Contrer les attaques DDoS

Vol de données, paralysie des services web, atteinte ciblée de ses concurrents, motifs politiques... les attaques par déni de service distribué (DDoS) sont lancées pour diverses raisons et constituent des défis de taille pour les entreprises et les institutions. Patrick Michel

Les attaques DoS et DDsO ont pour but de paralyser les infrastructures de serveurs et de communication des entreprises et institutions ou de perturber des systèmes tels que les pare-feu, répartiteurs de charges (load balancer), serveurs web et applicatifs, banques de données et solutions de stockage, qui ne peuvent plus assurer leurs fonctionnalités et rendent le service indisponible (Denial of Service). Les attaques DoS et DDoS représentent d'énormes défis pour les entreprises de toutes tailles et les organisations publiques. En effet, elles constituent des menaces potentielles, pouvant provoquer de graves dommages économiques, porter atteinte à la réputation des organisations ou entraîner la faillite des entreprises. Malgré l'importance capitale que revêtent ces cyberattaques, peu d'informations sur des attaques DDoS réussies sont rendues publiques. Cela s'explique sans doute par le fait que les entreprises touchées parviennent à dissimuler les attaques dont elles ont été l'objet.

Des cyberattaques déferlantes...

Par le passé, les attaques DoS et DDoS équivalaient à générer un important flux d'échanges (trafic) dans le but de paralyser les serveurs et les infrastructures de communication. Ce procédé est toujours utilisé, toutefois en moindre mesure. Un exemple typique de cette méthode de piratage au niveau du réseau sont les attaques dites SYN flood ou smurf (par réflexion). Elles consistent en l'envoi massif de requêtes HTTP au système cible en laissant les connexions semi-ouvertes (protocole de transport incomplet). En raison de la surcharge de ressources du serveur générée par le nombre de messages en attente, la victime est saturée et n'est plus en mesure de délivrer les contenus. Les services web tels que les boutiques internet, par exemple, sont ainsi paralysés de manière efficace.

Les attaques de ce genre se produisent en général via lesdits réseaux de zombies. Il s'agit d'une multitude d'ordinateurs infectés par des logiciels malveillants. Ceux-ci sont contrôlés et manipulés à distance par un cyberpirate, qui peut générer des milliers d'accès simultanés à une adresse cible afin de planter le système et causer un déni de service. Les vastes réseaux de zombies sont en mesure de générer un énorme trafic et de terrasser même les systèmes les mieux protégés. Les attaques DDoS sont contrôlées depuis des parcs de serveurs hébergés dans des pays dépourvus de réglementation efficace en matière d'internet, et ne peuvent donc guère être contrées. Le fait que les réseaux criminels proposent des attaques DoS sous forme de service vient en outre compliquer les choses. En effet, il est dès lors facile pour un non-pirate d'attaquer, par exemple, un concurrent inopportun.

... aux attaques DDoS «smart» et «lentes»

Contrairement aux vastes attaques déferlantes nécessitant des ressources extensives (réseaux de zombies), les attaques intelligentes DoS et DDos tendent à augmenter. Ces attaques «lentes» et «peu performantes» sont intelligentes et tout aussi efficaces que leurs pendants foudroyants. Les attaquants ont besoin de ressources relativement modestes, opèrent de manière dissimulée, prennent parfois des semaines ou des mois pour infecter les systèmes attaqués et la menace qu'ils constituent est très difficile à identifier. Selon un spécialiste américain de la sécurité des réseaux informatiques et fournisseur de systèmes de défense contre les attaques DDoS (DDS), les techniques suivantes figurent parmi les formes d'attaques intelligentes (non exhaustives):

Reflecting DDoS

Les attaques DDoS par réflexion profitent du handshake nécessaire à l'établissement d'une session TCP. En usurpant l'adresse IP source, les SYN ACK générés par les serveurs et les proxys sont dirigés de manière ciblée vers le réseau d'une entreprise tierce. La déferlante de SYN ACK entrants ainsi générée peut même terrasser de puissants pare-feu. Les attaques DDoS par réflexion peuvent être contrées par des techniques telles que le Stateful Flow Awareness et par la détection de violations de protocole (RFC Violation).

Outbound DDoS

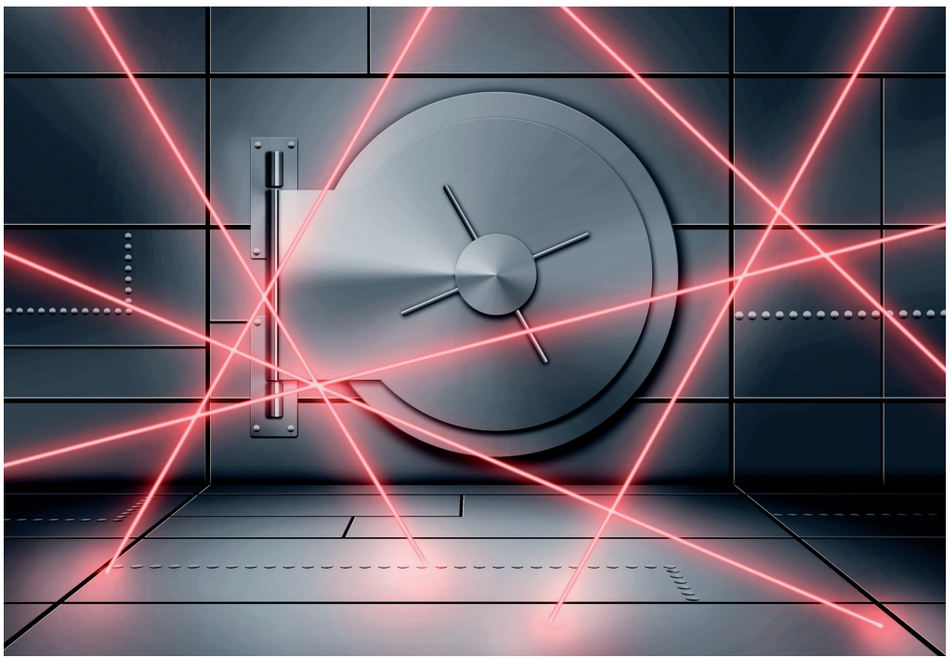
Dans ce type d'attaque, un code malicieux est installé sur les systèmes de l'entreprise attaquée, commandé à distance et activé pour lancer un DoS et bloquer tout ou partie du réseau de la victime. Si le trafic de données sortantes ainsi généré est identifié comme partie intégrante d'un réseau de zombies par l'ISP correspondant ou un fournisseur de sécurité, ce dernier peut bloquer la connexion internet ou les évaluer négativement dans des banques de données de réputation. L'entreprise touchée sera isolée de l'environnement et ne sera donc plus accessible via internet. Pour éviter ce scénario, la détection bidirectionnelle et la suppression de données indésirables sont nécessaires (Bi-Directional Flood Detection).

Application Layer DDoS

Dans ce type d'attaque au niveau de la couche applicative, des connexions TCP présumées valables sont établies à des fins criminelles. Si la connexion est établie, des requêtes sont transmises en continu par le système attaquant, jusqu'à ce que les ressources du système attaqué ne puissent plus maintenir le service. Les failles logicielles constituent également une bonne méthode d'attaque. Dans ce cas, les points faibles des applications sont utilisés pour déclencher des dysfonctionnements tels que, par exemple, le blocage d'un logiciel serveur. Les attaques DDoS des couches applicatives peuvent par exemple être évitées grâce à l'analyse comportementale. Ce procédé consiste à identifier le comportement – notamment la multiplication de l'accès à des sites web non existants – et à le comparer avec un système d'évaluation de référence. Les actions déviant de la normale entraînent, à partir d'une certaine valeur, le blocage temporaire d'un attaquant.

Specially Craftet Packet Attacks

Un autre type d'attaque par déni de service efficace est l'exploitation ciblée de la vulnérabilité du serveur. Des paquets logiciels conçus sur mesure permettent dans ce cas de mettre hors service le serveur attaqué ou ses services. Ces paquets logiciels peuvent assurer la détection des menaces et la protection contre les attaques via un système d'analyse protocolaire à états (SPA – Stateful Protocol Analysis), par le suivi des états du protocole et la détection de formes de commandes inattendues, comme dans l'utilisation des systèmes de prévention des intrusions réseau (IPS).



Les appliances DDS visant la protection contre les attaques DDoS de Corero détectent et filtrent le trafic de données malveillant, tout en autorisant le trafic régulier. Source:Boll

Pre-Attack Recon Scans

Les connaissances approfondies sur l'infrastructure à attaquer permettent aux pirates de mener leurs attaques de manière ciblée et efficace. Les Pre-Attack Recon Scans (techniques de balayage de ports à des fins de reconnaissance) par exemple permettent la détection de ports de pare-feu entrants ouverts et de dispositifs de sécurité exposés ou d'adresses IP adressées via ces mêmes ports. Ces connaissances sur la vulnérabilité des services proposés ainsi que sur les possibilités de les compromettre revêtent un grand intérêt. La dissimulation de l'infrastructure à protéger s'avère une mesure de défense efficace.

Advanced Evasion Techniques (AET)

Les techniques de contournement avancées (AET) conjuguent les techniques de contournement avec de nouvelles méthodes de camouflage afin d'infiltrer un code malicieux dans le réseau cible, sans se faire repérer le plus longtemps possible. De telles attaques ne sont pas détectées, même par les systèmes IPS modernes et autres solutions de sécurité de réseau. Pour la prévention des intrusions réseaux, les techniques dédiées «Advanced Evasion Detect» sont nécessaires.

Les pare-feu n'offrent pas une protection anti-DDoS efficace

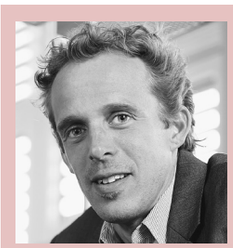
Même s'ils sont «sophistiqués» et performants, en raison de leur architecture, les appliances UTM et les pare-feu de nouvelle génération sont limités dans la détection des attaques DoS et DDoS – et encore moins capables de s'en défendre. Ils peuvent en revanche être eux-mêmes victime d'une attaque ciblée. De par leur architecture et leur fonctionnement, les pare-feu sont incapables de protéger la victime contre les différentes attaques DDoS. Un pare-feu doit couvrir tant de fonctions qu'il reste peu de ressources disponibles pour une défense efficace contre les DDoS. Par exemple, pour diriger les requêtes de service entrantes aux serveurs internes, des ports ouverts sont nécessaires (p. ex. le port 80 pour les applications web, le port TCP/UDP 53 pour le DNS, le port 25 pour l'e-mail, etc.). Et ce sont justement ces «portes ouvertes» qui permettent l'intrusion d'un code malicieux dans l'environnement du réseau et du système de l'entreprise attaquée. Qu'il s'agisse d'attaques, de requêtes ou de connexions excessives, de débordement de tampon, de DDoS au niveau applicatif, d'attaques par force brute de mot de passe ou de code infecté – les attaques de ce type ne sont pas bloquées par les pare-feu. Leur détection et leur blocage sont des tâches incombant davantage aux systèmes de défense de DDoS (DDS) performants, installés de manière transparente en amont du périmètre du pare-feu. Ils bloquent les formes d'attaques précitées et autres, savent déjouer les attaques sur le pare-feu et tous les systèmes sous-jacents et laissent passer les «bonnes» données, qui ne posent pas problème.

Les systèmes DDS performants intégrant la fonctionnalité IPS fournissent de précieux services tant aux clients (on premise) qu'aux ISP et aux fournisseurs cloud. Ils permettent la surveillance immédiate et contrent les attaques DoS et DDos à tous les niveaux imaginables – du niveau applicatif au niveau du protocole, en passant par le niveau HTTP et DNS – et assurent ainsi une disponibilité maximale et une performance illimitée des services et infrastructures protégés. Leurs mécanismes de sécurité et de défense sont complets. Ils bloquent les adresses IP menaçantes et le trafic indésirable de données par régions géographiques, limitent le nombre de requêtes et de connexions, stoppent l'utilisation abusive et les violations du protocole, contrent les AET (Advanced Evasion Techniques), bloquent les accès non autorisés (Intrusion Prevention), empêchent les débordements de tampon et exploits et bloquent l'intrusion d'un code exécutable (Code Injection).

Services automatisés et managés

Les solutions DDS performantes sont une chose, leur fonctionnement et leur réaction immédiate aux menaces changeantes en sont une autre. Un système devrait ainsi tenir compte du fait que le statut d'adresses IP peut changer de «bon» à «mauvais» en l'espace de quelques minutes. Face à cette situation, il importe de surveiller et d'identifier en temps réel les adresses IP changeant constamment dans le monde entier de manière à identifier les ordinateurs faisant partie d'un réseau de zombies et à bloquer automatiquement le trafic de données provenant d'adresse IP critiques. La géolocalisation permet en outre aux entreprises de mettre en place un contrôle des accès selon les pays et d'appliquer leur politique de sécurité à partir de l'origine géographique des adresses IP.

Un service complètement managé peut encore augmenter la sécurité. L'application DDS peut ainsi être par exemple configurée, maintenue et gérée via un canal crypté. Ce type de service ainsi que la mise à jour en continu de la sécurité et le monitoring proactif du DDS garantissent aux clients une sécurité maximale en permanence – malgré la complexité de la thématique de DDoS.



Patrick Michel est Head of Sales chez BOLL Engineering.