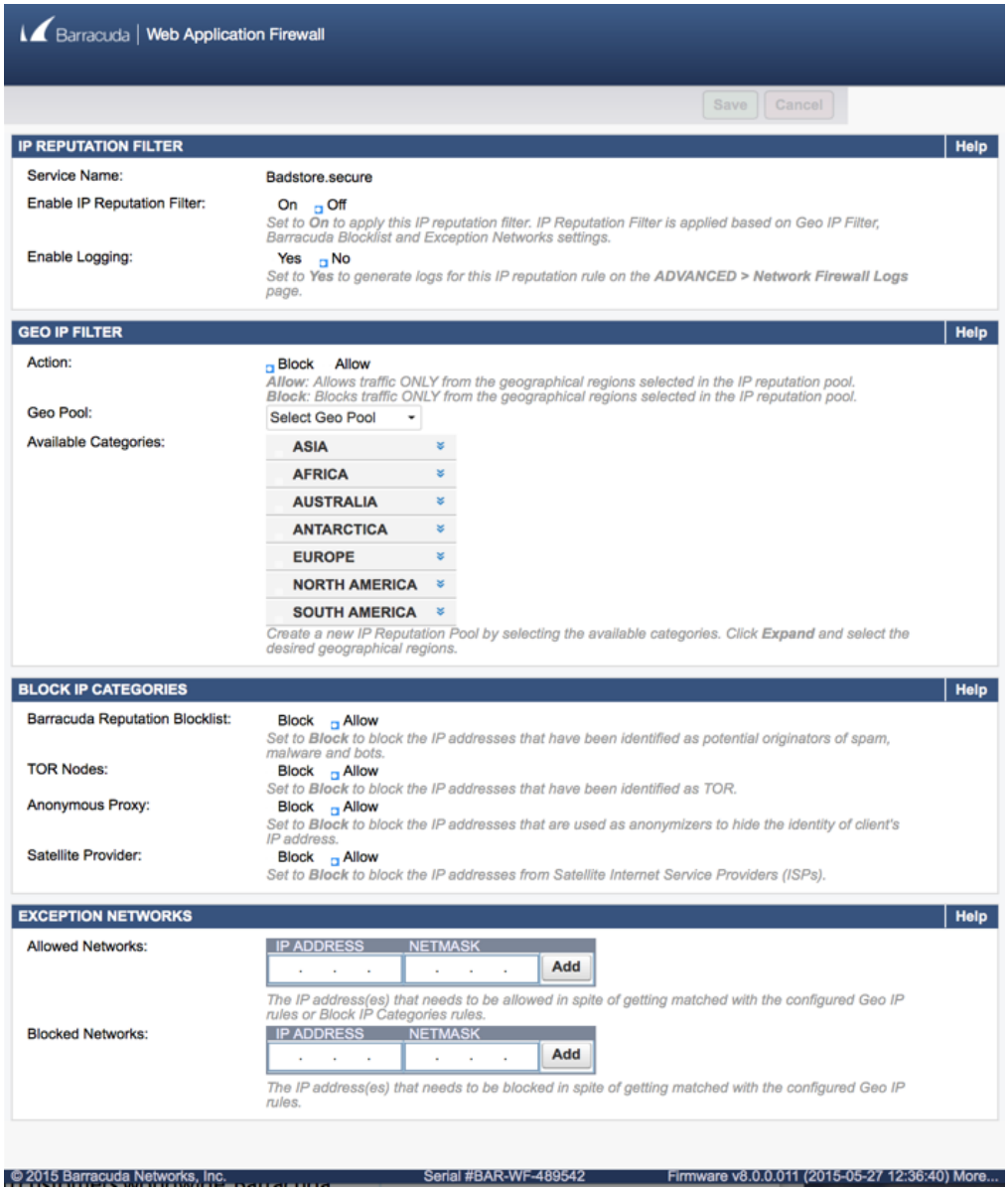


Name	IP:Port	Status	Geo Pool	Pool Name	Action	Barracuda Blocklist	TOR Nodes	Anonymou...	Satellite IP ...	Options
default										
Badstore.secure	64.235.145.33:443			NONE	Block					Edit
Corp.web	64.235.145.34:80	✔		AttackGeo	Block	✔	✔	✔		Edit
Demo1	64.235.145.35:80			NONE						Edit
Demo1.https	64.235.145.35:443			NONE						Edit
spam-demo	64.235.145.35:81			NONE	Block					Edit
Training	64.235.145.34:8080			NONE	Block					Edit

Étant donné que les défis CAPTCHA peuvent être considérés comme envahissants, les organisations peuvent utiliser des algorithmes de détection passifs et actifs, afin d'utiliser uniquement les CAPTCHA pour les clients suspects, après avoir administré les tests de clients passifs.

Atténuation à l'aide des contrôles de géolocalisation

Les botnets sont largement distribués dans le monde, en particulier dans les régions à forte pénétration informatique et à large bande. Le pare-feu Barracuda Web Application Firewall possède un module GeoIP intégré pouvant mapper l'adresse IP attaquante à son emplacement géographique. Lors d'une attaque, cela permet de bloquer le trafic provenant de l'extérieur de la géographie principale et des marchés d'une entreprise.



En fonction de l'empreinte mondiale du botnet, environ 30 à 70 % du trafic d'attaque peut être éliminé en utilisant simplement des ACL de géolocalisation. Cela permet non seulement de continuer à servir de véritables clients, mais également de libérer des capacités de calcul et de réseau.

Filtrage du trafic Botnet à l'aide du flux de réputation IP du client

Les botnets ont évolué et sont devenus des cadriciels génériques extensibles pouvant être utilisés pour les chevaux de Troie bancaires, le spam, les attaques DDoS, la fraude aux clics, les APT, etc. Barracuda Networks fournit des solutions de sécurité couvrant les applications de messagerie, Web, réseau et Web à plus de 150 000 clients dans le monde ; pr conséquent, il possède une base de données de réputation de pointe classant de nombreux vecteurs de menaces et IP malveillantes. Cette infrastructure est connue sous le nom de Barracuda Reputation Block List (BRBL) et est maintenue par Barracuda Labs.

Le pare-feu Barracuda Web Application Firewall s'intègre à BRBL pour fournir une protection contre les robots. Lors d'une attaque DDoS soutenue, cela fournit un excellent outil pour détecter et bloquer le trafic de botnet pouvant cibler vos serveurs. De plus, le pare-feu Barracuda Web Application Firewall est capable de bloquer les proxys anonymes et ouverts, ainsi que les FAI satellites, couramment utilisés par les pirates pour effectuer la reconnaissance et lancer des menaces persistantes avancées (APT).

Toute cette infrastructure est automatisée et de nouvelles définitions sont transmises automatiquement aux appliances sur le terrain à l'aide d'Energize Updates (EU) ; aucune intervention de l'administrateur n'est donc nécessaire.

Empêcher les serveurs d'applications de devenir des nœuds de botnets

Bien qu'il soit important de se protéger contre les DDoS d'application, il est tout aussi essentiel de s'assurer que le serveur d'applications et les ressources réseau ne soient pas forcés à faire partie d'un botnet ou d'un serveur C&C. Le rassemblement (herding) de serveurs d'applications est très intéressant pour les botmasters, car les serveurs leur offrent des ressources d'attaque considérablement plus importantes, ainsi qu'une excellente plateforme pour poursuivre leur recrutement de botnet.

Les serveurs d'applications peuvent disposer d'applications personnalisées, héritées ou tierces. Toute vulnérabilité du jour zéro contenue dans ces applications peut entraîner une attaque et le recrutement de votre serveur et de la bande passante pour effectuer des activités de botnet. Le pare-feu Barracuda Web Application Firewall offre une sécurité renforcée contre les téléchargements de logiciels malveillants, les injections de commandes du système d'exploitation, les traversées de répertoires ou toute reconnaissance ou attaque capturant des serveurs d'applications.

Résumé

La tendance des DDoS de la couche application devrait s'accélérer. Les recherches de Gartner indiquent que les pirates utilisent désormais les attaques DDoS pour distraire le personnel de sécurité, afin de pouvoir voler des informations sensibles ou de l'argent de comptes. Le rapport 2012 de Verizon sur les enquêtes concernant les violations de données confirme que de telles attaques sont « plus effrayantes que d'autres menaces, qu'elles soient réelles ou imaginaires ».Les appareils connectés à l'Internet, les réseaux sociaux et le cloud computing ont également alimenté de nouveaux vecteurs d'attaque. Les botnets ciblant les plateformes mobiles sont désormais courants. L'évolution du navigateur en tant que plateforme et de HTML5 ouvrira probablement de nouvelles avenues pour le bot-herding. L'accès aux kits de botnet et à la location est plus facile que jamais.

Au fur et à mesure que la valeur et la criticité de leurs sites Web augmentent, les organisations ne peuvent pas se permettre de devenir des cibles de botnets ni tolérer des perturbations prolongées de leurs services Web. Les botnets peuvent entraîner une érosion importante des revenus, des opérations, de la marque et de la confiance des consommateurs. L'absence d'une stratégie d'atténuation internationale rend plus difficile la lutte contre les botnets. Heureusement, le pare-feu Barracuda Web Application Firewall fournit une solution robuste contre les attaques DDoS basées sur les applications qui neutralise les effets négatifs d'une telle attaque.

Pour en savoir plus sur le pare-feu Barracuda Web Application Firewall, veuillez consulter le site http://www.barracuda.com/waf ou appeler Barracuda Networks pour obtenir un essai gratuit de 30 jours, au 1-408-342-5400 ou au 1-888-268-4772. Pour obtenir plus d'informations concernant nos autres solutions de sécurité et de productivité, veuillez visiter le site http://www.barracuda.com/products.

À propos de Barracuda Networks, Inc.

Barracuda fournit des solutions de sécurité et de stockage hébergées dans le cloud qui simplifient l'informatique. Ces solutions puissantes, faciles à utiliser et abordables sont approuvées par plus de 150 000 organisations dans le monde et sont livrées dans des déploiements d'appliance, d'appliance virtuelle, de cloud et hybrides. Le modèle commercial de Barracuda, centré sur le client, se concentre sur la fourniture de solutions informatiques à valeur ajoutée, basées sur l'abonnement, assurant la sécurité de bout en bout du réseau et des données. Pour de plus amples informations, veuillez visiter le site barracuda.com.

É-U 1.1 • Copyright © Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008
408-342-5400/888-268-4772 (États-Unis et Canada) • barracuda.com

Barracuda

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
États-Unis

Tél. : 1-408-342-5400
1-888-268-4772
(États-Unis et Canada)
E-mail : info@barracuda.com
Web : barracuda.com