Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Attaques de déni de service : Planification des mesures d'atténuation

Août 2012

Table des matières

Introduction

Ce livre blanc fournit une vue d'ensemble sur les attaques de déni de service, ainsi que sur les techniques et les outils employés, et décrit également la manière dont ces attaques peuvent être atténuées grâce à l'appliance DDoS Protector et les blades Check Point. Nous étudierons ensuite l'exemple concret d'un client qui a subi une attaque de déni de service, mais qui a pu bénéficier de l'assistance des équipes de Check Point pour atténuer l'attaque. Veillez noter que dans le présent document, le terme « déni de service » fait aussi bien référence aux attaques de déni de service qu'aux attaques de déni de service distribuées.

Les attaques de déni de service ciblent des réseaux et des services individuels, et les submergent de tellement de trafic qu'ils deviennent incapables de fonctionner. Que feriez-vous si tout à coup « ...le système ne répond plus... » ?

Scénario d'une attaque de déni de service

Nous avons tous déjà vu la scène classique d'un film de science-fiction dans laquelle les personnages principaux, qui ont la difficile tâche de surmonter les pires obstacles pour triompher, se retrouvent tout à coup face au message « ...le système ne répond plus... ». Ils ont perdu tout contrôle, naviguent à l'aveugle et sont apparemment incapables de s'en tirer.

C'est exactement ce qui se produit lorsque le réseau informatique d'une entreprise devient la proie d'une attaque de déni de service. Prenez n'importe quelle entreprise aujourd'hui, par exemple une petite banque régionale proposant des services bancaires au public, avec des titulaires de comptes, des services de versement de paie, de prêts hypothécaires et de prêts aux entreprises, de compensation de chèques et de transfert d'argent. Tout à coup, « ...le système ne répond plus... ». Ou ce peut-être un marchand qui fait la majorité de son chiffre d'affaires annuel pendant la saison des fêtes, et tout à coup, « ...le système ne répond plus... ». Ou encore une université pour laquelle sa présence en ligne est vitale au recrutement et à l'inscription de nouveaux étudiants pour générer des revenus et fournir des services scolaires quotidiens : plannings de cours, accès à des ressources pour les études et les travaux pratiques, communication d'urgence sur le campus, et tout à coup, « ...le système ne répond plus... ». Ou même une grande institution financière dont les activités quotidiennes sont essentielles à la continuité de l'activité économique d'un pays et du bien-être de sa population, et tout à coup, « ...le système ne répond plus... ».

Ce sont des exemples concrets illustrant la manière dont les attaques de déni de service ont aujourd'hui les moyens de submerger les réseaux protégés les plus sophistiqués, et causer des dommages aux grandes entreprises.

Qu'est-ce qu'une attaque de déni de service ?

Les attaques de déni de service ciblent les réseaux, les systèmes et les services individuels, pour les inonder d'une quantité de requêtes si élevée qu'ils deviennent incapables de fonctionner, ce qui dénie effectivement le service aux utilisateurs légitimes.

Une attaque de déni de service est lancée à partir d'une source unique pour submerger et désactiver le service ciblé, tandis qu'une attaque de déni de service distribuée est coordonnée et lancée simultanément depuis plusieurs sources pour submerger et désactiver le service ciblé. Ces sources multiples font généralement partie d'un « botnet » (un réseau d'ordinateurs compromis appelés « bots », diminutif de « robots ») et peuvent être dispersées dans le monde entier. Un botnet

peut agir de manière dynamique, en activant seulement certains robots à un moment donné pour attaquer la cible. Il peut donc être très difficile de détecter et de bloquer l'attaque.

Les symptômes d'une attaque de déni de service sont évidents : ralentissement de la performance du réseau, applications indisponibles ou réagissant lentement. Des dommages collatéraux sont également prévisibles : une attaque de déni de service qui inonde un réseau ou une application peut également influer sur la réactivité d'autres services situés sur le même segment de réseau.

Quoi qu'il en soit, les attaques de déni de service représentent une conduite inacceptable et sont même illégales. Elles violent l'esprit et les règles énoncées dans la RFC 1087 de l'IAB à propos d'*éthique* et d'*Internet*, et sont contraires à la loi dans la plupart des pays. En termes simples, il n'existe pas d'utilisation légitime des attaques de déni de service.

Qui utilise les attaques de déni de service et pourquoi ?

Les attaques de déni de service sont utilisées par toutes sortes d'organisations et de groupes pour faire avancer leur cause. Qui sont ces groupes et quelles sont leurs motivations ? Il existe trois catégories d'agresseurs :

1. Les hacktivistes
2. Les états
3. Les cybercriminels motivés par le gain

Les hacktivistes sont des individus ou des groupes motivés par des causes politiques ou sociales, qui ont principalement pour objectif de perturber les réseaux informatiques publics via des attaques de déni de service et autres types d'attaque. Selon Wikipédia[1], « Le terme a été inventé en 1996 par un membre du collectif de pirates Cult of the Dead Cow nommé Omega. » Si l'on considère que le piratage est une « effraction illégale d'un ordinateur », l'hacktivisme pourrait être défini comme étant « l'utilisation d'outils informatiques légaux et/ou illégaux à des fins politiques ». Au-delà des motivations sociales ou politiques, certains estiment qu'un sous-ensemble d'hacktivistes est en réalité lié au crime organisé et utilisent l'hacktivisme comme diversion pour dérober des informations à des fins lucratives.

Les attaques de déni de service conduites par des états, sans doute sanctionnées par un ou plusieurs gouvernements, sont également menées pour différentes raisons. Ces raisons sont classiques et évidentes : semer le chaos en perturbant les activités gouvernementales, ou tout simplement espionner et dérober des secrets d'état. Cependant, certaines attaques qui sembleraient provenir d'un état sont en fait des actes perpétrés par quelques individus dont les motivations sont leur propre perception du patriotisme.

L'appât du gain est un dénominateur commun pour la grande majorité des attaques de déni de service menées contre les gouvernements et les entreprises. Un agresseur peut par exemple être financé par une entreprise pour mener une attaque contre un concurrent. L'agresseur et l'acheteur profitent alors tous deux de l'opération. Dans d'autres cas, les attaques de déni de service ne sont qu'une diversion pour cacher l'objectif réel consistant à dérober des informations, notamment des dossiers personnels, des registres de comptes, de la propriété

Qui déclenche des attaques de déni de service et pourquoi ? Des groupes d'hacktivistes organisés et motivés pour faire avancer des causes sociales et politiques. Des états pour faire des ravages et perturber l'activité des gouvernements, et bien sûr pour espionner et voler des secrets d'état. Le crime organisé et les hacktivistes ne diffèrent vraisemblablement que sur le motif, le crime organisé étant généralement motivé par le gain financier, ce qui est sans doute le dénominateur commun à tous les groupes d'agresseurs.

intellectuelle, destinées à la revente ou à d'autres fins lucratives. Enfin, on peut noter quelques cas de « demande de rançon », dans lesquels les cibles sont forcées de payer une rançon sans quoi leurs systèmes deviendront victimes d'attaques de déni de service.

Types d'attaques de déni de service

Il existe aujourd'hui deux catégories principales d'attaques de déni de service : les attaques ciblant des réseaux et les attaques ciblant des applications. Même si les attaques menées contre les applications sont devenues plus fréquentes ces deux dernières années, les attaques menées contre les réseaux restent une technique de perturbation efficace couramment utilisée.

1. **Attaques de déni de service par inondation de réseau**
   Appelées également attaques volumétriques, ces attaques envoient d'énormes quantité de trafic UDP, SYN ou TCP sans importance pour consommer de la bande passante réseau et submerger les équipements réseau, ce qui rend le segment réseau, voire l'ensemble du réseau, inutilisable.
2. **Attaques de déni de service contre des applications**
   Les attaques de déni de service contre des applications ciblent des applications et les submergent de requêtes apparemment légitimes jusqu'à ce qu'elles ne puissent plus réagir. Ces attaques passent le plus souvent complètement inaperçues car elles émettent un petit volume de trafic qui consomme lentement les ressources jusqu'à ce que l'application s'arrête de fonctionner.

Ces deux types d'attaques peuvent être classés dans les catégories suivantes :

Asymétrie de l'utilisation des ressources
L'objectif de cette attaque est tout simplement de submerger les capacités de la cible. Il s'agit d'une attaque de déni de service menée contre un réseau ou une application dans laquelle l'agresseur a plus de ressources à sa disposition, en termes de capacité de traitement et/ou de bande passante, que la cible, et les utilise pour submerger la cible.

Attaque de déni de service pour diversion
Une attaque de déni de service est parfois utilisée comme diversion pour détourner l'attention de l'équipe de sécurité de la cible tandis que les agresseurs ont d'autres objectifs.

Méthodes et outils d'attaques de déni de service

Il existe aujourd'hui un large éventail de techniques et d'outils d'attaques de déni de service, enrichi régulièrement. Selon ce que l'agresseur veut infliger en termes de perturbation et d'impact, il existe probablement une technique ou un outil qui l'aidera à y parvenir. Il est important de noter que la durée de vie des outils est souvent très courte ; quelques mois seulement. Cette courte durée de vie illustre bien l'importance et l'efficacité des mesures de protection contre les attaques de déni de service, mais illustre également la résilience des agresseurs et leur capacité à créer de nouvelles méthodes et outils d'attaques de déni de service.

En fonction du type de perturbation et d'impact qu'un agresseur souhaite infliger, il existe une technique ou un outil qui les aidera à y parvenir. La durée de vie des outils d'attaque est généralement très courte, ce qui met en évidence l'importance et l'efficacité des mesures de protection contre les attaques de déni de service, mais souligne également la volonté de la communauté des agresseurs de création de nouvelles méthodes et outils d'attaques de déni de service.

Cette section donne un aperçu des techniques et des outils d'attaques de déni de service, allant de quelques-unes des techniques d'attaque d'origine radicalement simples, aux boîtes à outils clé en main sophistiquées d'aujourd'hui. Veuillez noter qu'il existe beaucoup plus de techniques et d'outils d'attaques de déni de service qu'il n'est mentionné ici.

Attaques SYN Flood
L'objectif de ces attaques est d'épuiser les ressources de la cible par un flot de connexions à moitié ouvertes. L'agresseur envoie à la cible des demandes d'ouverture de connexion (TCP/SYN) à plusieurs reprises à partir d'une adresse source usurpée. La cible accuse réception des demandes (SYN-ACK) auprès de la source usurpée, ouvrant ainsi une connexion pour chaque demande. Cependant, l'ouverture de la connexion en trois temps n'est jamais finalisé, car la source usurpée ne répond jamais, et la victime cible est finalement inondée de connexions semi-ouvertes. Les versions actuelles des applications les plus courantes sont généralement protégées contre ce type d'attaque de déni de service.

Attaques HTTP Flood
Ces attaques ciblent généralement des services qui génèrent une charge élevée tels que des moteurs de recherche sur un site ou des activités liées à des bases de données, qui consomment plus de ressources et ralentissent les services, ou les stoppent. Il existe différents types d'attaques HTTP Flood.

- **Attaques simples par « GET » ou « PUT »** — L'agresseur envoie des requêtes GET ou POST HTTP ciblant la page principale jusqu'à ce que le segment réseau, le serveur cible ou un autre équipement réseau soit débordé et ne puisse traiter les demandes. Ces attaques peuvent être modifiées par l'ajout de paramètres aléatoires dans les requêtes HTTP pour contourner les réseaux de diffusion de contenus (CDN) ou les services de mise en cache, ce qui redirige le trafic directement vers le site web plutôt que le CDN.
- **Attaques HTTP « lentes »** — Similaires aux attaques SYN Flood, mais au niveau de HTTP. Ces attaques épuisent les ressources des serveurs web via l'ouverture continuelle de nouvelles connexions. Les agresseurs envoient une requête « GET » puis réduisent sa taille à une petite valeur. Cela force les serveurs web à envoyer leur réponse dans des paquets plus petits que d'ordinaire. Les connexions restent ouvertes plus longtemps que d'ordinaire, et la table des connexions des serveurs se remplit complètement. Ces attaques sont lentes et silencieuses, et ne présentent aucun signe évident tel que l'utilisation élevée du processeur. Une attaque similaire peut être menée par l'utilisation de commandes POST, par lesquelles l'agresseur prétend envoyer une grande quantité de données, qui n'est au final jamais envoyée.
- **Attaques HTTP Flood sur une ressources ciblée** — L'agresseur identifie sur le site de la victime une ressource qui entraîne une charge particulièrement lourde sur les serveurs, telle qu'un moteur de recherche ou l'interrogation de la base de données. L'agresseur attaque alors ce service avec généralement des volumes de trafic très faibles. Un serveur capable de traiter généralement des milliers de connexions par seconde peut être complètement submergé et rendu inaccessible avec seulement 20 connexions par seconde via ce type d'attaque. « Slowloris » est un exemple d'outil qui utilise cette technique.

Les attaques ciblant les applications peuvent être lentes et silencieuses, et peuvent passer inaperçues. Lorsqu'il subit une attaque menée via l'outil Slowloris, un serveur capable de traiter habituellement des milliers de connexions par seconde peut être complètement submergé et rendu inaccessible en seulement une vingtaine de connexions par seconde avec ce type d'attaque.

Attaques UDP Flood
L'agresseur envoie des paquets contenant des datagrammes UDP à la cible, qui recherche alors l'application associée sur le port souhaité, et n'en trouvant pas, doit donc répondre par un paquet ICMP de destination injoignable. Cette attaque se poursuit jusqu'à ce que le réseau, le pare-feu ou un autre équipement réseau de la victime soit submergé. L'agresseur peut également usurper l'adresse IP des paquets UDP pour rester anonyme.

Attaques ICMP Flood
Commun dans les années 1990, ce type d'attaque de déni de service est maintenant généralement bloqué par les pare-feux et les politiques de sécurité des équipements réseau. Il existe deux techniques d'attaque ICMP Flood :

- **Ping Flood** — L'objectif de cette attaque consiste à submerger le réseau de trafic ICMP. Dans ce type d'attaque, l'agresseur envoie un grand volume de requêtes « ping » en utilisant l'adresse de la victime comme adresse source, qui est alors submergée de réponses aux requêtes ping.
- **Attaque Smurf** — L'objectif de cette attaque consiste à submerger la cible de trafic ICMP en utilisant le service de diffusion IPS. Les agresseurs génèrent du trafic ping ICMP en utilisant l'adresse de la victime comme adresse source, et en l'envoyant aux adresses de diffusion du réseau IP qui la diffusent à tous les hôtes, qui répondent ensuite à la victime, la submergeant de trafic.

Attaques de déni de service par ralentissement (LDOS)
L'objectif de ces attaques consiste à ralentir le débit TCP du système ciblé sans être détecté. Un agresseur exploite les faiblesses de synchronisation du protocole TCP pour mettre les équipements TCP de la victime en mode de retransmission continu, ce qui réduit considérablement le débit TCP.

Attaques P2P
L'objectif de ces attaques consiste à générer un afflux massif de demandes de connexion quasi simultanées auprès de la cible. Des bugs du logiciel serveur de peer-to-peer permettent aux agresseurs de détourner les clients du hub peer-to-peer, les déconnecter de leur réseau peer-to-peer, et les connecter au site de la victime, créant ainsi un afflux massif de demandes de connexion. Les clients des réseaux peer-to-peer pouvant se compter par dizaines, voire centaines de milliers, l'ampleur de ces attaques est immédiatement écrasante pour la victime.

Low-Orbit Ion Canon (LOIC)[2]
TIl s'agit d'un outil d'attaque de déni de service dont l'objectif est de perturber le service ciblé en l'inondant de paquets TCP ou UDP. Initialement un outil open source de test de charge et d'attaque de déni de service, il fait désormais partie du domaine public et est généralement utilisé comme outil d'attaque de déni de service. Le groupe Anonymous a utilisé LOIC pour attaquer plusieurs organismes gouvernementaux, y compris le FBI et le Ministère de la justice américains, dans le cadre de sa campagne de protestation contre la fermeture du site d'hébergement de fichiers MegaUpload, ainsi que les loi américaines SOPA (Stop Online Piracy Act) et PIPA (Preventing Real Online Threats to Economic Creativity and theft of Intellectual Property Act) relatives au piratage de propriétés intellectuelles.

La simple menace d'une attaque de déni de service force les cibles à investir. L'attaque « Operation New Son » programmée pour le 25 mai 2012 a publiquement déclaré cibler des entreprises connues. La menace a conduit un grand nombre de ces entreprises à prendre des mesures en vue de l'attaque. En fin de compte, il semble qu'aucune attaque n'ait été effectivement menée à cette date.

Une attaque appelée « Operation New Son » (OpNewSon) prétendument menée par Anonymous devait avoir lieu le 25 mai 2012 et devait utiliser LOIC comme outil de choix. L'attaque consistait à cibler de nombreuses sociétés connues afin de provoquer des perturbations et des interruptions. La menace a contraint la plupart de ces entreprises à prendre des mesures en vue de l'attaque. Il semble cependant qu'aucune attaque n'ait été effectivement lancée à cette date.[3]

High-Orbit Ion Canon (HOIC)
Cet outil d'attaque de déni de service est le récent successeur de LOIC. Alors que LOIC s'attaque aux protocoles TCP, UDP et HTTP, HOIC s'attaque uniquement au protocole HTTP. L'objectif de HOIC consiste à perturber simultanément plusieurs services ciblés en les inondant de requêtes HTTP POST et GET. HOIC diffère de LOIC dans deux autres domaines. Tout d'abord, il peut attaquer jusqu'à 256 adresses web différentes en même temps, ou encore multiplier par 256 sa puissance d'attaque sur une cible unique. Ensuite, il peut modifier dynamiquement sa signature attaque, ce qui rend sa détection extrêmement difficile.

Slowloris
Il s'agit d'un outil d'attaque de déni de service ciblant des applications, dont l'objectif consiste à lentement stopper le serveur web ciblé. L'attaque ouvre lentement des connexions au serveur de la victime et les maintient ouvertes en envoyant des bribes d'informations supplémentaires, mais sans jamais compléter la requête. Il poursuit cette tactique jusqu'à ce que le serveur web ciblé soit submergé de requêtes (nombre maximum de connexions atteint, mémoire épuisée) et ne puisse plus fonctionner.

R-U-Dead Yet (RUDY)
Il s'agit d'un outil d'attaque de déni de service ciblant des applications, dont l'objectif consiste à maximiser l'utilisation des sessions du serveur web ciblé. Semblable à Slowloris, RUDY consomme des sessions par l'envoi répété de transmissions POST avec des en-têtes volumineux.

Google+[4]
Il y a moins d'un an de cela, cette technique exploitait les services publics de Google sous forme de proxy pour lancer des attaques de déni de service sur une cible. L'automatisation par un script permettait de submerger la cible par le nombre de demandes. L'équipe de sécurité de Google a réagi rapidement et a corrigé la vulnérabilité permettant de détourner le service.

THC-SSL-DOS (appelé également THC-SSL-DDoS)[4]
Il s'agit d'un outil d'attaque de déni de service contre des applications, visant des serveurs web. Dans ce scénario, un seul ordinateur peut submerger un serveur web prenant en charge la renégociation SSL. Cette option de configuration permet au serveur web de créer une nouvelle clé secrète pour la connexion SSL actuelle, ce qui force une renégociation et consomme des ressources. L'envoi de nombreuses requêtes de ce type peut submerger le serveur web.

Apache Killer[4]
Il s'agit d'une technique dont la durée de vie a été très courte. Elle est apparue dans le courant du second trimestre 2011 et a été résolue durant ce même trimestre. Cette technique exploitait des vulnérabilités d'Apache HTTPD pour provoquer l'épuisement des ressources, principalement la mémoire, par l'envoi d'un grand nombre de plages d'en-tête HTTP erronées au serveur. Apache a résolu cette vulnérabilité dans les versions les plus récentes.

Slowloris est un outil d'attaque de déni de service dont l'objectif est de lentement et silencieusement rendre des serveurs web cible inaccessibles. L'agresseur ouvre des connexions avec le serveur de la victime, et les maintient ouvertes en envoyant des bribes de données supplémentaires sans jamais compléter la requête. Il poursuit cette tactique jusqu'à ce que la cible soit surchargée de requêtes, atteint le nombre de connexions maximales ou épuise sa mémoire, et ne peut plus fonctionner.

Bot Darkness (Optima)[5]
Initialement publiée en 2009, la boîte à outil de création de bot d'attaque de déni de service distribuée « Optima », est depuis devenue « Darkness Optima », et sa 10ème version a été publiée en octobre 2011 sous le nom « Darkness X Bot ». Selon une publicité :

« Darkness X, bot d'attaque de déni de service distribuée puissant avec tableau de bord d'administration « Optima » (bons baisers de Russie), 4 types d'attaques de déni de service distribuées / modules complémentaires / 7 packages / support technique »

La boîte à outils propose des techniques d'attaque HTTP, ICMP, SYN et UDP, la possibilité d'attaquer simultanément plusieurs adresses d'un serveur, des méthodes pour contourner les protections, et un support technique en temps réel.

Dirt Jumper et ses variations[6,7]
Il s'agit d'un autre exemple de boîte à outils qui a évolué au fil du temps. Publiée initialement en 2009 sous le nom « Russkill » et proposant des attaques HTTP et SYN Flood, elle est devenue « Dirt Jumper » début 2011. Son prix de vente initial était de 600 dollars. « Dirt Jumper September » a suivi fin 2011. Cette boîte à outils propose plusieurs techniques d'attaques de déni de service :

- **Inondation HTTP (HTTP Flood)** — Provoque la surcharge d'un serveur par l'envoi simultané d'un grand nombre de requêtes HTTP
- **Inondation synchrone (Synchronous Flood)** — Provoque la surcharge d'un serveur par la répétition de multiples requêtes simultanées
- **Inondation par téléchargement (Downloading Flood)** — Provoque la surcharge d'un serveur par la répétition de multiples requêtes simultanées
- **Inondation POST (Post Flood)** — Consomme la bande passante d'un serveur web ciblé par des commandes GET et POST simultanées

Les boîtes à outil « Dirt Jumper » continuent d'évoluer et de proliférer. « Trojan.Khan » semble en être une copie exacte, tandis que Di BoTNet en est une version qui intègre la possibilité de désactiver les bots concurrents.

Ce ne sont que quelques exemples de techniques et d'outils de déni de service, mais il est clair que la communauté des agresseurs fait preuve de résilience et est financièrement motivée pour mettre au point de nouveaux outils provoquant des perturbations et des dommages. Bien que les techniques Google+, TC-SSL-DDoS et Apache Killer n'ont eu qu'une courte durée de vie, elles ont cependant été très efficaces. Les boites à outil Darkness/Optima et Dirt Jumper présentent les caractéristiques d'une véritable gestion de produit et d'une évolution robuste. Pour autant que la motivation de lancer des attaques de déni de service soit souvent d'ordre financier, il est clair que la demande en techniques d'attaques de déni de service et d'outils clés en main est forte et continue. Elle est également lucrative pour leurs auteurs.

Tout comme la motivation de mener des attaques de déni de service est souvent d'ordre financier, il est clair que le marché des techniques d'attaques de déni de service et d'outils clé en main est robuste, résistant même, pour ne pas mentionner lucratif pour ses auteurs.

Comment se défendre contre les attaques de déni de service ?

À ce stade, il devrait être clair qu'une protection contre les attaques de déni de service est extrêmement difficile à mettre en œuvre. En fait, il n'existe pas de solution miracle pour protéger complètement contre les attaques de déni de service. Ces attaques frappent généralement sans avertissement, ce qui les rend très efficaces. Cela souligne l'importance d'une préparation par avance. Afin de se préparer, chaque entreprise devrait se demander :

« Que devons-nous faire si une attaque de déni de service nous frappe maintenant et que nos systèmes ne répondent plus ? »

La réponse à cette question est à la base de l'élaboration d'un plan d'action pour atténuer les attaques de déni de service et s'en protéger. Dès que vous tombez sous le coup d'une attaque de déni de service lourde et que vos systèmes ne répondent plus, la situation devient d'une urgence extrême, très confuse, très stressant et très tendue. Qui en est à l'origine ? Pourquoi l'ont-ils lancée ? Comment l'ont-ils lancée ? Combien de temps va-t-elle durer ? Que devons-nous faire ? Qui doit être prévenu ? Quels partenaires ou fournisseurs peuvent nous aider ? La direction demande « que faites-vous pour la stopper et quand l'aurez-vous stoppée ?! » par l'intermédiaire d'une ligne ouverte. Et ainsi de suite. La planification est absolument indispensable !

L'élaboration d'un « Plan de mesures d'atténuation » est vraiment essentiel pour réduire l'impact des attaques de déni de service, voire les stopper. En outre, l'équipe informatique doit être en mesure d'exécuter immédiatement le plan en cas d'attaque de déni de service.

Élaborez un plan de défense !
L'élaboration d'un « Plan de mesures d'atténuation» est véritablement essentielle pour atténuer et éventuellement stopper une attaque de déni de service. En outre, la totalité de l'équipe informatique devrait avoir connaissance du plan pour être en mesure de l'exécuter immédiatement.

Considérez les éléments suivants d'un solide plan d'atténuation d'attaques de déni de service :

1.Qui est responsable du plan ?
Dès le début et tout au long de l'attaque de déni de service, il est important d'avoir déjà clairement désigné un responsable approprié en charge. Qui sont les membres de l'équipe de traitement des incidents, quels sont leurs rôles, et qui est en charge de diriger l'équipe et les efforts d'atténuation ?

2. Quelles mesures doivent être prises ?
A. Analyser le trafic
Utilisez des outils internes et externes existants pour analyser le trafic et identifier le profil de l'attaque. Par exemple :
- Identifier les origines géographiques suspectes
- Vérifier si ces adresses IP suspectes correspondent à des adresses IP dangereuses connues
- Identifier les pics de types de trafic et de trafic d'application, ainsi que les pics de trafic en fonction de la provenance géographique, etc.
- Identifier les méthodes de connexion qui diffèrent de leur norme

B. Implémenter des règles de blocage
Définissez des règles pour bloquer le trafic répondant au profil d'attaque identifié. Par exemple :
- Bloquer la totalité du trafic provenant de pays suspects
- Bloquer les adresses IP connues pour être des adresses IP dangereuses
- Bloquer tous les types de trafic/d'attaque suspects identifiés
- Bloquer la totalité du trafic selon le modèle de connexion suspect identifié et/ou tous les schémas de connexion qui diffèrent de leur norme
- Tout autre type de blocage approprié

3. Demander l'aide de votre FAI

Contactez votre FAI pour déterminer quels services et outils de protection sont proposés pour vous aider à atténuer et bloquer les attaques de déni de service. Maîtrisez et documentez les processus pour le contacter et mettre en œuvre ses services. Quels services propose-t-il, et dans quelles circonstances doit-il être contacté ? Comment ces services sont-ils facturés — par incident, selon la quantité de données, ou par une prime d'assurance trimestrielle ou annuelle ? Le FAI peut offrir une assistance considérable pour atténuer les attaques de déni de service, mais il faut le temps de comprendre ses services, ses processus et les coûts, avant et non pendant une attaque de déni de service.

4. Demander l'assistance de tiers spécialisés

Au-delà du FAI, des sociétés tierces proposent des services spécialisés d'atténuation d'attaque de déni de service, appelés notamment « tuyaux propres ». Ces services sont parfois la seule option viable pour atténuer d'importantes attaques de déni de service volumétriques. Encore une fois, dans le cadre de votre plan d'atténuation d'attaques de déni de service, identifiez et contactez ces fournisseurs pour comprendre quels sont les services qu'ils proposent, leurs coûts, leurs processus et les étapes requises pour faire appel à leurs services. Par exemple, comprenez et documentez les étapes requises pour rediriger la totalité du trafic Internet vers leurs installations pour « nettoyer les tuyaux » en cas d'attaque volumétrique.

5. Contacte les autorités

Contactez les autorités, telles que les cellules anticriminalité spécialisées de la police de votre pays si vous avez l'opportunité de mener une action en justice. Assurez-vous de conserver les journaux et autres preuves qui pourraient être utiles pour identifier et poursuivre les agresseurs. Les autorités nationales collaborent de plus en plus chaque jour pour identifier conjointement et stopper les pourvoyeurs de spam, de botnets, d'attaques de déni de service et autres cybercriminels.

La création d'un plan d'action contre les attaques de déni de service est de loin l'étape la plus importante que vous puissiez mettre en œuvre pour vous défendre contre une éventuelle attaque de déni de service. De l'avis de l'auteur de ce livre blanc, l'importance du plan ne peut être surestimée. Lorsque vous tombez sous le coup d'une attaque de déni de service, soit vous savez exactement ce qu'il faut faire dès l'instant où l'attaque est identifiée, soit vous vous laissez submerger par une vague de confusion, d'incertitude, de panique et la pression de la direction parce que « ...le système ne répond plus... ».

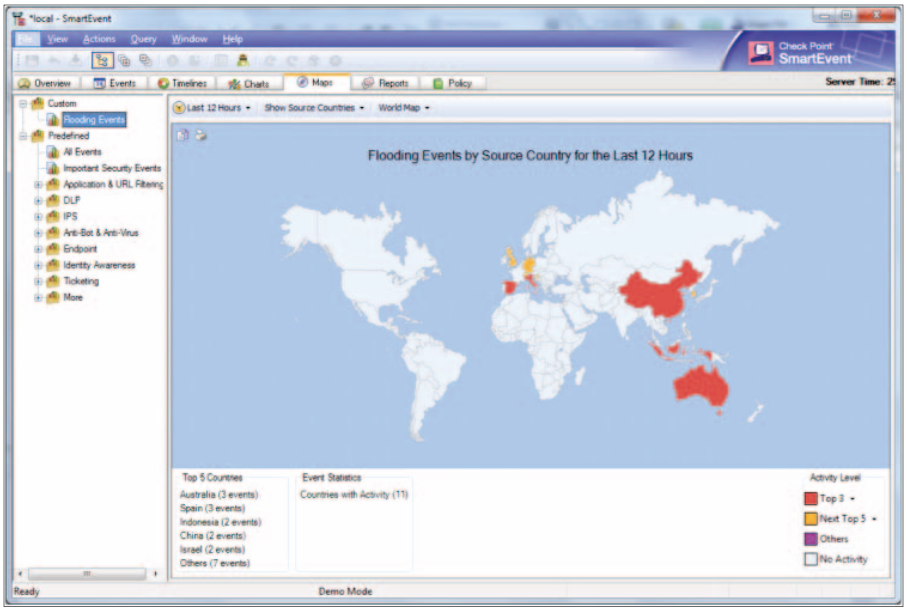
Lorsque vous tombez sous le coup d'une attaque de déni de service, soit vous savez exactement ce qu'il faut faire à partir de l'instant où l'attaque est identifiée, soit vous vous retrouvez submergé par une vague irrésistible de confusion, d'incertitude et de panique, et par la pression de la direction parce que « ...le système ne répond plus... ».

Blades Check Point pour atténuer les attaques de déni de service

Bien qu'il n'y ait pas de solution miracle contre les attaques de déni de service, un sous-ensemble de blades Check Point peuvent se révéler être des outils très efficaces pour vous aider à atténuer les attaques de déni de service. Les utilisateurs qui ont déployé ces blades peuvent facilement exploiter leurs possibilités au cours d'une attaque de déni de service pour identifier les sources de l'attaque, les méthodes d'attaque et autres éléments d'identification afin d'atténuer l'attaque.

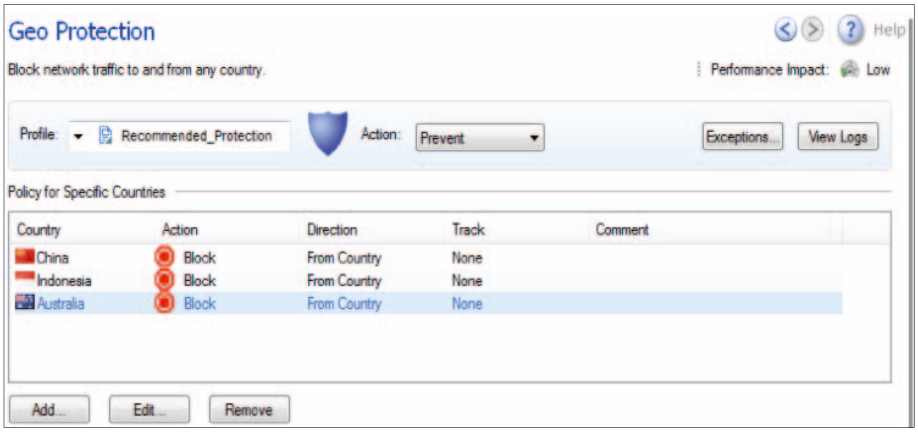
SmartEvent
La blade SmartEvent est l'outil indispensable pour identifier rapidement le profil et les méthodes d'attaque. Que ce soit à l'aide de son panneau représentant visuellement les principales sources géographiques d'attaque, ou de son écran d'analyse des alertes avec tri et corrélation automatiques permettant d'identifier les méthodes d'attaque, SmartEvent est un outil essentiel pour analyser et identifier les modèles de trafic d'une attaque de déni de service distribuée.

La capture d'écran ci-dessous illustre par exemple les principaux événements par pays d'origine.



Il est possible de facilement bloquer les pays incriminés de façon permanente ou seulement pendant la durée de l'attaque.

Fonctionnalité SmartLog de la blade Logging and Status



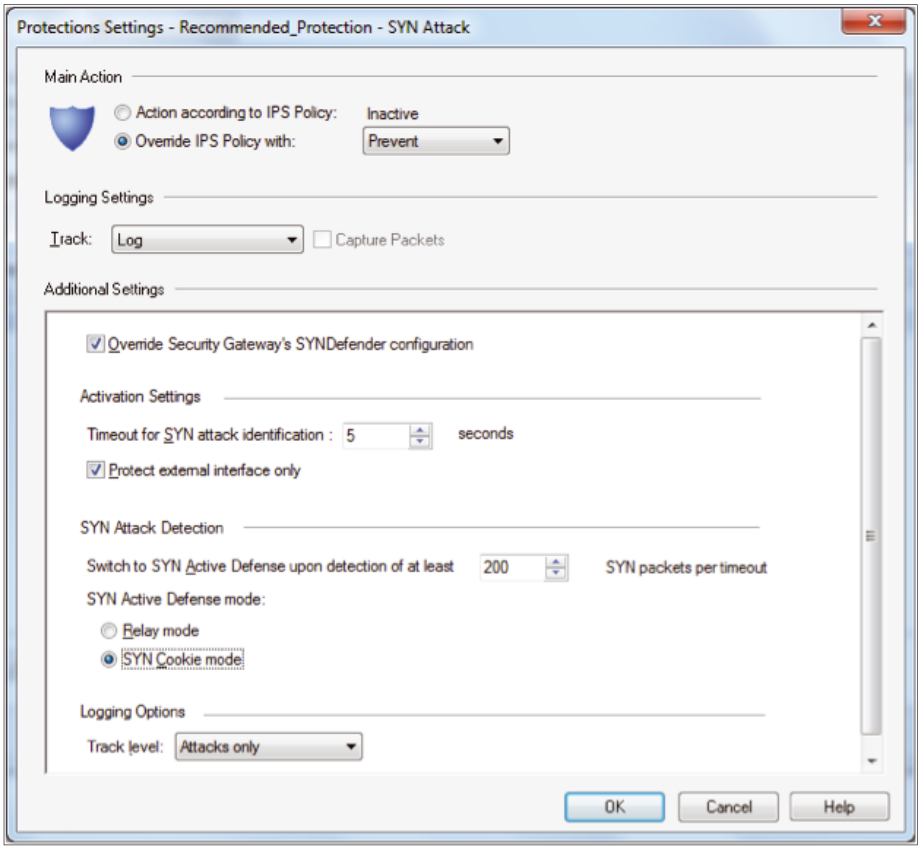
La fonctionnalité SmartLog de la blade Logging and Status permet d'identifier rapidement les profils et méthodes d'une attaque de déni de service. SmartLog fournit une analyse approfondie des journaux grâce à des fonctions de recherche en une fraction de seconde parmi des milliards de lignes de journal et depuis

Les blades Check Point sont des outils très efficaces pour atténuer les attaques de déni de service. Elles peuvent facilement être mises à profit pour identifier les sources d'attaque, les pays d'où elles proviennent, les modèles d'attaque et d'autres éléments d'identification pour aider à atténuer l'attaque.

plusieurs journaux, périodes, passerelles, domaines, actions, utilisateurs ou données géographiques.

Blade Firewall
Le pare-feu est en première ligne pour atténuer les attaques de déni de service en fonction de certains éléments d'attaque. Les fonctions suivantes peuvent être employées :

- **Vieillissement agressif** — Les connexions restant inactives au-delà du seuil défini peuvent être supprimées de la table des connexions de la passerelle. Cette technique protège contre les attaques lentes consommant des connexions. Le seuil par défaut est de 60 secondes, mais il peut être nettement abaissé en cas d'attaque.
- **Quota réseau** — Quota réseau — Une limite est appliquée au nombre de connexions autorisées à partir de la même adresse IP source. Lorsqu'une adresse source dépasse le nombre de connexions autorisées, la fonction peut soit bloquer toutes les nouvelles tentatives de connexion provenant de cette adresse ou surveiller l'événement.
- **Blocage du trafic ICMP/UDP** entrant au périmètre grâce à une règle placée en tête des autres règles.
- **Minuteurs Stateful Inspection** — Abaissez ces minuteurs pour protéger contre les attaques de déni de service lentes et consommatrices de ressources :
  - Timeout de début, de session et de fin (TCP)
  - Timeout UDP, ICMP et session virtuelle IP
- Créez un service personnalisé avec des règles de temporisations de session plus agressives.



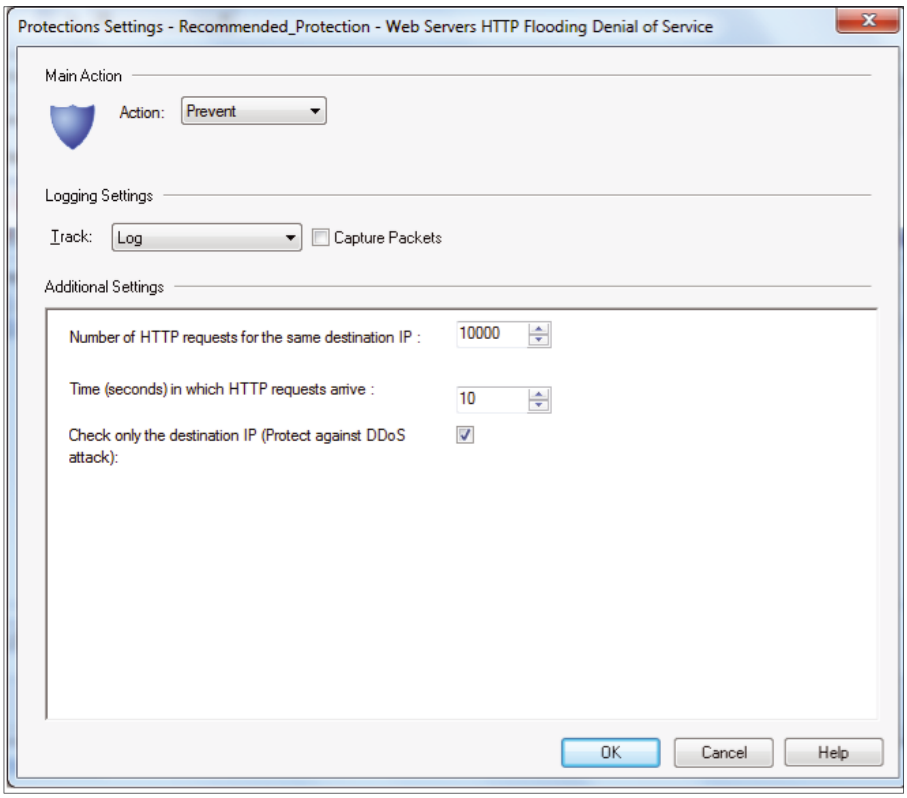
Les solutions Check Point qui peuvent vous aider à lutter contre les attaques de déni de service sont

- Blade SmartEvent
- Blade Firewall
- Blade IPS
- DDoS Protector

Blade IPS

La blade IPS offre des possibilités supplémentaires pour atténuer et bloquer les attaques de déni de service. En voici quelques exemples :

- **Blocage par pays** — Blocage de la totalité du trafic en provenance de pays semblant être à la source de l'attaque et également des pays avec lesquels votre entreprise ne fait pas d'affaires.
- **Signature de détection de ver** — L'activation de cette signature permet de bloquer les URL d'attaque identifiées.
- **Taille des paquets TCP stricte** — Protection contre deux vulnérabilités spécifiques de TCP souvent exploitées par les attaques de déni de service. La première consiste à configurer la fenêtre de réception TCP à une petite taille pour ensuite inonder de connexions TCP. La seconde consiste à submerger le système de connexions ayant un état d'attente infinie.
- **Protection SYN Flood** — Une protection supplémentaire et spécifique contre les attaques SYN Flood. Dans la capture d'écran ci-dessous, la protection contre les attaques SYN est activée et définie dans le « Profil recommandé ». Plus précisément, lorsque la blade IPS détecte au moins 200 paquets SYN par intervalle de 5 secondes, la protection est activée pour bloquer le trafic incriminé.
- **Protection HTTP Flood** — Cette protection des serveurs web contre les attaques de déni de service visant le protocole HTTP apporte plus de protection contre les attaques par inondation HTTP. Dans la capture d'écran ci-dessous, la protection contre les attaques HTTP est activée et définie dans le « Profil recommandé ». Plus précisément, lorsque plus de 10 000 requêtes HTTP sont dirigées vers la même adresse IP de destination en moins de 10 secondes, la protection est activée pour bloquer le trafic incriminé.



Pour vous préparer à atténuer une attaque de déni de service, il est important de comprendre et de documenter dans votre plan d'atténuation tous les outils et les techniques d'atténuation disponibles dans vos solutions Check Point et autres produits de sécurité. Vos produits de sécurité existants sont votre première ligne de défense pour détecter et vous protéger contre les attaques de déni de service, et vous permettent d'analyser le trafic puis d'étendre les mesures de sécurité pour atténuer les attaques.

Cette protection peut être réglée pour s'adapter à votre environnement spécifique. Configurez-la d'abord en mode de détection pour 10 requêtes HTTP par seconde. Évaluez vos journaux, ajustez les seuils, et en l'absence de journaux générés à partir de trafic normal, augmentez le nombre de requêtes autorisées et passez la protection en mode blocage.

Les blades Check Point proposent de nombreuses fonctionnalités pour combattre les attaques de déni de service : des outils d'analyse permettant d'identifier le profil du trafic d'attaque, à des fonctions de sécurité permettant de détecter et de bloquer plusieurs types d'attaques de déni de service. Pour vous préparer à atténuer une attaque de déni de service, il est important de comprendre et de documenter dans votre plan d'atténuation tous les outils et les techniques d'atténuation disponibles dans votre solution Check Point et autres produits de sécurité. Vos produits de sécurité existants sont votre première ligne de défense pour détecter les attaques de déni de service, et sont votre boîte à outils essentielle pour analyser le trafic et étendre les mesures de sécurité pour atténuer les attaques.

Check Point DDoS Protector

Check Point DDoS Protector est une solution d'atténuation d'attaques de déni de service qui emploie des logiciels spécialisés fonctionnant sur une plate-forme avec accélération matérielle. Elle est déployée à l'extérieur du pare-feu de périmètre pour détecter et atténuer les attaques de déni de service avant qu'elles ne puissent affecter le réseau de production. Protector s'appuie sur trois techniques de protection pour protéger contre les attaques de déni de service :

- **Protection contre les inondations réseau** - Protector utilise l'analyse comportementale pour fournir une protection contre les inondations réseau. Protector étudie les modèles de trafic quotidiens et hebdomadaires du réseau et des applications, pour identifier ensuite le trafic anormal, en particulier les pics dus à des attaques.
- **Protection contre les inondations serveur** - Protector protège contre l'utilisation abusive des ressources avec génération automatique de signature. Il génère automatiquement de nouvelles signatures pour atténuer les attaques, tandis que des signatures prédéfinies se chargent des mauvais comportements. Les adresses IP sources, les protocoles, les seuils et la renégociation SSL font partie des éléments clés des signatures.
- **Protection de la couche applicative** - Protector bloque les outils automatisés et les faux utilisateurs à l'aide de techniques de questions/réponses, tandis que les utilisateurs légitimes sont redirigés en toute transparence vers la destination souhaitée.

DDoS Protector combine ces techniques pour atténuer efficacement les attaques de déni de service, en particulier pour les attaques lentes et silencieuses.

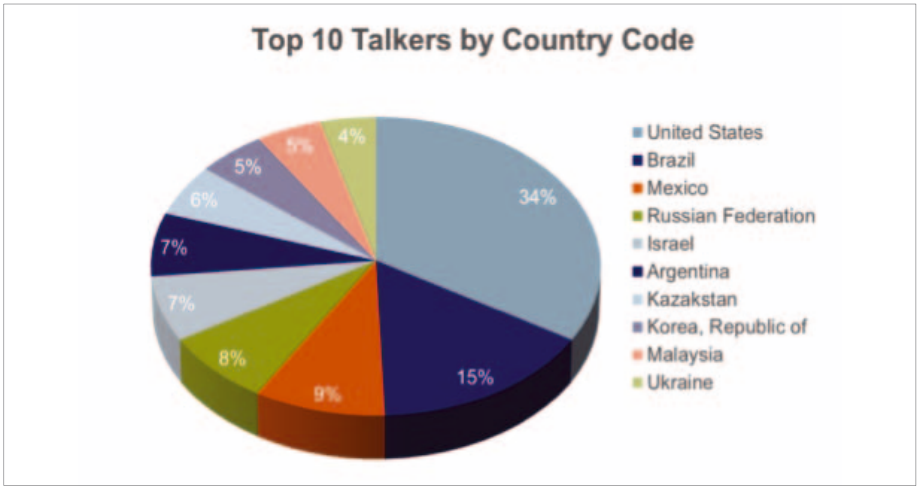
Exemple d'atténuation d'attaque de déni de service

Banque régionale américaine

Une petite banque régionale aux États-Unis est tombée sous le coup d'une attaque de déni de service et a contacté les équipes de Check Point pour lui venir en aide. L'attaque était déjà en cours depuis plusieurs heures quand Check Point a été contacté, le client a renforcé son équipe informatique et a pris contact avec les autorités. Comme le client n'avait pas de plan d'atténuation en place, les mesures d'atténuation ont été définies et déterminées à la volée.

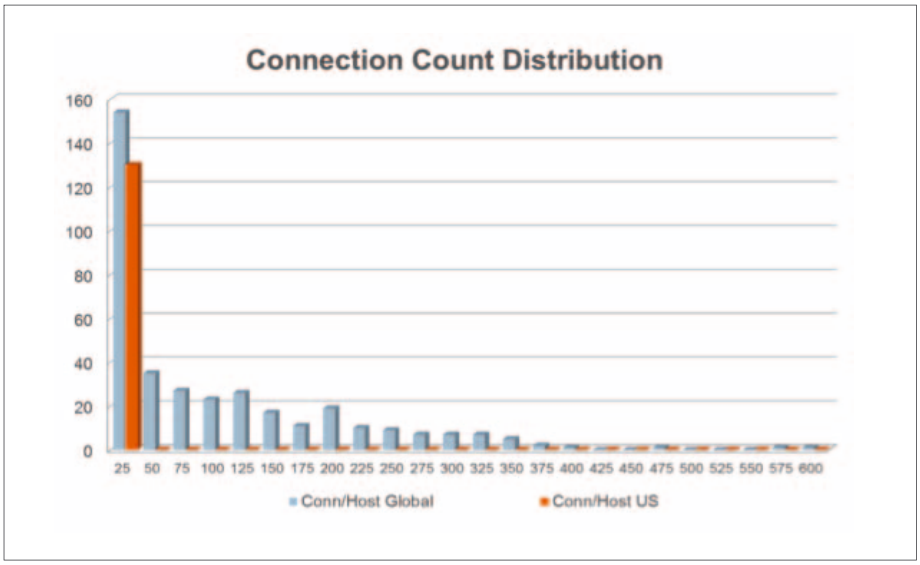
Une petite banque régionale américaine est tombée sous le coup d'une attaque de déni de service. N'ayant pas de plan d'atténuation en place, les mesures d'atténuation ont été définies et déterminées à la volée.

Dès que l'équipe Check Point est arrivée sur place, l'ingénieur sécurité a recherché dans les journaux SmartEvent les adresses IP, les provenances géographiques, les URL et les schémas de connexion. L'analyse des journaux via SmartEvent n'a pris que quelques minutes et a été très révélatrice. Tout d'abord, un simple tri sur le « pays source » dans l'écran des événements SmartEvent a immédiatement montré que la répartition géographique était mondiale :



pour cette petite banque régionale américaine, 66% du trafic provenait de l'étranger, et 35% du trafic provenait d'Europe et d'Asie.

Ensuite, l'analyse des journaux a révélé des données intéressantes sur le nombre de connexions par pays.



Encore une fois, rappelons qu'il s'agit d'une banque régionale et le graphique ci-dessus montre clairement que le nombre de connexions provenant d'hôtes américains (axe des y) n'est jamais supérieur à 25 (axe des x), tandis que le nombre de connexions provenant d'hôtes dans le reste du monde est clairement hors norme.

Les outils des blades Check Point ont permis d'identifier rapidement que les attaques avaient des empreintes spécifiques pour lesquelles de règles de pare-feu et IPS ont pu être définies pour les bloquer.

Enfin, l'équipe Check Point a défini une signature IPS personnalisée pour analyser les empreintes TCP. Cette signature a révélé la présence de petits paquets TCP associés à de mauvaises adresses IP connues (Voir blade IPS, Taille des paquets TCP stricte, dans ce document) :

Mesures d'atténuation

L'analyse a révélé plusieurs modèles de comportement de l'attaque de déni de service menée contre la banque. Grâce à ces informations, l'équipe Check Point et le client ont pu implémenter des règles pour bloquer le trafic suspect. Plus précisément, les mesures d'atténuation suivantes ont été prises :

- **Blade Firewall** — Ajout d'une règle de quota pour limiter à moins de 25 le nombre de connexions à certains serveurs.
- **Blade IPS** — Ajout de règles pour bloquer le trafic provenant d'environ 40 pays.
- **Blade IPS** — Déploiement d'une signature personnalisée pour mettre en liste noire les utilisateurs fermant les connexions comportant de petits paquets TCP.

Les blades Firewall, IPS et SmartEvent ont fourni ici les outils nécessaires à l'analyse du trafic et l'identification des modèles de l'attaque de déni de service. Grâce à ces informations et au profil de comportement, l'équipe Check Point et le personnel technique du client ont pu définir et déployer de nouvelles règles pour atténuer l'attaque de déni de service avec succès. Notez cependant que si le réseau de la banque avait été protégé par une appliance Check Point DDoS Protector, il est très probable qu'elle ait été automatiquement protégée contre l'attaque sans avoir à impliquer l'équipe Check Point.

Résumé

La menace des attaques de déni de service est réelle, et le problème ne va pas disparaître. La communauté des agresseurs est active et motivée par une forte demande en outils pour provoquer des perturbations et des dommages au nom de causes nationales ou sociales, et bien entendu à des fins lucratives. Bien qu'il n'existe pas de solution miracle pour protéger contre toutes les formes d'attaques de déni de service, de nombreuses mesures peuvent être mises en œuvre pour atténuer une attaque lorsqu'elle se produit. La préparation d'un plan d'atténuation précisant le leadership, les outils, les étapes d'analyse et les mesures d'atténuation qui devraient être mises en œuvre en cas d'attaque de déni de service, est la première étape. En l'absence d'un tel plan, l'équipe de sécurité devra improviser un plan sur le moment pour atténuer l'attaque.

Pour obtenir des informations complémentaires sur les solutions Check Point mentionnées dans le présent livre blanc, veuillez consulter les liens suivants :

Blade SmartEvent

Blade Firewall

Blade IPS

DDoS Protector

Veillez à préparer un plan d'atténuation de sorte que votre équipe de sécurité n'ait pas à improviser en temps réel pour atténuer les attaques.

[1] Wikipédia

[2] Alerte (TA12-024A) Attaque de déni de service des « Anonymous » — US-Cert

[3] threatpost.com

[4] Plan d'atténuation d'attaques de déni de service en 2011 — SecureList

[5] « A Peek Inside the Darkness (Optima) DDoS Bot » — Webroot Threat Blog

[6] Alerte ProLexic

[7] « A DDoS Family Affair: Dirt Jumper Bot Family Continues to Evolve » — Arbor Networks

À propos de Check Point Software Technologies Ltd.

Leader mondial de la sécurité sur Internet, Check Point Software Technologies Ltd. (www.checkpoint.com) est le seul acteur du marché à proposer des solutions de sécurité totale pour les réseaux, les données et les postes utilisateurs, via une plate-forme d'administration unifiée. Check Point assure aux clients un niveau optimal de protection contre tous types de menaces, simplifie l'installation et la maintenance des dispositifs de sécurité, et réduit leur coût total de possession. Précurseur de la technologie Firewall-1 et du standard de la sécurité des réseaux Stateful Inspection, Check Point est toujours à la pointe de la technologie. Grâce à sa nouvelle architecture dynamique Software Blade, Check Point offre des solutions à la fois fiables, flexibles et simples d'utilisation, qui peuvent être totalement personnalisées pour répondre aux besoins spécifiques de chaque entreprise ou de chaque environnement informatique. Check Point compte parmi ses clients les 100 sociétés figurant au classement des Fortune 100 ainsi que plusieurs dizaines de milliers d'entreprises et d'organisations de toute taille. Les solutions ZoneAlarm protègent les PC de millions de particuliers contre les pirates, les logiciels espions et les vols de données.

BUREAUX CHECK POINT

Siège mondial
5 Ha'Solelim Street
Tel Aviv 67897, Israël
Tél. : +972 3 753 4555
Fax : +972 3 624 1100
Email : info@checkpoint.com

Siège français
1 place Victor Hugo
Les Renardières
92400 Courbevoie, France
Tél. : +33 (0)1 55 49 12 00
Fax : +33 (0)1 55 49 12 01
Email : info_fr@checkpoint.com
www.checkpoint.com

10 août 2012