Protection efficace contre les attaques DDoS Appliances DDoS de Corero

Selon de nombreuses études réalisées, les attaques par déni de service distribué «Distributed Denial of Service» (DDoS) font partie des risques les plus dangereux pour les infrastructures et applications IT. Pour détecter de telles attaques et les contrer en toute efficacité, il est recommandé de faire appel aux systèmes de défense DDoS (DDS) haute performance de Corero.

Les systèmes de défense contre les attaques DDoS de Corero protègent, avec la même efficacité, aussi bien les applications que les infrastructures.

Les attaques DoS et DDoS lancent de gros défis aux entreprises et aux organisations. Leur objectif est de paralyser les applications et les serveurs et de perturber le fonctionnement des pare-feu, équilibreurs de charge, serveurs web et serveurs d'applications, bases de données et solutions de stockage, de telle sorte qu'ils ne puissent plus remplir leurs tâches («Denial of Service»). Pour y parvenir, les hackers se servent, d'une part, des attaques de grande envergure. D'autre part, ils lancent des attaques multi-vecteurs intelligentes ainsi que des attaques au niveau des applications.

Dans la première variante, un tel nombre de requêtes HTTP est transmis avec un handshaking incomplet au système attaqué, que celui-ci n'est plus en mesure de fournir des contenus du fait de la surcharge ainsi générée. Les types d'attaques comme les attaques SYN-Flood ou Smurf font partie de cette catégorie.

Une forte progression est enregistrée au niveau des attaques multi-couches. Ces attaques «lentes» et «de faible intensité» ne requièrent que de faibles ressources et prennent souvent beaucoup de temps pour infester les systèmes attaqués. De ce fait, elles ne sont – en règle générale – que difficilement détectables comme sources de danger. Parmi les attaques élégantes, on peut notamment citer les attaques Reflecting-DDoS, les attaques DDoS sur la couche applicative, l'exploitation ciblée des vulnérabilités des serveurs, les Pre-Attack Recon Scans (permettant de se procurer une connaissance approfondie de l'infrastructure à attaquer) et les Advanced Evasion Techniques (combinaison de techniques d'évasion connues avec de nouvelles méthodes de camouflage permettant d'injecter du code malveillant dans le réseau cible souhaité).

Détecter les attaques et les contrer

Afin de détecter et de contrer les attaques DoS et DDoS – depuis la couche applicative, en passant par les couches DNS et HTTP, jusqu'à la couche protocole – le spécialiste de la sécurité des réseaux Corero propose des systèmes de défense contre les attaques DDoS (DDS) haute performance, dotés de fonctionnalités IPS intégrées. Ces systèmes fournissent de précieux services, aussi bien dans les entreprises (on-premise) que chez les ISP et les prestataires de services cloud. En effet, ils bloquent les adresses IP dangereuses et les échanges de données non souhaités par régions géographiques, limitent le nombre de requêtes et de liaisons, stoppent l'usurpation et la violation de protocoles et protègent contre les techniques AET (Advanced Evasion Techniques). En outre, ils bloquent tout accès non autorisé (Intrusion Prevention), contrent les débordements de tampon (Buffer Overflow) et les Exploits et empêchent toute injection de code exécutable (Code Injection). En bref, les appliances DDS de Corero constituent un dispositif de sécurité unique en son genre contre les attaques DDoS de toutes sortes.

Pour répondre à tout instant et sur le long terme à cette exigence, ils sont dotés d'un système d'évaluation interne. Celui-ci surveille en permanence la situation changeante des risques d'attaque par DDoS et actualise automatiquement les mécanismes pour contrer les attaques. De plus, un service externe d'évaluation, le Reputation Watch est mis à disposition. Celui-ci surveille en permanence les adresses IP changeantes quant à leur réputation et bloque automatiquement l'échange de données dès qu'une valeur limite est atteinte.

Corero – empêcher les attaques DDoS

Les systèmes haute performance de défense DDoS (DDS) de Corero permettent une surveillance sans failles et le blocage de toutes les attaques DDoS.

- Appliances pour la protection contre les attaques DDoS – depuis la couche applicative, en passant par les couches DNS et HTTP, jusqu'à la couche protocole
- Fonctionnalités IPS intégrées
- Système d'évaluation interne et service externe «Reputation Watch» pour la détection et le blocage efficace des attaques DDoS
- Protection contre l'usurpation de protocoles, les techniques AET (Advanced Evasion Techniques), les débordements de tampon (Buffer Overflow) et les Exploits
- Protection contre toute injection de code exécutable (Code Injection)
- Filtrage GEO-IP

BOLL
IT Security Distribution

Boll Engineering SA
En Budron C7
1052 Le Mont s. Lausanne
Tél. 021 533 01 60
contact@boll.ch
www.boll.ch