Mettre fin aux attaques DDoS

Dans un monde où le nombre d'appareils connectés ne cesse de grandir, de nouvelles opportunités commerciales et de croissance passionnantes voient le jour dans des domaines tels que l'Internet des objets (IdO), la virtualisation, le commerce en ligne et les divertissements.

Cependant, en même temps, cela offre aux criminels davantage de possibilités de tirer profit de cyberattaques de plus en plus sophistiquées. Avec l'essor des appareils IdO, de nombreuses attaques prennent désormais la forme d'attaques par déni de service distribué (DDoS), c'est-à-dire qu'un afflux de trafic interrompt les flux normaux de l'Internet et empêche le passage du trafic normal.

Ces invasions DDoS existent sous différentes formes, l'une des plus courantes étant les attaques volumétriques. Celles-ci sont conçues pour consommer la bande passante disponible en submergeant le réseau de trafic et proviennent généralement de dispositifs compromis ou de l'exploitation de certains protocoles de réseau. Un autre type est celui des attaques de la couche application, qui ont tendance à cibler un service spécifique sur le réseau hôte tel qu'un moteur de recherche.

La menace devrait encore s'accroître à mesure que l'IdO prolifère avec l'évolution vers la 5G et son utilisation dans des domaines tels que les voitures connectées, qui pourraient effectivement créer des points d'accès mobiles permettant de lancer des attaques.

Tendances en matière de DDoS

Ces dernières années ont vu des attaques DDoS à l'échelle du térabit sans précédent. Celles-ci ont été facilitées par des méthodes qui ont vu le jour comme la technique Memcached utilisée au début de 2018, lorsqu'une attaque DDoS de 1,7 Tb/s, qui battait alors le record, a rapidement suivi une attaque de 1,35 Tb/s quelques jours auparavant.

En 2020, une attaque DDoS a même surpassé ces dernières, Amazon Web Services ayant rapporté un événement de 2,3 Tb/s qui a entraîné trois jours de menace élevée et qui était 44 % plus important que toutes les attaques volumétriques détectées auparavant.

NETSCOUT, quant à lui, a rapporté une augmentation de 16 % de la fréquence des attaques DDoS au niveau mondial au cours du second semestre de 2019 par rapport à l'année précédente. Bien que l'organisation ait noté une baisse significative de la régularité des attaques supérieures à 200 Gb/s, les auteurs ont intensifié ces activités à plus petite échelle tout en utilisant un éventail toujours croissant de vecteurs d'attaque nouveaux ou de plus en plus populaires, puisque NETSCOUT souligne qu'il y en a eu sept rien qu'en 2019.

La COVID-19 a également mis en évidence l'impact potentiel des événements soudains qui transforment le comportement des consommateurs. La société de services et de technologies de l'information Neustar souligne qu'au cours du premier semestre de 2020, une augmentation « précipitée » de l'activité DDoS a reflété une croissance du trafic Internet, les gens passant beaucoup plus de temps en ligne à la maison pour des activités telles que les achats, les jeux et le travail durant la pandémie. Au total, Neustar a constaté une augmentation de 150 % du nombre de ces attaques au cours des six premiers mois de l'année 2020, par rapport à l'année précédente.

Une tendance récente est l'augmentation des attaques DDoS dans le domaine des jeux, où il est devenu plus facile et beaucoup plus accessible pour les utilisateurs réguliers armés d'une carte de crédit d'accéder à des services bon marché qui provoquent un ralentissement de connexion chez les rivaux. Les services « booter » ou « stresser » DDoS à bas prix peuvent être utilisés pour mettre hors ligne d'autres joueurs ou lancer des attaques contre des cibles telles que les services financiers, les services informatiques ou les fournisseurs de cloud qui peuvent héberger des applications pour d'autres secteurs.

Un autre facteur à prendre en compte est que ces menaces peuvent affecter une grande variété de secteurs, ce qui signifie que les entreprises ne peuvent tout simplement pas se permettre de baisser leur garde.

Une tendance récente est **l'augmentation des attaques DDoS** dans le domaine des jeux... **Les services « booter »** ou **« stresser » DDoS** peuvent être utilisés pour mettre hors ligne d'autres joueurs...

Stratégie pour la lutte

Pour lutter contre ces menaces, il existe toute une série de mesures que les opérateurs et les entreprises peuvent prendre pour se préparer. L'une des mesures clés consiste à identifier les actifs qui sont essentiels à l'entreprise, tels que les serveurs de noms et de base.

De plus, il est conseillé d'exploiter les centres d'opérations réseau pour surveiller les niveaux de trafic normaux afin que l'impact d'une attaque puisse être plus facilement et plus rapidement identifié avant qu'elle n'ait la chance de s'installer et de provoquer le chaos. De nombreuses entreprises ne savent toujours pas quels sont leurs comportements habituels, ce qui rend difficile l'identification de niveaux d'activité inhabituels.

Certains outils comme NetFlow peuvent être utilisés pour recueillir des données et du trafic réseau à des fins d'analyse, avec l'avantage de fournir des logiciels commerciaux et open-source adaptés à tous les budgets.

Ces ressources permettent de recueillir des données historiques et aident à déterminer à l'avenir toute augmentation importante du trafic qui pourrait indiquer une attaque et même sa provenance.

Il est également utile de tenir un journal détaillé de toute attaque pour aider à se préparer correctement à des événements futurs similaires, ce qui permet de créer une liste de contrôle et d'aider à l'examen de services de sécurité potentiels qui peuvent traiter les types de modèles identifiés.

Des simulations d'attaques peuvent également être effectuées pour s'assurer que les centres d'opérations réseau sont capables de faire face aux menaces et disposent d'un plan d'action spécifique lorsqu'elles se produisent, ce qui permet d'identifier les équipements critiques avant que l'entreprise ne soit attaquée. La Network Security Team (NST) de la division Global IP Network de NTT est prête à participer à ces « jeux de guerre », et encourage donc activement les clients à contacter l'entreprise s'ils souhaitent les mettre en place. Par ailleurs, l'établissement d'une relation rapprochée avec les équipes de sécurité des fournisseurs est un moyen efficace de contribuer à atténuer le stress lorsqu'une attaque éclate.

En prenant de telles mesures, une réponse aux attaques peut être élaborée plus rapidement en collaboration avec un fournisseur de réseau comme NTT.

Les équipes peuvent alors travailler ensemble de manière efficace pour éradiquer toute menace, en utilisant des méthodes telles que le blocage, le nettoyage et l'épuration du trafic, selon les besoins. L'atténuation automatisée avec des fournisseurs tels que NTT peut permettre une réponse rapide en 30 secondes seulement, ce qui est important étant donné le nombre croissant d'attaques très courtes dans des domaines tels que les jeux, où elles durent souvent moins de cinq minutes.

L'atténuation automatisée avec des fournisseurs tels que NTT peut permettre une réponse rapide en **30 secondes** seulement.

Examiner et collaborer

Le travail ne doit pas s'arrêter une fois l'attaque terminée, car il est alors temps de procéder à une autopsie, d'analyser ce qui s'est passé et d'identifier les défaillances des équipements et les trous qu'il peut y avoir dans les défenses afin d'être encore mieux préparé pour les prochaines attaques.

Ainsi, il est possible d'évaluer des facteurs tels que la capacité des pare-feu à gérer le mauvais trafic, la présence de serveurs compromis ou vulnérables et la nécessité d'envisager des mises à niveau ou d'utiliser un service d'atténuation plus intelligent.

Documenter le type d'attaque peut aider les équipes des centres d'opérations réseau à identifier les mauvais types de trafic à l'avenir, permettant une réponse plus rapide. Au lendemain d'une attaque, il peut également être possible de remonter jusqu'à l'agresseur et de prendre des mesures contre lui.

De surcroît, la collaboration entre les entreprises est essentielle pour réduire l'impact des menaces : le Global Leaders Forum cherche à rassembler les opérateurs et les acteurs qui sont régulièrement confrontés aux DDoS afin de partager des idées et des informations, ainsi qu'à aider les gens à faire connaissance pour former des points de contact rapides. Les groupes de sécurité en ligne tels que NSP-SEC et Ops-Trust sont d'autres voies de coopération.

NTT collabore par le biais de nombreux groupes et lors d'événements, et est donc prêt à organiser des réunions pour discuter de meilleures approches pour atténuer les attaques DDoS.

Protection contre les DDoS avec NTT

Faire de la protection un élément central lors du lancement de nouveaux produits et services reste une nécessité ; c'est un domaine dans lequel NTT adopte une approche proactive. Cela signifie que ces menaces peuvent être stoppées rapidement, plutôt que d'adopter une approche réactive lorsque le mal est déjà fait.

Dans cette optique, les services de protection DDoS (DPS) proposés par la division Global IP Network de NTT fournissent des capacités intelligentes d'atténuation des DDoS qui nettoient le trafic malveillant avant qu'il n'ait un impact sur la connexion Internet du client. Le trafic est alors dévié vers les centres d'épuration de l'entreprise, où il est analysé et le trafic d'attaque est supprimé avant que le reste ne soit transmis au réseau du client.

Entre-temps, NTT a développé différents niveaux de DPS qui répondent aux différents niveaux de protection dont les clients de Global IP Network ont besoin.

Le service DPS Max est destiné aux clients qui souhaitent une protection complète, y compris la détection des attaques et les fonctions automatiques d'atténuation. Cette dernière fonction permet aux clients de bénéficier d'une atténuation immédiate grâce à la plateforme qui détecte les attaques et met automatiquement en place des mesures défensives en fonction de seuils définis par le client. Une fois l'attaque terminée, la plateforme ramène le trafic des clients au routage standard d'avant l'attaque.

Les autres niveaux de service de NTT sont DPS Control, DPS Core et DPS Detect. Le premier est un service d'entrée de gamme qui permet aux clients de définir des listes de contrôle d'accès permanentes pour bloquer certains types de trafic sur le réseau. Les types de clients qui conviennent le mieux à ce service sont les utilisateurs avancés qui comprennent leur profil de trafic et ont la capacité d'atténuer les attaques par eux-mêmes, mais qui veulent réduire leur exposition à des types de menaces spécifiques.

En tant que niveau intermédiaire, DPS Core franchit une nouvelle étape en offrant une série de fonctionnalités supplémentaires par rapport au service de base. L'un des points forts de ce service est l'utilisation d'une technologie de pointe qui permet de répondre rapidement aux demandes d'atténuation. Cela permet de répondre dans un délai de 15 minutes aux demandes soumises via le portail DPS de l'entreprise, un portail exclusif pour les services de protection DDoS.

Le portail DPS offre des avantages majeurs aux clients, outre l'amélioration de la rapidité. En plus de permettre l'ouverture de cas d'assistance auprès du support de NTT, il avertit immédiatement un ingénieur de sécurité de garde pour qu'il intervienne auprès du client. Par l'intermédiaire du portail, les clients peuvent également demander des changements de configuration, comme l'ajout de préfixes de protection, et peuvent examiner l'historique et les graphiques des attaques.

Parallèlement, DPS Detect est un autre niveau de service qui fournit les fonctionnalités offertes par DPS Core et ajoute des services tels que des capacités de détection pour avertir les clients d'attaques potentielles et une atténuation à l'initiative du client par simple pression sur un bouton.

NTT propose également à ses clients de Global IP Network un blackholing sélectif pour bloquer le trafic sur le réseau et limiter les attaques au niveau géographique. Cela peut s'avérer efficace pour empêcher la propagation d'attaques volumétriques à grande échelle.

> Les services de protection DDoS (DPS) proposés par la division Global IP Network de NTT fournissent des capacités intelligentes d'atténuation des DDoS qui **nettoient le trafic malveillant avant qu'il n'ait un impact** sur la connexion Internet du client.

Assurance supplémentaire

Un niveau d'assurance supplémentaire est fourni par le support de l'équipe de sécurité de Global IP Network, grâce auquel les utilisateurs des services DPS peuvent bénéficier d'un accès direct à des experts ayant une expérience moyenne de plus de 10 ans, apportant une vaste palette de compétences pour aider à atténuer les attaques.

Les services DPS de Global IP Network sont parfaitement adaptés à toutes les entreprises qui ont besoin d'un niveau élevé de disponibilité de l'Internet, notamment les acteurs du commerce en ligne, les opérateurs de télécommunications, les fournisseurs de services Internet, les fournisseurs de contenu tels que les sociétés de vidéo et de jeux, et les réseaux sociaux.

Dans l'ensemble, une approche multistratégies est souvent recommandée par les fournisseurs comme la meilleure stratégie, la plus complète, pour faire face aux attaques DDoS de nos jours. Il s'agit d'une combinaison de filtrage en amont pour bloquer les applications non utilisées, de blackholing sélectif et d'atténuation des DDoS par une épuration intelligente.

En prenant les mesures recommandées ci-dessus et en travaillant en étroite collaboration avec NTT et ses mécanismes de sécurité bien établis, de grands progrès peuvent être réalisés pour résoudre ensemble les problèmes de DDoS.

Together we do great things

Pour en savoir plus ou pour nous faire part de vos commentaires, contactez-nous à l'adresse suivante : gin@ntt.net

Suivez-nous sur Twitter
@GinNTTnet
#globalipnetwork #AS2914

Consultez le site : gin.ntt.net

©2020 NTT Ltd. et le logo NTT sont des marques commerciales et/ou des marques de service de la Nippon Telegraph and Telephone Corporation (NTT).
Tous droits réservés.