Services de protection contre les attaques DSD

Global IP Network | Brochure de service

Un monde de cybersécurité

Un nombre record de consommateurs utilisent le commerce, l'actualité et le divertissement vidéo en ligne; l'essor de nouveaux secteurs d'activité passionnants, tels que l'Internet des objets (IdO) et la virtualisation : voilà les tendances que nous voyons aujourd'hui. Mais un monde plus connecté signifie également davantage de possibilités à exploiter pour les criminels, avec des cyberattaques de plus en plus sophistiquées. Les entreprises traditionnelles et celles centrées sur Internet ne peuvent tout simplement pas se permettre de relâcher leur vigilance, ces violations ayant le potentiel de perturber les réseaux et de coûter des millions. Faire de la protection une caractéristique centrale lors du lancement de nouveaux produits et services reste donc un impératif, et l'une des préoccupations commerciales les plus critiques du moment.

Attaques DSD

Les principales préoccupations d'aujourd'hui sont les attaques par déni de service distribué (DSD), qui sont devenues une menace régulière pour la communauté des entreprises en ligne. Celles-ci peuvent survenir à tout moment, ce qui peut avoir des effets dévastateurs sur votre réseau, endommager des actifs et entraîner des pertes de revenus importantes. Et elles augmentent en taille, fréquence et complexité, certaines ayant mis en péril des centaines de milliers d'appareils. Il est donc essentiel de les éliminer avant qu'elles ne puissent faire de véritables dégâts.

Attaques volumétriques

Les attaques volumétriques sont conçues pour submerger un hôte ou un réseau et le rendre inaccessible. Ces types d'attaques proviennent généralement de machines compromises ou de l'exploitation de certains protocoles réseau, entraînant souvent des dommages collatéraux et rendant le réseau inaccessible au-delà de la cible prévue.

- **Inondation par paquets TCP SYN**
- **Inondation par paquets UDP**
- **Inondation par paquets ICMP**
- **Attaque par réflexion**

Attaques de couche d'application

Les attaques de couche d'application sont des attaques bien conçues ciblant un service spécifique sur l'hôte. Celles-ci peuvent être difficiles à détecter, car elles ressemblent à une connexion légitime, mais sont souvent remplies de demandes absurdes. En raison des nombreux outils disponibles, tels que LOIC tool, ces attaques sont devenues encore plus populaires parmi les pirates informatiques.

- **Attaque par requête HTTP-GET**
- **Attaque par requête HTTP-POST**
- **Attaques SSL**

Attaques par épuisement des tables d'état

Ces attaques peuvent être de nature volumétrique et/ou de la couche d'application, souvent représentées par un script Slowloris d'attaques HTTP-GET ou SSL.

Une approche proactive de la sécurité réseau

Au sein de Global IP Network (GIN), nous comprenons parfaitement la nécessité de nous tenir au courant de ces menaces de plus en plus complexes. C'est pourquoi nous adoptons une approche proactive pour les arrêter, et non une approche réactive une fois que le dommage est déjà fait. Nos produits de sécurité sont conçus pour prendre en charge des environnements de sécurité multimenaces, et nous proposons des options personnalisées vous permettant de choisir la prise en charge correspondant le mieux à la stratégie de cyberdéfense de votre organisation.

Nous écoutons également vos besoins spécifiques en matière de sécurité pour vous aider à faire le meilleur choix. Vous pouvez être assuré que nous disposons de l'équipe idéale pour vous soutenir : notre équipe de sécurité réseau (NST) est dédiée, a une ancienneté moyenne de plus de 10 ans et offre une grande expertise. Combinée à notre backbone Global IP Tier-1, notre offre de sécurité est inégalée.

Services de protection contre les attaques (SDSD)

Nos services de protection contre les attaques par déni de service distribué (SDSD) offrent une approche complète et progressive de l'atténuation des attaques par déni de service distribué, en fonction du type et du niveau de protection que vous souhaitez. Ces options vous donnent la possibilité d'obtenir la protection qui correspond le mieux à votre stratégie de défense, que vous souhaitiez une prise en charge de niveau basique, intermédiaire ou élevée. Et si vous avez besoin d'une protection avancée, nos services ont les capacités de faire face aux attaques à grande échelle, de rediriger et de nettoyer le trafic via notre plateforme d'atténuation. Alors, contactez-nous et défiez les criminels avant qu'ils ne puissent rendre votre service inaccessible.

SDSD de contrôle

Le SDSD de contrôle est notre service d'entrée de gamme. Grâce à ce service, les clients peuvent définir des listes de contrôle d'accès (LCA) permanentes pour bloquer le réseau à certains types de trafic déterminés par le client. Donc, si vous n'avez pas besoin d'une assistance complète pour l'atténuation des attaques, mais que vous souhaitez quand même un service robuste sur lequel vous pouvez vraiment compter pour une protection basique, ce pourrait être l'option pour vous. Ce service offre les fonctionnalités suivantes:

Support LCA permanent

- Support pour des LCA jusqu'à 50 lignes
- Support standard et d'urgence pour le changement de LCA

Accord de niveau de service (ANS) relatif au temps de réponse des LCA

- ANS autour d'un temps de réponse de 30 minutes pour les demandes LCA d'urgence
- ANS autour d'un temps de réponse d'un jour pour les demandes LCA normales

SDSD central

Notre niveau de protection suivant est le SDSD central. Outre sa gamme de fonctionnalités supplémentaires, le support fournit par notre équipe de sécurité réseau (NST) rajoute une garantie – c'est la même équipe qui défend GIN contre les attaques. En utilisant une technologie de pointe en réponse à une demande d'atténuation d'attaque, notre équipe peut rapidement analyser une attaque et prendre toutes les contre-mesures nécessaires pour l'éliminer, comme l'identification des vecteurs d'attaque clés, le filtrage du trafic et son réacheminement vers notre plateforme d'atténuation à des fins de nettoyage. Obtenez cette option si vous souhaitez une réponse rapide et efficace aux activités DSD malveillantes. En plus des fonctions basiques du SDSD de contrôle, ce service comprend :

Accès à l'équipe de sécurité réseau

- Les abonnés au SDSD de contrôle ont un accès direct à notre équipe de sécurité réseau hautement compétente, afin qu'ils puissent rester à jour pendant les atténuations d'attaque

Atténuation des attaques

- Notre équipe NST emploie une approche multicouche pour l'atténuation des attaques et utilisera toute une gamme d'outils et de techniques, y compris l'épuration du trafic d'attaques à l'aide de notre plateforme d'atténuation

Accord de niveau de service relatif au temps de réponse de l'atténuation

- Temps de réponse de 15 minutes pour les demandes via le portail de SDSD
- 30 minutes pour les demandes effectuées par e-mail, téléphone ou portail client

Portail et rapports

- Notre portail SDSD exclusif permet d'accéder aux rapports d'atténuation et à l'historique pertinent

SDSD de détection

Vous voulez un niveau de prise en charge encore plus élevé, plus approfondi ? La réponse pourrait être le SDSD de détection. En plus de toutes les fonctionnalités exceptionnelles offertes par le SDSD central, il ajoute des services tels que des capacités de détection pour aider à informer les clients des attaques potentielles, et des atténuations initiées par le client en un seul clic sur le portail SDSD. Les clients peuvent également examiner leur historique de détection et leurs rapports d'atténuation passés, et demander des modifications de configuration. Donc, pour un service de protection complet contre les attaques DSD qui couvre toutes les bases, obtenez le SDSD de détection. Les fonctionnalités ci-dessous sont uniquement incluses dans le SDSD de détection :

Détection d'attaque

- En fonction des seuils définis par le client, les clients du SDSD de détection seront avertis des attaques potentielles via le portail SDSD, et de façon facultative, par e-mail ou syslog

Atténuation auto-initiée

- Sur le portail SDSD, les clients peuvent initier une atténuation basée sur une alerte de détection active, ou en spécifiant l'adresse IP cible

SDSD Max

L'offre la plus complète pour la protection contre les attaques DSD pour les clients Global IP Network est le SDSD Max. Ce service utilise une combinaison de ressources, d'expertise et de stratégies d'atténuation de NTT pour protéger les clients affectés par les attaques DSD, y compris la détection d'attaques et l'atténuation automatique. Le service est pris en charge par notre équipe NST, qui est également chargée de la défense du Global IP Network contre les attaques.

Atténuation automatique

- Lorsqu'elle est avertie d'une possible attaque DSD, la plateforme lance automatiquement une atténuation, redirige le trafic vers notre plateforme d'atténuation et arrête l'atténuation une fois l'attaque terminée. Aucune action du client nécessaire

Pour plus d'informations et de mises à jour sur Global IP Network :

Nous contacter à : gin@ntt.net
www.gin.ntt.net

Suivez-nous sur Twitter
@GinNTTnet
#globalipnetwork #AS2914

v202101FRdps