RÉSEAU AU SERVICE DU SAVOIR

SERVICE R-SÉCURITÉ

Une solution novatrice aux attaques par déni de service (DDos).

EN MATIÈRE DE SÉCURITÉ, BIEN QU'AUCUN SERVICE NE PUISSE GARANTIR UNE PROTECTION INFAILLIBLE, IL EST POSSIBLE DE CONCEVOIR DES SOLUTIONS NOVATRICES AFIN D'ASSURER UNE PROTECTION OPTIMALE.

C'est dans cette optique que le RISQ a mis en place le service R-Sécurité, qui propose une protection contre les attaques par déni de service (DDoS). De telles attaques peuvent paralyser partiellement ou totalement un réseau en surchargeant ses liens ou en saturant ses ressources (site Web, serveur de courriel, etc.). L'objectif du RISQ est donc de protéger le périmètre de son réseau pour laisser suffisamment de bande passante pour les besoins de sa clientèle. Il est à noter que ce service ne se substitue pas aux mécanismes de sécurité en place dans chacune des institutions.

Le service R-Sécurité protège le service Internet commercial du RISQ en temps réel (aucune activation requise). La détection et le traitement des attaques se font en amont de votre réseau, directement sur la dorsale du RISQ. Autrement dit, les attaques ne se rendent pas à votre réseau.

Le RISQ travaille continuellement à l'amélioration de la qualité et de la disponibilité de ses services. Depuis l'été 2018, R-Sécurité s'inscrit dans cette optique en offrant un service Internet protégé en tout temps contre les attaques DDoS.

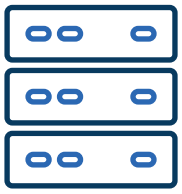
- ☑ Service clé en main
- ☑ Protection en temps réel

VECTEURS D'ATTAQUES DDoS

VOLUMÉTRIQUE

L'objectif de l'attaquant est de remplir le tuyau Internet de la cible. L'attaque est donc supérieure à la capacité.

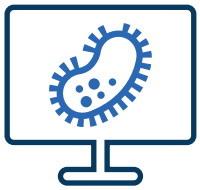
On parle d'une attaque en amont du réseau de la cible, ce qui veut dire qu'aucun équipement dans le réseau de la cible ne pourra contrôler l'attaque.



APPLICATIF

L'objectif de l'attaquant est d'atteindre les ressources applicatives (HTTP, site web, serveur de courriel, etc.) et de les rendre indisponibles par l'envoi de plusieurs requêtes.

Ces attaques sont souvent plus sophistiquées et plus difficiles à détecter.



PROTOCOLAIRE

L'objectif de l'attaquant est d'identifier des faiblesses à exploiter et ensuite cibler des équipements réseau.

L'attaquant bloque ces équipements en envoyant une très grande quantité d'information à traiter.

SURVOL DES PLUS GRANDES ATTAQUES PAR DÉNIS DE SERVICE (DDoS)

FÉVRIER 2018 – GITHUB

GitHub est une plateforme de développement en ligne très populaire qui est utilisée par des millions de développeurs. **Au plus fort de l'attaque, le trafic entrant a atteint un niveau record de 1,3 téraoctet par seconde (Tbps), ce qui s'est traduit par l'envoi de paquets à un taux de 126,9 millions par seconde.**

Les attaquants ont utilisé l'effet d'amplification d'un système général servant à gérer la mémoire cache distribuée (memcached). En noyant les serveurs memcached avec des usurpations d'adresses IP, technique de piratage qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet, l'amplification a pu atteindre des niveaux de 50 000 fois. **La durée de l'attaque a été d'environ une vingtaine de minutes.**

OCTOBRE 2016 – DYN

Cette attaque a visé Dyn, un acteur majeur au niveau de la gestion des DNS. Elle a eu des répercussions dévastatrices pour des sites comme AirBnB, Netflix, PayPal, Amazon, etc. Dans ce cas-ci, les attaquants ont utilisé un logiciel malveillant appelé Mirai. Ce logiciel a créé des machines zombies en utilisant des objets connectés à Internet, comme des téléviseurs intelligents, des caméras, des imprimantes et des routeurs pour la maison. Ces objets ont donc été programmés pour envoyer des requêtes à une cible identifiée. **La durée de l'attaque a été d'une journée, paralysant ainsi une partie de l'Internet.**

2015 – GITHUB

Cette attaque a aussi ciblé GitHub et a duré plusieurs jours. Le vecteur d'attaque consistait à injecter des codes JavaScript dans les navigateurs internet de tous les utilisateurs du moteur de recherche Baidu, engin le plus utilisé en Chine. Des requêtes HTTP étaient envoyées sur des pages ciblées de GitHub. **Une des particularités de cette attaque est qu'elle s'adaptait aux différentes stratégies de mitigation d'attaques DDoS en place.**

RÉSEAU AU SERVICE DU SAVOIR

Le RISQ, un réseau étendu, fiable, performant et sécuritaire qui évolue avec les besoins grandissants de ses membres.

AVANTAGES SUPPLÉMENTAIRES

- Traitement en amont afin d'éviter la saturation.
- Entièrement géré par le RISQ.
- Aucune intervention requise lors d'une attaque.
- Protection des protocoles IPv4 et IPv6.
- Service technique offert en anglais et en français.

Si vous avez des questions sur le service R-Sécurité offert par le RISQ, **n'hésitez pas à nous contacter.**

www.risq.quebec

514 845-7181 poste 246

sam@risq.quebec