Comprendre et anticiper les attaques DDoS

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Document réalisé par l'ANSSI (Agence nationale de la sécurité des systèmes d'information), en collaboration avec les sociétés suivantes :

- Acorus Networks ;
- Bouygues Telecom ;
- Cyber Test Systems ;
- France-IX ;
- Free / Online (groupe Iliad) ;
- Jaguar-Network ;
- Orange France ;
- SFR ;
- Zayo France.

Vous pouvez adresser vos commentaires et remarques à l'adresse suivante :

`guide.ddos@ssi.gouv.fr`

Table des matières

Introduction

Les attaques par déni de service distribué (*Distributed Denial of Service* ou DDoS) sont aujourd'hui fréquentes, notamment du fait de la relative simplicité de leur mise en œuvre, et de leur efficacité contre une cible non préparée. Ces attaques peuvent engendrer des pertes financières non négligeables par l'interruption de service ou encore indirectement, par l'atteinte portée à l'image de la cible.

Pour cette raison, il est nécessaire d'anticiper cette menace, et de prendre un certain nombre de mesures techniques et organisationnelles afin d'y faire face. Ce document présente les attaques par déni de service distribué ainsi que la liste des éléments à prendre en compte afin de s'en protéger. Par ailleurs, le dernier chapitre du document rappelle les bonnes pratiques à mettre en œuvre afin de ne pas participer involontairement à une attaque DDoS.

Ce document est principalement destiné aux responsables de la sécurité des systèmes d'information des sociétés et organismes clients d'opérateurs de transit ou de fournisseurs d'accès à Internet, et cherchant à se protéger contre les attaques DDoS.

Chapitre 1

Les attaques DDoS

1.1 Qu'est-ce qu'une attaque DDoS ?

Une attaque par déni de service vise à rendre indisponible un ou plusieurs services. Un déni de service peut consister à exploiter, par exemple, une vulnérabilité logicielle ou matérielle. L'interruption de service peut également s'effectuer en empêchant l'accès à ce service, par exemple en saturant la bande passante du réseau : on parle alors d'attaques volumétriques. Par ailleurs, une attaque peut solliciter, jusqu'à épuisement, une ou plusieurs ressources d'un service. Il peut s'agir, par exemple, de l'ouverture d'un grand nombre de nouvelles sessions TCP dans un intervalle de temps très court, ou encore d'un nombre trop important de traitements concurrents effectués par une base de données.

On parle de « déni de service distribué » (de l'anglais *Distributed Denial of Service* ou DDoS) lorsque l'attaque fait intervenir un réseau de machines (souvent compromises) afin d'interrompre le ou les services visés.

1.2 Qui peut être visé ?

Toute entité dont l'activité dépend d'une infrastructure réseau connectée à Internet peut être la cible d'une attaque DDoS. Les motivations et objectifs des attaquants sont divers, allant des revendications idéologiques à la vengeance, en passant par les extorsions de fonds. Par ailleurs, certaines attaques semblent être menées afin de détourner l'attention, et de couvrir d'autres actions illégales, comme des transactions bancaires frauduleuses [1] [2].

Bien que bon nombre d'entités soient concernées par cette menace, certains types d'activités sont plus sujets à être cibles de DDoS. Parmi ceux-ci, on peut notamment citer le *e-commerce*, les institutions financières, les gouvernements, ou encore les structures d'hébergement informatique. Dans ce cadre, il est d'autant plus important de prévoir des solutions de protection appropriées dès le début des projets de mise en place de système d'information et d'infrastructure réseau.

Les attaques DDoS sont aujourd'hui fréquentes. À titre d'exemple, des opérateurs français ont constaté jusqu'à plus d'un millier d'attaques par jour en 2014. Par ailleurs, plusieurs rapports publics font état de la croissance du nombre de ces attaques [3]. Outre l'augmentation en nombre, l'ampleur des attaques a crû de manière significa-

tive au cours des dernières années [4, 5]. Ainsi, en 2014, des opérateurs français ont constaté des attaques dont le volume était de l'ordre de la centaine de gigabits par seconde, et le débit, en nombre de paquets par seconde, de l'ordre de la dizaine de millions.

Au cours des années précédentes, les opérateurs français ont constaté que la plupart des attaques durent moins d'une demi-heure. Cependant, les attaques menées dans le but d'extorquer des fonds à une société durent souvent plusieurs jours. Des attaques de ce type visant des petites et moyennes entreprises ont été rapportées dans l'actualité récente :

- le 24 mars 2014, la société *Basecamp* a été touchée par une attaque DDoS. Le groupe d'attaquants demandait une rançon afin de mettre fin à l'attaque. La société n'a pas obtempéré, et a bénéficié de l'aide de leurs fournisseurs d'accès à Internet pour mettre fin à l'attaque [6] ;
- en juin 2014, la *start-up Feedly* a elle aussi été visée par une tentative d'extorsion de fonds. La société ayant refusé d'accéder aux demandes de l'attaquant, elle a ensuite été touchée par plusieurs vagues d'attaques DDoS. Elle a dû recourir à un service de protection dédié afin de contrer les attaques [7].

Enfin, il faut noter que les attaques par déni de service sont, la plupart du temps, efficaces contre des cibles non préparées.

À retenir

Le nombre d'attaques par déni de service distribué a augmenté au cours des dernières années. Ces attaques sont aujourd'hui fréquentes, et peuvent viser toute entité disposant d'une infrastructure réseau connectée à Internet.

1.3 Quelques vecteurs d'attaque

1.3.1 Les botnets

Les attaques DDoS peuvent être lancées à partir de réseaux de machines compromises appelés *botnets*.

De nombreux outils accessibles en ligne permettent d'exploiter des *botnets* [8] [9]. Au cours des dernières années, des services de DDoS en ligne, couramment appelés *booter* ou *stresser*, ont fait leur apparition [10]. Ces services proposent des tarifs autorisant leur usage par des particuliers, et permettent à un utilisateur de lancer des attaques contre la cible de son choix. Par ailleurs, certains *booter* proposent de tester le service gratuitement pendant quelques minutes. La diversité des outils et services permettant de lancer des attaques par déni de service distribué contribue à l'augmentation du nombre de ces attaques.

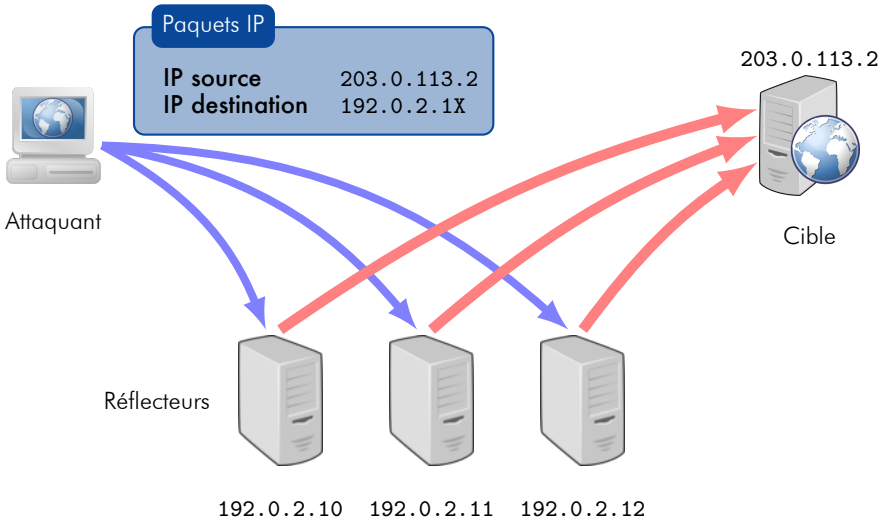


Figure 1.1 – Principe d'une attaque par réflexion.

1.3.2 Les attaques basées sur la réflexion

Certaines attaques utilisent des machines accessibles sur Internet et répondant à des requêtes émanant d'une source quelconque : il s'agit de réflecteurs. Une attaque par réflexion consiste à envoyer des paquets à ces réflecteurs en utilisant l'adresse IP de la victime comme adresse IP source : on parle alors d'usurpation d'adresse IP. Les réponses de ces réflecteurs à la victime induisent la génération d'un trafic non sollicité à destination de cette dernière. Ce trafic peut être suffisamment important pour saturer les liens réseau de la victime, entraînant un déni de service. La figure 1.1 illustre le principe des attaques par réflexion. L'attaquant interroge des serveurs en usurpant l'adresse IP de sa victime (`203.0.113.2`). Par conséquent, les serveurs envoient les réponses aux requêtes générées par l'attaquant vers la victime. Le déni de service est effectif si le volume de trafic induit par ces réponses excède la bande passante réseau dont la victime dispose.

Les attaques par réflexion impliquent souvent des protocoles reposant sur le protocole de transport UDP. En effet, le protocole UDP laisse à la couche applicative la tâche d'identification de la source, ce qui permet l'usurpation d'adresse IP. Par ailleurs, UDP ne nécessite pas l'établissement d'une session (contrairement au protocole TCP) préalablement à l'envoi de données. Cette particularité permet à un attaquant d'envoyer une requête à un service utilisant UDP au moyen d'un seul paquet, et de générer une réponse de la part du réflecteur.

Les attaques par réflexion ne sont pas uniquement limitées au protocole de transport UDP. Par exemple, il est possible d'envoyer des paquets TCP `SYN` en usurpant l'adresse IP d'une victime pour générer des paquets `SYN-ACK` en réponse vers la cible.

Enfin, il convient de noter que des attaques par réflexion peuvent être initiées à partir

de *botnets*.

1.3.3 Les attaques basées sur l'amplification

Une attaque volumétrique a pour objectif d'épuiser la bande passante réseau disponible afin de rendre un ou plusieurs services inaccessibles. Ce type d'attaque est souvent mené en exploitant les propriétés de certains protocoles afin de maximiser le volume de trafic généré. Par ailleurs, des attaques volumétriques visent à générer un très grand nombre de paquets par seconde afin de saturer les ressources de traitement d'une cible.

Certains protocoles génèrent des réponses d'une taille très supérieure à celle de la requête. Le nombre de paquets induit par la réponse peut également être plus important que le nombre de paquets nécessaire à l'envoi de la requête. L'amplification générée par ces protocoles peut être exploitée pour mener des attaques volumétriques.

La plupart du temps, les attaques volumétriques tirent parti de la réflexion et de l'amplification. Il existe un certain nombre de protocoles pouvant être exploités pour mener ce type d'attaques. Parmi ceux-ci, on peut notamment citer DNS (*Domain Name System* [11]), NTP (*Network Time Protocol* [12]), SNMP (*Simple Network Management Protocol* [13]), SSDP (*Simple Service Discovery Protocol*) [14], ou encore CHARGEN (*Character Generator protocol* [15]).

Il est important de remarquer qu'une entité peut être victime d'une attaque volumétrique exploitant un protocole bien qu'elle ne dispose pas de service actif exposé sur Internet reposant sur ce même protocole.

Important

Une entité peut être victime d'une attaque DDoS volumétrique exploitant un protocole bien qu'elle n'expose pas de service reposant sur ce même protocole.

1.3.3.1 Attaques par amplification DNS

Le protocole DNS est un système de nommage permettant notamment d'associer un nom facile à retenir à une adresse IP. Une description du principe de fonctionnement de DNS est donnée dans le chapitre 2 du guide de l'ANSSI relatif à l'acquisition et à l'exploitation de noms de domaine [16].

Pour mener des attaques par amplification DNS, l'attaquant peut interroger :

- des serveurs faisant autorité pour des zones comportant des enregistrements de grande taille ;

- des serveurs récursifs répondant à des questions provenant d'Internet.

Il est possible de limiter la participation à des attaques DDoS par amplification DNS en employant des mécanismes de *rate-limiting*, à l'instar de celui décrit dans le chapitre 4 de ce document.

1.3.3.2 Attaques par amplification NTP

Certaines implémentations de NTP, un protocole permettant la synchronisation temporelle de machines sur un réseau IP, peuvent également être exploitées afin de mener des attaques par amplification.

L'amplification peut provenir de l'envoi d'un message de contrôle (par exemple, *readvar*) permettant de récupérer des informations sur l'état d'un serveur et éventuellement, de modifier cet état. L'amplification résultant de ce type de requête varie en fonction du système et de l'implémentation. Des observations permettent de constater un facteur d'amplification significatif en termes de bande passante d'environ 30. Ainsi, un attaquant peut générer un trafic à destination d'une cible dont le volume est 30 fois plus important que celui nécessaire à l'interrogation des serveurs vulnérables.

Par ailleurs, une requête implémentée dans *ntpd* [17] et destinée à des fins de supervision, permet de récupérer la liste des adresses IP ayant interrogé le serveur. Cette liste comporte en outre diverses informations relatives aux requêtes, comme les dates d'interrogation ou encore le nombre de paquets reçus. Les implémentations disposant de cette fonctionnalité conservent en mémoire les données des 600 dernières requêtes que le serveur a reçues. En exploitant cette fonctionnalité, des tests permettent de constater qu'il est possible d'obtenir un facteur d'amplification en termes de bande passante d'environ 1290, et un facteur d'amplification en termes de nombre de paquets de 99.

Le chapitre 4 de ce document donne des éléments à prendre en compte afin de ne pas participer à des attaques par amplification NTP.

1.3.4 Les attaques ciblant des applications

Certaines attaques visent à épuiser les capacités de traitement d'une cible. Par exemple, un attaquant peut chercher à atteindre la limite du nombre de connexions concurrentes qu'un serveur web peut traiter. Dans ce cas, l'attaquant envoie en permanence un grand nombre de requêtes HTTP `GET` ou `POST` au serveur ciblé. Il est également possible d'envoyer des requêtes partielles, puis de transmettre la suite de ces requêtes à intervalles réguliers, dans le but de maintenir les connexions ouvertes le plus longtemps possible et d'éviter la fermeture des connexions au-delà d'un délai fixé [18].

D'autres types d'attaques applicatives cherchent à épuiser les ressources de calcul d'un serveur en initiant un grand nombre de sessions TLS, ou encore à tirer parti de faiblesses dans la conception d'une application web [19].

1.3.5 Autres types d'attaque DDoS

1.3.5.1 Épuisement des tables d'état

Les équipements comme les pare-feux, les répartiteurs de charge ou encore les systèmes de détection d'intrusion recourent, la plupart de temps, au suivi de connexion. Dans le cas des pare-feux, le suivi de connexion permet, par exemple, de rejeter les paquets n'appartenant pas à une connexion existante initiée depuis un hôte autorisé.

Le suivi de connexion nécessite le maintien d'une table d'état des connexions existantes. Pour chaque paquet entrant, ces équipements effectuent une recherche dans leur table d'état pour déterminer si le paquet correspond à une connexion existante. Dans le cas contraire, une nouvelle connexion est alors ajoutée en mémoire.

Ce mode de fonctionnement est parfois nécessaire, mais rend les équipements vulnérables à des attaques visant à saturer la table d'état.

1.3.5.2 Attaques utilisant la fragmentation IP

Un paquet IP peut traverser des réseaux hétérogènes où la taille maximale des paquets varie. En particulier, lorsqu'un paquet arrive sur un réseau dont la MTU [1] est plus basse, il est nécessaire de fragmenter ce paquet afin qu'il puisse atteindre sa destination. Le paquet initial est alors découpé en plusieurs paquets dont la taille n'excède pas celle de la MTU. Les paquets ainsi générés sont réassemblés une fois arrivés à leur destination [2]. Certaines attaques exploitent le mécanisme de fragmentation afin d'induire une charge supplémentaire sur les équipements ciblés, ceux-ci devant effectuer le réassemblage des paquets.

1. *Maximum Transmission Unit*, c'est-à-dire la taille maximale d'un paquet pouvant être transmis sans être fragmenté sur un lien IP.

2. Pour plus de détails sur le mécanisme de fragmentation, le lecteur peut se référer à la RFC 791 [20].

Chapitre 2

Comment se protéger contre les DDoS ?

Il existe différentes solutions de protection qui peuvent être mises en œuvre afin de lutter contre les attaques DDoS. Le déploiement d'équipements de filtrage en bordure du système d'information d'une entité offre une protection pour les attaques dont le volume n'excède pas la capacité des liens réseau.

Lorsque les liens réseau d'une entité sont saturés, il est souvent nécessaire de solliciter l'opérateur de transit ou le fournisseur d'accès à Internet afin de filtrer le trafic en amont. Par ailleurs, des prestataires offrent des solutions de protection dédiées dites « dans le *cloud* », qui sont hébergées sur leurs propres infrastructures.

Il est possible de combiner l'usage d'équipements dédiés en bordure du réseau d'une entité à un filtrage effectué « dans le *cloud* ». Ce type de protection hybride permet notamment de protéger l'entité contre des attaques volumétriques tout en lui donnant la capacité de lutter contre des attaques de débit plus faible.

Ce chapitre décrit les différentes solutions de protection pouvant être envisagées, en indiquant les limites de chacune d'entre elles.

2.1 Filtrage en bordure du réseau de l'entité

Cette section présente les types d'équipement permettant d'effectuer du filtrage en bordure du réseau d'une entité. Ce type de solution offre une protection pour des attaques ne saturant pas les liens réseau d'une entité.

2.1.1 Équipements de type pare-feu

Les pare-feux et les répartiteurs de charge peuvent contribuer à absorber certaines attaques DDoS, par exemple celles générant un trafic relativement faible. Les pare-feux peuvent ainsi être utilisés pour filtrer du trafic en fonction du protocole de transport et des ports source ou destination, ou encore limiter le nombre de requêtes par adresse IP source à destination d'un serveur.

Limites

Il faut veiller à ne pas recourir au suivi de connexions entrantes pour des pare-feux qui sont placés devant des serveurs à forte audience (par exemple, des serveurs web). En

effet, certaines attaques DDoS visent spécifiquement à épuiser les ressources mémoire de la cible. Dans ce cas, les pare-feux et répartiteurs de charges sont les premiers éléments de l'infrastructure à être touchés. S'agissant d'éléments placés en coupure, la défaillance de l'un d'entre eux suffit à rendre un déni de service effectif. Cependant, il est parfois possible de modifier la configuration de ces équipements afin d'accroître leur résistance face à ce type d'attaque, par exemple en augmentant la taille des tables d'état et en réduisant les durées de suivi de connexions.

Ces équipements ne permettent pas de se prémunir, d'une manière générale, contre les attaques applicatives. Par exemple, il peut être difficile de définir des règles de filtrage pour certaines attaques exploitant des applications web, comme une inondation de requêtes HTTP `GET` provenant de sources multiples.

À retenir

Les pare-feux et les répartiteurs de charge peuvent contribuer à absorber certaines attaques DDoS, mais ils ne constituent pas une protection suffisante contre ce type d'attaque d'une manière générale. Par ailleurs, les limites de ces équipements sont parfois exploitées pour rendre des services indisponibles. Cependant, il est parfois possible de modifier la configuration de ces équipements afin d'améliorer leur résistance face à ce dernier type d'attaque (par exemple, en augmentant la taille des tables d'état).

2.1.2 Recours à des équipements spécifiques

Une entité peut recourir à des équipements de filtrage spécifiques aux attaques DDoS. Ces équipements possèdent, en général, des capacités de traitement adaptées, et offrent plusieurs types de contre-mesures. En plus de fonctions de filtrage par liste blanche ou liste noire, ils permettent, entre autres :

- d'effectuer du filtrage basé sur la position géographique des sources ;
- de définir des règles précises pour filtrer des paquets sur leur contenu (par exemple à l'aide d'expressions régulières) ;
- de limiter le nombre de requêtes dans un intervalle de temps donné pour des ressources particulières (par exemple, pour une page web)
- de définir des seuils de détection d'attaque en fonction de paramètres comme la bande passante, ou le nombre de paquets par seconde.

Il faut également noter que ce type d'équipement peut être employé pour effectuer du filtrage applicatif lorsque les échanges sont chiffrés (par exemple, pour du trafic HTTPS) tout en permettant à l'entité de conserver sa clé privée. Pour plus d'information, le

lecteur peut consulter les recommandations de sécurité concernant l'analyse des flux HTTPS de l'ANSSI [21].

Limites

Certaines activités connaissent des variations significatives de leur trafic (notamment en termes de volumétrie) lors d'événements particuliers. Par exemple, les sites de journaux en ligne peuvent connaître des pics de trafic à l'occasion d'événements sportifs, ou encore lors de la publication de résultats d'examens. Ainsi, il peut être nécessaire de faire évoluer les seuils définis dans les paramètres des contre-mesures au cours du temps. De plus, plusieurs vecteurs (amplification DNS, `SYN` *flood*, attaques applicatives) peuvent être exploités, simultanément ou non, au cours d'une même attaque [4]. Dans ce cas, il est nécessaire d'adapter les contre-mesures aux évolutions de cette dernière. La mise en œuvre de contre-mesures actives en permanence n'est donc pas toujours possible. Dans la pratique, les équipements permettent d'établir plusieurs modèles de contre-mesures afin de bénéficier de paramétrages prédéfinis et applicables en fonction du besoin.

Par ailleurs, les contre-mesures ne rentrent pas toujours immédiatement en action lorsqu'une attaque survient. Un délai de quelques minutes est souvent nécessaire pour la détection, en particulier lorsque les algorithmes de détection reposent, au moins en partie, sur un apprentissage. Il est donc possible qu'une attaque soit effective pendant la durée nécessaire à l'équipement pour la détecter.

En outre, il convient de noter que la capacité de traitement de ces équipements varie en fonction des contre-mesures mises en œuvre. En particulier, les contre-mesures reposant sur le maintien de tables d'état ou l'analyse protocolaire nécessitent plus de ressources (notamment en matière de puissance de calcul).

Enfin, lors de l'achat d'équipements de filtrage spécifiques aux attaques DDoS, il est nécessaire de prendre en compte les mises à jour logicielles de ces équipements, qui peuvent être très onéreuses.

Mise en œuvre

Au sein de l'infrastructure réseau de l'entité, ces équipements peuvent être placés en coupure, ou, si l'architecture du réseau le permet, en dérivation. Dans ce dernier cas, le trafic est redirigé vers l'équipement lors d'une attaque par une modification du routage.

Le paramétrage des contre-mesures peut s'avérer complexe. En conséquence, la mise en œuvre de ce type d'équipement nécessite une prise en main préalable, et une étude du trafic généré par l'entité. Un mauvais paramétrage peut en effet rendre le système inefficace, ou encore entraîner des pertes de trafic légitime.

À retenir

Certains équipements dédiés offrent différentes contre-mesures spécifiques aux attaques DDoS. Leur mise en œuvre nécessite une prise en main préalable, et un paramétrage adapté au trafic de l'entité.

2.2 Protection externalisée

2.2.1 Protection offerte par les hébergeurs

Certains hébergeurs offrent une protection contre les attaques DDoS. Différents niveaux de protection sont souvent proposés, une protection par défaut étant parfois incluse dans les offres d'hébergement. Dans ce dernier cas, il convient de s'assurer du niveau de protection offert. En effet, le filtrage mis en œuvre est parfois limité. Souvent, ces offres ne permettent pas de définir des règles de filtrage spécifiques, ou de bénéficier de l'intervention du support pour le traitement d'une attaque, ces possibilités n'étant parfois accessibles qu'au travers d'options supplémentaires. Néanmoins, ces dernières peuvent constituer une solution de protection pour les structures faisant appel à une société externe pour l'hébergement de leurs services.

À retenir

Les hébergeurs offrent parfois une protection contre les attaques DDoS. Les différentes options proposées peuvent constituer une solution pour les structures faisant appel à une société externe pour l'hébergement de leurs serveurs.

2.2.2 Filtrage par l'opérateur de transit

L'intervention de l'opérateur de transit [3] peut aider à contrecarrer partiellement ou totalement les effets d'une attaque DDoS. Cette intervention est parfois nécessaire, en particulier lorsque les liens réseau mis à la disposition du client sont saturés.

2.2.2.1 Filtrage au niveau du réseau de l'opérateur de transit

L'opérateur de transit peut mettre en place un filtrage du trafic basé sur les adresses IP source ou destination, le protocole de transport utilisé ainsi que les ports source ou destination. Il faut noter que le filtrage sur les adresses IP source peut être difficile à mettre en oeuvre lorsque celles-ci sont très nombreuses.

3. L'opérateur de transit permet à ses clients de joindre l'Internet [22].

En dernier recours, l'opérateur peut éliminer la totalité du trafic vers une destination donnée. Dans ce cas, le trafic à destination d'une ou plusieurs destinations données n'est tout simplement pas traité. L'opérateur crée ainsi un « trou noir » pour la ou les destinations en question. Cette méthode de filtrage est couramment désigné par l'expression *blackholing*. Il faut noter que le *blackholing* du trafic basé sur la destination rend un déni de service effectif. Pour autant, ce type de filtrage peut s'avérer utile, notamment lorsque le trafic destiné à la cible de l'attaque affecte d'autres services que cette dernière opère, ou dont elle peut bénéficier. Certains opérateurs peuvent également proposer un filtrage similaire basé sur les adresses IP sources de l'attaque [23].

Un filtrage de type *blackholing* peut parfois être déclenché à distance par une entité, notamment lorsque celle-ci a la gestion de ses équipements de routage et est interconnectée avec l'opérateur à l'aide du protocole BGP [24].

Limites

En l'absence de solution de filtrage spécifique aux attaques DDoS, le filtrage effectué par l'opérateur ne permet pas de définir des filtres sur le contenu des données échangées au niveau applicatif.

Mise en œuvre

Le délai de mise en œuvre d'une de ces méthodes de filtrage par l'opérateur dépend de plusieurs facteurs. En premier lieu, il dépend de la capacité du client et de l'opérateur à détecter rapidement l'attaque DDoS. Ensuite, afin de pouvoir mettre en place des règles de filtrage, une analyse du trafic doit être effectuée afin de déterminer les discriminants permettant de distinguer le trafic légitime du trafic généré par l'attaque. Le délai de mise en place des règles dépend donc également de la complexité de l'analyse du trafic illégitime.

2.2.2.2 Service de filtrage spécifique aux attaques DDoS

L'opérateur de transit fournit parfois un service de filtrage spécifique aux attaques par déni de service distribué. Dans la pratique, deux modes d'opérations principaux peuvent être rencontrés :

- le service est géré par l'opérateur. Ce dernier peut disposer d'un SOC (*Security Operations Center*[4]) dédié, ou simplement d'une protection générique appliquée pour tous ses clients ;
- il peut s'agir d'une plate-forme mise à disposition par l'opérateur, mais que le client doit lui-même opérer.

4. Un *Security Operations Center* est un centre de supervision d'une infrastructure réseau ou d'un système d'information. Les SOC sont chargés du traitement des incidents de sécurité.

Quel que soit le mode d'opération, il convient de s'assurer des capacités de traitement de la solution, d'autant plus que les plates-formes de filtrage dédiées sont en général partagées par plusieurs clients.

Limites

Les services spécifiques aux attaques DDoS sont souvent proposés en option par l'opérateur de transit, ce qui implique un coût supplémentaire.

Mise en œuvre

Comme décrit en section 2.1.2 de ce chapitre, le paramétrage des équipements de filtrage spécifiques aux attaques DDoS peut être complexe. L'exploitation d'une plate-forme de filtrage mise à disposition par l'opérateur nécessite donc une prise en main préalable.

À retenir

L'intervention de l'opérateur de transit est parfois nécessaire, en particulier lorsque le lien réseau mis à disposition du client est saturé. Les opérateurs permettent souvent d'effectuer du *blackholing* de trafic basé sur la destination. Il convient de noter que cette mesure, parfois nécessaire, rend le déni de service effectif. L'opérateur peut également offrir un service de filtrage de trafic. Dans le cas où ce service est opéré par le client, ce dernier doit s'assurer de maîtriser la configuration des différentes contre-mesures offertes par la plate-forme.

2.2.3 Recours à un Content Delivery Network (CDN)

Un *Content Delivery Network* (CDN) est une infrastructure de serveurs répartie dans plusieurs *data centres*, et dont l'objectif est de se substituer aux services d'une entité pour servir ses contenus au plus proche des utilisateurs. Les CDN ont ainsi une fonction de cache, et permettent notamment d'augmenter la disponibilité des ressources ou encore d'accroître la vitesse de mise à disposition des données, généralement des pages web ou des flux multimédia.

Pour ce faire, les CDN exploitent principalement deux méthodes :

1. La géolocalisation de l'adresse IP source des requêtes DNS émises depuis le client. Il est ainsi possible de diriger ce dernier vers les serveurs les plus proches de sa position géographique ;
2. La technique d'adressage dite *anycast*, qui consiste à partager la même adresse IP entre plusieurs serveurs, aussi appelés nœuds dans le contexte

de l'anycast. Le routage IP permet à un utilisateur d'être dirigé vers le serveur ou le nœud « le plus proche ».

Bénéfices en termes de sécurité

La répartition de la charge de traitement sur un grand nombre de serveurs peut contribuer à améliorer la résistance à certaines attaques DDoS. Par exemple, une attaque menée depuis des sources concentrées dans une même région géographique n'affectera que les nœuds servant cette région. Par ailleurs, une attaque provenant de sources réparties dans le monde pourrait avoir un impact moindre, l'attaque étant absorbée par l'ensemble des serveurs du CDN [25].

À retenir

Les CDN permettent la répartition de ressources sur un grand nombre de serveurs, ce qui peut contribuer à améliorer la résistance aux attaques DDoS.

2.2.4 Services de protection dédiés

En dehors des hébergeurs, des sociétés offrent un service de protection contre les attaques DDoS dit « dans le *cloud* ». Ce service de protection fonctionne principalement selon deux modèles différents décrits dans cette section.

2.2.4.1 Redirection via le protocole DNS

Certains services de protection reposent sur une redirection DNS. Le but est de diriger le trafic à destination d'un domaine, comme `example.com`, vers l'adresse IP d'un serveur du fournisseur de protection. Ce dernier se charge ensuite de filtrer le trafic, puis de le rediriger vers la destination originelle. Ce modèle de fonctionnement est souvent offert par des CDN pour protéger les serveurs web de leurs clients.

La figure 2.1 illustre le principe de fonctionnement de cette méthode. Lorsqu'un client souhaite accéder au site web `www.example.com`, il interroge premièrement un serveur DNS pour connaître l'adresse IP du serveur web (étape 1). Le serveur répond par l'adresse IP d'un des nœuds du nuage *anycast* du fournisseur du service de protection. Le trafic entre le client et le serveur web va donc transiter par le CDN (étape 2), qui peut ainsi filtrer le trafic avant, éventuellement, de le transmettre au serveur web protégé (étape 3).

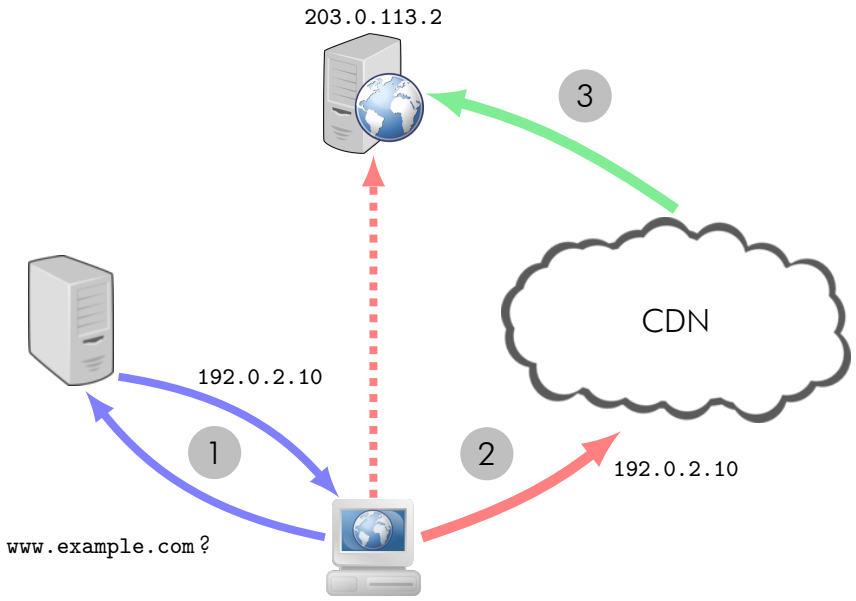


Figure 2.1 – Principe de la solution basée sur DNS.

Limites

Il est important de noter que lorsque cette méthode est employée, le trafic à destination de l'adresse IP du serveur ainsi protégé (aussi appelée adresse IP originelle) n'est pas bloqué. En effet, pour rediriger le trafic vers le service de protection, cette méthode repose uniquement sur le mécanisme de résolution de nom fourni par le DNS. Si un attaquant connait l'adresse IP originelle (par exemple, `203.0.113.2` sur la figure 2.1), il peut accéder directement au serveur sans passer par le CDN.

Important

En cas de recours à une redirection *via* le protocole DNS, il faut s'assurer qu'il n'existe pas de moyen trivial de découvrir l'adresse IP à protéger.

L'entrée en action de ce type de protection est effective lorsque les caches DNS ont été mis à jour. Le délai d'entrée en action dépend donc en partie de la durée de vie des enregistrements DNS dans les caches.

Certains CDN concentrent le trafic en sortie de leur réseau et à destination d'une entité protégée sur un nombre restreint de nœuds bien identifiés. Ceci permet à l'entité bénéficiant de la protection de créer et de maintenir une liste blanche d'adresses IP pouvant contacter ses serveurs. Cependant, il est important de noter qu'un filtrage sur les adresses IP des nœuds du CDN n'offre qu'une protection limitée : par exemple, cette mesure ne permet pas de se protéger contre les attaques volumétriques.

Enfin, si les extensions de sécurité DNSSEC [26] sont mises en œuvre pour signer la zone devant être protégée, il est nécessaire de s'assurer que le fournisseur du service de protection est en mesure de prendre en charge les signatures DNSSEC, et que sa clé de signature est publiée au préalable dans la zone parente. Dans le cas contraire, l'activation du service de protection rendra la zone inaccessible.

Mise en œuvre

Plusieurs précautions doivent être prises afin de protéger l'adresse IP originelle :

- les enregistrements du domaine protégé (ainsi que de ses sous-domaines) ne doivent pas contenir l'adresse IP originelle du serveur pour lequel la protection est destinée ;
- Il est nécessaire de s'assurer que le serveur ne divulgue pas son adresse IP au travers d'un message d'erreur, ou n'expose pas des éléments de configuration qui pourraient la révéler ;
- après avoir activé le service de protection, l'adresse IP du serveur doit être changée. Il est en effet possible de consulter un historique des enregistrements DNS qui peut contenir l'adresse IP originelle. Lorsque c'est possible, il est préférable de choisir une adresse IP dans un bloc différent de celui auquel l'adresse précédemment utilisée appartient.

En cas d'urgence, ce type de protection ne nécessite qu'une modification des enregistrements DNS, ce qui offre l'avantage de pouvoir être mis en œuvre relativement rapidement. Cependant, il est important de noter qu'au vu des limites de cette solution, une mise en œuvre dans des conditions de sécurité acceptables peut être coûteuse en temps.

À retenir

Il est nécessaire de prendre des précautions avant la mise en œuvre d'une protection contre les attaques DDoS basée sur la résolution de nom. Cette méthode a une limite importante : le trafic à destination de l'entité ainsi protégée ne transite pas forcément par le fournisseur de la protection.

2.2.4.2 Déroutement du trafic par des annonces BGP

L'objectif de cette méthode est de diriger l'ensemble du trafic à destination d'un bloc d'adresses IP vers le fournisseur de service de protection. Le déroulement de cette opération est présenté sur la figure 2.2. Lorsque le service de protection n'est pas utilisé (cas a), le trafic provenant de l'Internet est acheminé à l'entité par ses opérateurs de transit. Afin de mettre en œuvre une redirection de trafic, une interconnexion doit être

établie entre l'entité et le fournisseur du service de protection (étape 1). En général, le protocole GRE (*Generic Routing Encapsulation* [27]) est utilisé pour établir un tunnel permettant d'encapsuler l'intégralité du trafic au niveau du protocole IP. Parfois, les fournisseurs de protection proposent une interconnexion physique directe avec le client. L'établissement d'un tunnel avec l'entité n'est alors pas nécessaire.

Pour faire transiter l'ensemble du trafic provenant d'Internet par le fournisseur du service de protection, la victime annonce premièrement au fournisseur de ce service les routes permettant d'atteindre ses blocs d'adresses IP au moyen du protocole BGP [5] (étape 2 de la figure 2.2). Ensuite, elle cesse d'annoncer ces mêmes blocs à ses opérateurs de transit, ce qui entraîne la redirection du trafic qui lui est destiné vers le fournisseur du service de protection (étape 3 de la figure 2.2).

Ce dernier peut alors filtrer le trafic et transmettre le trafic légitime vers la victime au moyen de l'interconnexion préalablement établie (étape 4 de la figure 2.2). Contrairement à un service utilisant une redirection *via* la protocole DNS, cette solution permet ainsi de protéger les serveurs hébergés aux adresses IP dites originelles.

Lors de la mise en œuvre de cette solution, le trafic sortant de l'entité ne passe pas par le fournisseur du service de protection, mais par ses opérateurs de transit (étape 5 de la figure 2.2).

Limites

Cette solution peut être adoptée si l'entité dispose d'un bloc d'adresses IP annonçable sur Internet et utilise déjà le protocole BGP.

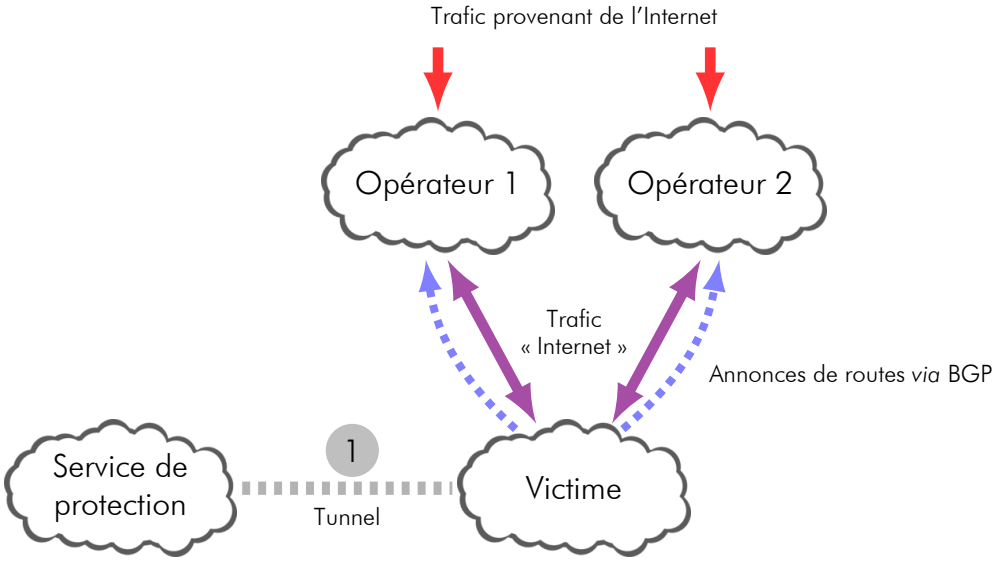
Par ailleurs, ce service de protection est en général significativement plus onéreux qu'un service basé sur une redirection de trafic utilisant DNS telle que décrite dans la section 2.2.4.1.

Mise en œuvre

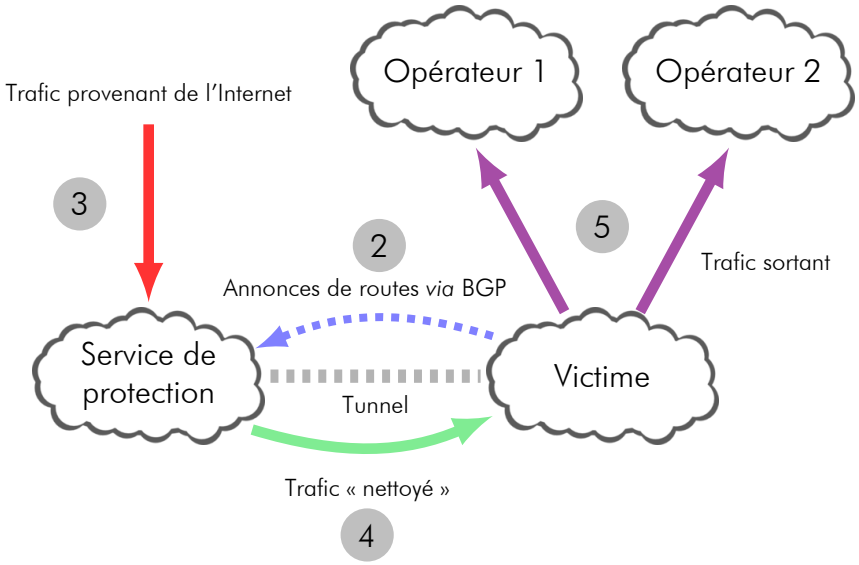
Cette solution de protection nécessite une préparation préalable : il faut en effet mettre en place un tunnel (par exemple, un tunnel GRE) entre l'infrastructure du service de protection et l'entité devant être protégée (ou établir une interconnexion directe, le cas échéant).

Hormis l'étape de préparation, la mise en œuvre et l'entrée en action de ce mécanisme est plus rapide qu'une solution basée sur une redirection DNS. En effet, une fois la modification des annonces de routes effectuée, la redirection du trafic à destination de l'entité dépend du temps de propagation des routes dans l'Internet, qui est de l'ordre de la minute [28].

5. Une description de BGP est donnée dans l'introduction du rapport de l'observatoire de la résilience de l'Internet français [22].



(a) Avant le déroutement de trafic.



(b) Après le déroutement de trafic.

Figure 2.2 – Principe du déroutement de trafic à l'aide de BGP.

Important

Le recours à cette solution de protection nécessite la mise en œuvre d'une interconnexion entre l'entité et le fournisseur du service de protection. Cette interconnexion peut consister en l'établissement d'un tunnel GRE, ou, lorsque c'est possible, être directe et établie physiquement.

En cas d'attaque, les opérateurs de transit peuvent contribuer à filtrer le trafic le temps de mettre en place un tunnel GRE ou une interconnexion directe avec le prestataire. Par ailleurs, durant l'établissement de cette interconnexion, le recours à une solution reposant sur une redirection *via* DNS peut également être envisagé.

À retenir

Le déroutement de trafic permet de faire transiter l'intégralité du trafic vers le fournisseur du service de protection. Cette solution offre un bien meilleur niveau de protection qu'une solution basée sur la résolution de nom. En revanche, la souscription à ce type de service est généralement plus onéreuse.

2.3 Autres mesures techniques et organisationnelles

En dehors des solutions de protection spécifiques, des bonnes pratiques peuvent contribuer à améliorer la résistance à une attaque par déni de service. Parmi celles-ci, on peut notamment citer :

- la segmentation du réseau de l'entité de manière à faciliter le filtrage en cas d'attaque, et l'isolement éventuel de certains sous-réseaux ou de certains serveurs ;
- la mise en œuvre d'un filtrage à la bordure du réseau de l'entité afin de n'autoriser que les flux nécessaires au fonctionnement de cette dernière.

Ces pratiques contribuent également à limiter le risque de participation involontaire à une attaque en déni de service (voir chapitre 4). Par ailleurs, la mise en place d'un réseau d'administration dédié est nécessaire. En effet, une attaque peut affecter significativement l'infrastructure réseau d'une entité, et ainsi entraîner des difficultés d'accès aux équipements. Au minimum, le trafic d'administration doit être marqué comme prioritaire au moyen de la mise en place d'un marquage QoS (*Quality of Service*).

Pour faire face à une attaque par déni de service, il est nécessaire de recenser les systèmes susceptibles d'être visés, et de connaître les équipes responsables de l'administration de ces systèmes. En outre, afin de favoriser un traitement rapide de l'attaque,

il est impératif de disposer des contacts appropriés en interne, chez les opérateurs de transit, ainsi qu'auprès des fournisseurs d'un service de protection contre les attaques DDoS.

Important

Il est impératif de disposer de contacts appropriés en interne, chez les opérateurs de transit, ainsi qu'auprès des fournisseurs d'un service de protection pour réagir efficacement en cas d'attaque.

2.4 Services fournis par des entités externes

Une entité peut être touchée indirectement par une attaque DDoS : une attaque contre une société peut affecter d'autres entités partageant la même infrastructure réseau, ou bénéficiant d'un service fourni par la cible de l'attaque. Les interruptions de services engendrées par des attaques DDoS contre des fournisseurs de service ne sont pas rares. Un exemple est celui de la société nord-américaine Neustar, qui a connu une attaque DDoS entre fin avril et début mai 2014 [29]. Cet incident a entraîné des perturbations du service DNS fourni à ses clients [30].

Il est important de ne pas oublier des services qui sont parfois considérés comme étant en marge du système d'information, à l'instar de la téléphonie. À titre d'exemple, une société nord-américaine fournissant un service de téléphonie sur IP a été victime d'une série d'attaques DDoS pendant plusieurs mois entre fin 2012 et début 2013 [31]. Ces attaques ont entraîné des interruptions du service, affectant des clients de la société.

Important

Dans la mesure du possible, il est important de s'assurer que les fournisseurs de services dont dépend une entité sont préparés aux attaques DDoS.

Chapitre 3

Comment réagir face à un DDoS ?

Les attaques DDoS sont souvent très efficaces contre une entité non préparée. Il est donc nécessaire d'anticiper cette menace en mettant en œuvre des moyens de protection appropriés, et de planifier la réponse à ce type d'incident. Cette section donne des éléments relatifs à la détection d'une attaque, et aux mesures pouvant être prises pour y faire face. Par ailleurs, le lecteur pourra également consulter la note d'information du CERT-FR [6] concernant les dénis de services [32].

3.1 Détection d'une attaque DDoS

Pour détecter un incident, il est indispensable de disposer de moyens de supervision de l'infrastructure, tant au niveau du réseau que des services opérés. La supervision permet notamment de suivre l'évolution de la consommation de ressources, comme la bande passante réseau, les ressources processeur et mémoire, ou encore l'espace disque. Des variations significatives constatées au niveau de ces ressources peuvent indiquer un problème opérationnel, et éventuellement un déni de service.

Par exemple, le trafic réseau peut être supervisé à l'aide de protocoles tels que NetFlow [33] ou IPFIX (*IP Flow Information Export*) [34]. Ces protocoles permettent d'obtenir des informations sur les échanges réseau sous forme de flux décrits par les adresses IP source ou destination, le protocole de transport utilisé, les ports source ou destination, ainsi que d'autres éléments caractéristiques du trafic. NetFlow ou IPFIX sont aujourd'hui disponibles sur un grand nombre d'équipements réseau, et permettent l'export des flux vers des collecteurs qui peuvent ainsi agréger, en temps réel, les informations relatives au trafic réseau. L'analyse des données remontées à l'aide d'outils d'analyse NetFlow ou IPFIX peut permettre de détecter des variations significatives de trafic.

Important

Il est nécessaire de disposer de moyens de supervision et d'alerte afin de détecter un incident.

6. Le CERT-FR est le centre gouvernemental de veille, d'alerte et de réponses aux attaques informatiques : `http://www.cert.ssi.gouv.fr`.

En premier lieu, il convient de déterminer les causes d'un incident. En effet, un service peut devenir inaccessible pour plusieurs raisons autres qu'une attaque :

- une panne de routage provoquée par une erreur de configuration ;
- le dysfonctionnement d'un service critique comme DNS ;
- des pics de fréquentation d'un site web dus à la survenue d'événements particuliers ;
- une erreur d'implémentation entraînant l'arrêt d'un serveur.

Parmi les éléments permettant d'identifier les causes d'un incident, on peut notamment citer les journaux des équipements et des serveurs, qui contiennent très souvent des informations utiles pour diagnostiquer un problème. Afin de mettre en œuvre un système de journalisation dans de bonnes conditions de sécurité, le lecteur peut se référer aux recommandations de sécurité pour la mise en œuvre d'un système de journalisation de l'ANSSI [35].

3.2 Réaction face à une attaque

Avant de mettre en œuvre une contre-mesure, il est important d'identifier :

- l'élément défaillant. S'agit-il d'une saturation des liens réseau, d'une surcharge au niveau d'un serveur ou plus précisément, d'une application ? L'attaque cible-t-elle un seul hôte, ou un bloc entier du réseau de l'entité ?
- le ou les protocoles utilisés. Dans le cas où le protocole de transport est UDP, il convient de prendre en compte le fait que ce protocole ne permet pas d'identifier les sources d'une attaque (possibilité d'usurpation de l'adresse IP source) ;
- les sources de l'attaque : s'agit-il de paquets provenant d'un réseau interne à l'entité, ou de l'extérieur ? L'attaque est-elle générée par un nombre restreint de sources ? Le trafic lié à l'attaque transite-t-il par un seul opérateur ?
- un ou plusieurs discriminants permettant de distinguer le trafic légitime du trafic généré par l'attaque (par exemple, des motifs récurrents dans le contenu des paquets, des valeurs remarquables dans les en-têtes HTTP).

Une fois les caractéristiques de l'attaque identifiées, plusieurs actions peuvent être décidées en fonction de la nature de celle-ci. Par exemple, si la bande passante des liens réseau fournis par les opérateurs est saturée, ceux-ci doivent être contactés afin de filtrer le trafic. Par ailleurs, l'entité peut mettre en œuvre le service de protection éventuel dont elle peut bénéficier si celui-ci n'est pas actif (par exemple, en modifiant sa politique de routage pour faire transiter le trafic en entrée par un service de protection, comme présenté dans la section 2.2.4.2).

En outre, un certain nombre de dispositions peuvent être prises au niveau de l'entité ciblée. Parmi celles-ci, on peut notamment citer :

- le blocage des adresses IP sources identifiées comme étant à l'origine de l'attaque ;

- le blocage du type de trafic impliqué dans l'attaque, et non nécessaire au bon fonctionnement de l'entité (filtrage sur le port destination, par exemple) ;
- la limitation du nombre de connexions concurrentes par adresse IP source au niveau d'un pare-feu ;
- la réduction des délais de garde des connexions TCP (par exemple sur des serveurs web ou SMTP) ;
- le blocage du trafic à destination des cibles, en fonction de l'impact de l'attaque sur le reste de l'infrastructure réseau.

Lors du traitement d'une attaque, il est important de noter que certains attaquants semblent utiliser le déni de service comme diversion : une attaque DDoS peut chercher à couvrir une tentative d'intrusion ou une extraction de données [1]. Il faut donc s'assurer que le système d'information n'est pas la cible d'une autre attaque, et procéder à un contrôle global du système d'information de l'entité une fois l'attaque terminée.

3.2.1 Déclaration d'incident

Selon la nature de l'organisme attaqué, la loi peut imposer une déclaration d'incident. Cette déclaration ne constitue en aucun cas un dépôt de plainte, et ne s'assortit d'aucune garantie d'assistance technique.

3.2.1.1 Opérateurs de communications électroniques

Les opérateurs de communications électroniques, en application du Code des Postes et des Communications Électroniques (CPCE, article D98-5) [36], ont l'obligation de déclarer les incidents qui ont un impact « significatif » sur la disponibilité des services auprès du Centre Opérationnel de Gestion Interministériel de Crise (COGIC) du ministère de l'Intérieur. Par ailleurs, dans le cas d'un incident significatif dû à une attaque informatique, à l'instar d'une attaque DDoS, les opérateurs doivent effectuer une déclaration auprès de l'ANSSI. Aujourd'hui, un incident est considéré comme significatif s'il affecte au minimum 100 000 abonnés. Il convient de noter que ce seuil est susceptible d'évoluer dans le futur.

3.2.1.2 Opérateurs d'importance vitale

Les opérateurs d'importance vitale sont tenus d'informer sans délai l'ANSSI des incidents affectant le fonctionnement ou la sécurité des systèmes d'information d'importance vitale (article L1332-6-2 du Code de la défense [37]).

3.2.1.3 Autres organismes et sociétés

Selon leur activité et la gravité des incidents dont ils sont victimes, certains organismes ou sociétés peuvent être soumis à des obligations similaires à celles décrites aux sections 3.2.1.1 et 3.2.1.2. Les incidents sont alors déclarés, selon les cas, auprès de l'administration ou de l'autorité sectorielle correspondante.

3.2.2 Dépôt de plainte

Une attaque DDoS constitue une atteinte aux systèmes de traitement automatisé de données (ou STAD), tels que définis par la loi Godfrain du 5 janvier 1988 [38]. Ces atteintes sont prévues et réprimées par les articles 323-1 et suivants du Code pénal [39]. Une société ou un organisme victime d'une attaque DDoS peut donc effectuer un dépôt de plainte. À cette fin, il est nécessaire de collecter l'ensemble des éléments techniques décrivant l'attaque (journaux, captures de trafic réseau, données NetFlow), et de garder une trace des échanges effectués avec des tiers pendant le traitement de l'incident [35].

3.2.2.1 Où déposer plainte ?

L'organisme auprès duquel la plainte doit être déposée dépend de la nature de la société ou de l'organisme ciblé.

Opérateurs d'importance vitale

La Direction générale de la sécurité intérieure (DGSI), anciennement la Direction centrale du renseignement intérieur (DCRI), est compétente pour les attaques ciblées contre les systèmes d'information d'opérateurs d'importance vitale, de l'État, ou encore d'établissements composés de Zones à Régime Restrictif [40].

Autres sociétés et organismes

Les sociétés et organismes n'étant pas des opérateurs d'importance vitale peuvent déposer plainte auprès des services de la police nationale ou de la gendarmerie nationale décrits par la suite. L'orientation vers l'un ou l'autre de ces services dépend de la localisation géographique du système d'information attaqué.

- La BEFTI (Brigade d'enquête sur les fraudes aux technologies de l'information) [41] est compétente si le système d'information est localisé à Paris ou au sein des trois départements limitrophes de la capitale (Hauts-de-Seine, Seine-Saint-Denis et Val-de-Marne) ;
- La Sous-direction de lutte contre la cybercriminalité (SDLC) [42], qui dépend de la Direction centrale de la police judiciaire, est compétente pour les attaques ayant ciblé un système d'information situé à l'extérieur du périmètre d'intervention de la BEFTI ;

- Au même titre que la SDLC, le Centre de lutte contre les criminalités numériques (C3N), anciennement la Division de lutte contre la cybercriminalité (DLCC) [43], du Service technique de recherches judiciaires et de documentation (STRJD) [44] de la gendarmerie nationale peut être contactée afin d'effectuer un dépôt de plainte.

Il est également possible de déposer plainte auprès des enquêteurs spécialisés des services territoriaux de la police (Investigateurs en cybercriminalité ou ICC) ou de la gendarmerie nationale (N-TECH), qui pourront réorienter les demandes vers les services spécialisés en cas de nécessité.

Les contacts des différents organismes sont donnés sur le site web de l'ANSSI :

`http://www.ssi.gouv.fr/en-cas-dincident`

Chapitre 4

Comment éviter de participer à un DDoS ?

S'il est indispensable de prendre en compte les risques d'attaque DDoS, il convient également de veiller à ne pas être un vecteur utilisé pour mener ce type d'attaque. Pour ce faire, il est nécessaire d'appliquer un certain nombre d'éléments d'hygiène informatique [45]. Cette section, sans être exhaustive, décrit certaines bonnes pratiques devant être mises en œuvre. Par ailleurs, il est important de noter que ces bonnes pratiques ne sont pas forcément spécifiques aux attaques DDoS, et que leur mise en œuvre augmente le niveau de sécurité général d'un système d'information.

4.1 Réduction de la surface d'attaque

La plupart des attaques DDoS sont menées grâce à des réseaux de machines compromises. D'une manière générale, il convient de réduire la surface d'attaque d'un système d'information.

4.1.1 Désactivation des services inutiles

Des services inutilisés peuvent être exploités pour mener des attaques DDoS. Par exemple, le protocole CHARGEN est régulièrement utilisé pour mener des attaques volumétriques [46]. Les services inutilisés doivent donc être désactivés au niveau des serveurs. Par ailleurs, une entité hébergeant des services exploitables peut interdire l'interrogation de tels services au moyen de règles de pare-feu à la bordure de son réseau.

Important

Les services inutilisés doivent être désactivés au niveau des serveurs. Par ailleurs, une entité hébergeant des services exploitables peut mettre en place des règles permettant de limiter le trafic à la bordure de son réseau, voire de le filtrer afin d'interdire l'interrogation de tels services.

4.1.2 Durcissement des systèmes d'exploitation

Afin de réduire le risque de compromission des serveurs exposés, et, en particulier, la participation à un *botnet*, les systèmes d'exploitation doivent faire l'objet de mesures de durcissement. Concernant les serveurs Linux, les recommandations de sécurité de l'ANSSI recensent les mesures à mettre en œuvre [47]. Parmi les points d'attention, on peut notamment citer :

- l'application du principe de moindre privilège aux logiciels ;
- la configuration des options de montage des partitions. Par exemple, les fichiers servis par un serveur web peuvent être placés sur une partition dédiée, et disposant des options de montage `nosuid` [48], `nodev` [48] et `noexec` [48] ;
- la mise en œuvre d'un noyau durci à l'aide de correctifs de durcissement tels *grsecurity* [49] et *PaX* [50].

4.1.3 Durcissement des configurations des services

Il est important de restreindre la configuration des services aux seules fonctions nécessaires. En effet, des implémentations offrent parfois certaines fonctionnalités dont l'usage peut être détourné à des fins malveillantes. Il peut s'agir, par exemple, de mécanismes de supervision, ou encore de fonctions de débogage. Lorsque ces fonctionnalités sont nécessaires, il faut veiller à ce qu'elles puissent être opérées uniquement depuis les réseaux d'administration ou de supervision. D'une manière générale, il faut, dans la mesure du possible, restreindre les interfaces réseau depuis lesquelles les services sont accessibles.

Des services n'ayant pas vocation à être utilisés en dehors d'un réseau local peuvent également être exploités. C'est notamment le cas de SSDP (*Simple Service Discovery Protocol*), employé pour la découverte d'équipements UPnP [14] (*Universal Plug and Play*) sur un réseau local. Dans ce cas, il convient de s'assurer que les équipements sur lesquels le service est nécessaire sont configurés de manière à ne pas répondre aux requêtes provenant d'un réseau externe à l'entité (comme l'Internet). Lorsque c'est possible, des mises à jour ou des correctifs de sécurité doivent être appliqués.

Par ailleurs, les bonnes pratiques de configuration des services et protocoles mis en œuvre doivent être appliquées. Par exemple, le protocole SNMP permet d'administrer et de superviser des équipements au moyen de l'envoi de requêtes spécifiant une chaîne de caractère appelée communauté. Dans les versions antérieures à la version 3, la sécurité de ce protocole reposait sur la connaissance des communautés. Ces dernières doivent donc être traitées comme des mots de passe [7]. En particulier, les chaînes par défaut (*public* pour la lecture, *private* pour l'écriture) doivent être modifiées. Par ailleurs, l'accès aux équipements *via* le protocole SNMP doit également être restreint au réseau d'administration ou de supervision. En outre, l'usage de la version 3 du protocole SNMP (niveau de sécurité `authPriv`) doit être privilégié.

7. L'ANSSI fournit des recommandations permettant de choisir judicieusement un mot de passe [51].

Enfin, le recours à des vérifications régulières du réseau peut contribuer à détecter des services indésirables. Des initiatives publiques telles que l'*Open Resolver Project* [52], l'*Open NTP Project* [53], l'*Open SNMP Project* [54] ou encore l'*Open SSDP Project* [55] peuvent aider à découvrir des équipements mal configurés.

4.1.3.1 L'exemple de NTP

L'exploitation de l'implémentation *ntpd* présentée à la section 1.3.3.2 donne un exemple d'utilisation malveillante de fonctionnalité de supervision.

Les mesures de précaution suivantes sont nécessaires afin de ne pas participer à une attaque par déni de service utilisant NTP :

- s'assurer que la fonctionnalité *monlist* est désactivée, en mettant à jour l'implémentation, et en la désactivant explicitement dans la configuration du serveur (instruction `disable monitor` pour *ntpd*). Si cette fonctionnalité est utilisée à des fins de supervision, il est nécessaire de s'assurer qu'elle ne peut l'être que depuis des réseaux d'administration prévus à cet effet ;
- restreindre l'accès aux fonctions utilisant les paquets *mode 6* (par exemple, la commande *readvar*) aux sous-réseaux ou adresses IP depuis lesquels cette fonction peut être utilisée légitimement au niveau de la configuration du serveur NTP. Ceci peut s'effectuer en interdisant, par défaut, de répondre aux requêtes des clients (instruction `noquery` pour *ntpd*), et en s'assurant que la configuration comporte cette instruction pour les sous-réseaux ou hôtes non autorisés.

Par ailleurs, le lecteur peut se référer aux modèles de configuration fournis par *Team Cymru* [56].

À retenir

Les services ou fonctionnalités inutilisés doivent être désactivés. Au minimum, ces services ne doivent pas être accessibles *via* l'internet. Les fonctionnalités de supervision ou de débogage ne doivent être accessibles que depuis les réseaux d'administration de l'entité.

4.1.4 Sécurité des applications web

Les applications web peuvent comporter des vulnérabilités susceptibles d'être exploitées pour mener des attaques DDoS [57].

Un attaquant peut exploiter une inclusion dynamique de fichiers (*Remote File Inclusion* ou RFI) dans le code d'une application pour déposer des scripts qui lui permettront ensuite d'exécuter des commandes (par exemple, un *shell* PHP). Les RFI sont parfois

utilisés pour créer des *botnets*. En 2012, une campagne d'attaques par déni de service contre des institutions financières nord-américaines a été menée à partir d'applications compromises *via* ce type de vulnérabilité [58].

Les failles XSS (*Cross-Site Scripting*) peuvent également être utilisées pour mener des attaques DDoS. Par exemple, en avril 2014, une faille XSS présente sur un site web très populaire a été exploitée pour générer un nombre important de requêtes HTTP `GET` vers un serveur web [59].

Afin de limiter la surface d'attaque et l'impact des tentatives de déni de service, les applications web ainsi que les *frameworks*, les CMS (*Content Management System*) et les greffons utilisés doivent être maintenus à jour. Par ailleurs, le développement de ces applications doit suivre les bonnes pratiques. Un audit de code peut révéler des failles qui pourraient être exploitées par des attaquants. Pour plus d'informations, le lecteur peut consulter les recommandations de l'ANSSI [60] concernant la sécurité des applications web.

À retenir

Les applications web peuvent être exploitées pour mener des attaques par déni de service distribué. Les *frameworks*, les CMS (*Content Management System*) et les greffons utilisés doivent être maintenus à jour. Par ailleurs, le développement de ces applications doit respecter les bonnes pratiques.

4.2 Filtrage du trafic

D'une manière générale, l'accès aux services doit être restreint afin de n'autoriser que les réseaux internes d'une entité. Par exemple, les résolveurs DNS d'une société ne doivent être interrogés que depuis des sous-réseaux de cette société.

La mise en place de règles de *rate-limiting* peut réduire une éventuelle participation à une attaque par déni de service. Un exemple concerne la mise en œuvre de mécanismes de type RRL (*Response Rate Limiting* [61]) sur les serveurs DNS faisant autorité. Ce mécanisme permet de limiter le nombre maximum de réponses par seconde envoyées à un client, et réduit ainsi le volume de trafic généré par un attaquant qui chercherait à exploiter le serveur. Il convient de noter que la limitation de trafic peut cependant être mise à profit par un attaquant et se retourner contre la victime. Cela est d'autant plus vrai pour les protocoles autorisant l'usurpation d'adresse IP, comme le protocole UDP [62].

En outre, il convient de filtrer le trafic sortant de l'entité. En particulier, le trafic sortant avec des adresses IP sources n'appartenant pas à un sous-réseau géré par l'entité

doit être filtré. Cette mesure permet d'éviter l'envoi de trafic pour lequel les adresses IP sources sont usurpées. Elle peut être mise en œuvre à l'aide de règles de pare-feu ou en activant des mécanismes de type URPF (*Unicast Reverse Path Forwarding*) [63]. L'URPF empêche le transfert de paquets dont les adresses IP sources ne sont pas joignables par une route empruntant l'interface sur laquelle les paquets ont été reçus.

Enfin, il est nécessaire de superviser le réseau d'une entité afin de détecter des anomalies dans le trafic, comme une augmentation de volume significative.

À retenir

L'accès aux services d'une entité doit être restreint afin de n'autoriser que les réseaux internes à celle-ci. Par ailleurs, la mise en place de règles de *rate-limiting* peut réduire une éventuelle participation à une attaque par déni de service. Enfin, le trafic sortant de l'entité doit être filtré afin de bloquer l'envoi de trafic pour lequel les adresses IP sources sont usurpées.

Chapitre 5

Rappel des points essentiels

À retenir

Le nombre d'attaques par déni de service distribué a augmenté au cours des dernières années. Ces attaques sont aujourd'hui fréquentes, et peuvent viser toute entité disposant d'une infrastructure réseau connectée à Internet.

Important

Une entité peut être victime d'une attaque DDoS volumétrique exploitant un protocole bien qu'elle n'expose pas de service reposant sur ce même protocole.

À retenir

Les pare-feux et les répartiteurs de charge peuvent contribuer à absorber certaines attaques DDoS, mais ils ne constituent pas une protection suffisante contre ce type d'attaque d'une manière générale. Par ailleurs, les limites de ces équipements sont parfois exploitées pour rendre des services indisponibles. Cependant, il est parfois possible de modifier la configuration de ces équipements afin d'améliorer leur résistance face à ce dernier type d'attaque (par exemple, en augmentant la taille des tables d'état).

À retenir

Certains équipements dédiés offrent différentes contre-mesures spécifiques aux attaques DDoS. Leur mise en œuvre nécessite une prise en main préalable, et un paramétrage adapté au trafic de l'entité.

À retenir

L'intervention de l'opérateur de transit est parfois nécessaire, en particulier lorsque le lien réseau mis à disposition du client est saturé. Les opérateurs permettent souvent d'effectuer du *blackholing* de trafic basé sur la destination. Il convient de noter que cette mesure, parfois nécessaire, rend le déni de service effectif. L'opérateur peut également offrir un service de filtrage de trafic. Dans le cas où ce service est opéré par le client, ce dernier doit s'assurer de maîtriser la configuration des différentes contre-mesures offertes par la plate-forme.

À retenir

Les hébergeurs offrent parfois une protection contre les attaques DDoS. Les différentes options proposées peuvent constituer une solution pour les structures faisant appel à une société externe pour l'hébergement de leurs serveurs.

À retenir

Les CDN permettent la répartition de ressources sur un grand nombre de serveurs, ce qui peut contribuer à améliorer la résistance aux attaques DDoS.

Important

En cas de recours à une redirection *via* le protocole DNS, il faut s'assurer qu'il n'existe pas de moyen trivial de découvrir l'adresse IP à protéger.

À retenir

Il est nécessaire de prendre des précautions avant la mise en œuvre d'une protection contre les attaques DDoS basée sur la résolution de nom. Cette méthode a une limite importante : le trafic à destination de l'entité ainsi protégée ne transite pas forcément par le fournisseur de la protection.

Important

Le recours à cette solution de protection nécessite la mise en œuvre d'une interconnexion entre l'entité et le fournisseur du service de protection. Cette interconnexion peut consister en l'établissement d'un tunnel GRE, ou, lorsque c'est possible, être directe et établie physiquement.

À retenir

Le déroutement de trafic permet de faire transiter l'intégralité du trafic vers le fournisseur du service de protection. Cette solution offre un bien meilleur niveau de protection qu'une solution basée sur la résolution de nom. En revanche, la souscription à ce type de service est généralement plus onéreuse.

Important

Il est impératif de disposer de contacts appropriés en interne, chez les opérateurs de transit, ainsi qu'auprès des fournisseurs d'un service de protection pour réagir efficacement en cas d'attaque.

Important

Dans la mesure du possible, il est important de s'assurer que les fournisseurs de services dont dépend une entité sont préparés aux attaques DDoS.

Important

Il est nécessaire de disposer de moyens de supervision et d'alerte afin de détecter un incident.

Important

Les services inutilisés doivent être désactivés au niveau des serveurs. Par ailleurs, une entité hébergeant des services exploitables peut mettre en place des règles permettant de limiter le trafic à la bordure de son réseau, voire de le filtrer afin d'interdire l'interrogation de tels services.

À retenir

Les services ou fonctionnalités inutilisés doivent être désactivés. Au minimum, ces services ne doivent pas être accessibles *via* l'internet. Les fonctionnalités de supervision ou de débogage ne doivent être accessibles que depuis les réseaux d'administration de l'entité.

À retenir

Les applications web peuvent être exploitées pour mener des attaques par déni de service distribué. Les *frameworks*, les CMS (*Content Management System*) et les greffons utilisés doivent être maintenus à jour. Par ailleurs, le développement de ces applications doit respecter les bonnes pratiques.

À retenir

L'accès aux services d'une entité doit être restreint afin de n'autoriser que les réseaux internes à celle-ci. Par ailleurs, la mise en place de règles de *rate-limiting* peut réduire une éventuelle participation à une attaque par déni de service. Enfin, le trafic sortant de l'entité doit être filtré afin de bloquer l'envoi de trafic pour lequel les adresses IP sources sont usurpées.

Bibliographie

[1] Bill Brenner, Akamai, « DDoS Attacks Used As Cover For Other Crimes ». <https://blogs.akamai.com/2013/08/DDoS-Attacks-Used-As-Cover-For-Other-Crimes.html>, août 2013.

[2] FBI, FS-ISAC, IC3, « Fraud Alert - Cyber Criminals Targeting Financial Institution Employee Credentials to Conduct Wire Transfer Fraud ». <http://www.ic3.gov/media/2012/FraudAlertFinancialInstitutionEmployeeCredentialsTargeted.pdf>, sept. 2012.

[3] Prolexic Security Engineering & Research Team, « Q4 2014 State of the Internet – Security Report ». <http://www.stateoftheinternet.com/resources-web-security-2014-q4-internet-security-report.html>, jan. 2015.

[4] Prolexic Security Engineering & Response Team, « Prolexic Quarterly Global DDoS Attack Report Q4 2013 ». <http://www.stateoftheinternet.com/resources-web-security-2013-q4-global-ddos-attack-report.html>, jan. 2014.

[5] Prolexic Security Engineering & Response Team, « Prolexic Quarterly Global DDoS Attack Report Q4 2012 ». <http://www.stateoftheinternet.com/resources-web-security-2012-q4-global-ddos-attack-report.html>, jan. 2013.

[6] Basecamp, « Basecamp was under network attack this morning ». <https://signalvnoise.com/posts/3728-basecamp-was-under-network-attack-this-morning>, mars 2014.

[7] Feedly, « Denial of service attack [Neutralized] ». <http://blog.feedly.com/2014/06/11/denial-of-service-attack/>, juin 2014.

[8] Curt Wilson, Arbor Networks ASERT, « Attack of the Shuriken: Many Hands, Many Weapons ». <http://www.arbornetworks.com/asert/2012/02/ddos-tools/>, fév. 2012.

[9] Prolexic Security Engineering & Response Team, « Prolexic Quarterly Global DDoS Attack Report Q3 2013 ». <http://www.stateoftheinternet.com/resources-web-security-2013-q3-global-ddos-attack-report.html>, oct. 2013.

[10] Brian Krebs, « DDoS Services Advertise Openly, Take PayPal ». <http://krebsonsecurity.com/2013/05/ddos-services-advertise-openly-take-paypal/>, mai 2013.

[11] P. Mockapetris, « Domain names - concepts and facilities ». RFC 1034 (INTERNET STANDARD), nov. 1987. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936.

[12] D. Mills, J. Martin, J. Burbank et W. Kasch, « Network Time Protocol Version 4 : Protocol and Algorithms Specification ». RFC 5905 (Proposed Standard), juin 2010.

[13] R. Presuhn, « Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) ». RFC 3416 (INTERNET STANDARD), déc. 2002.

[14] Contributing Members of the UPnP Forum, « UPnP™ Device Architecture 1.1 ». <http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf>, oct. 2008.

[15] J. Postel, « Character Generator Protocol ». RFC 864 (INTERNET STANDARD), mai 1983.

[16] Agence nationale de la sécurité des systèmes d'information (ANSSI), « Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine ». <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-des-reseaux/bonnes-pratiques-pour-lacquisition-lexploitation-de-noms-de-domaine.html>, mai 2014.

[17] NTP development team, « NTP Software Downloads ». <http://www.ntp.org/downloads.html>.

[18] Wong Onn Chee, Tom Brennan, « H.....t.....t....p.....p....o....s....t ». <https://www.owasp.org/images/4/43/Layer_7_DDOS.pdf>, nov. 2010.

[19] Roland Dobbins, « Breaking the Bank - An Analysis of the 2012 - 2013 Operation Ababil' Financial Industry DDoS Attack Campaign ». <https://ripe67.ripe.net/presentations/199-breakingthebank.pdf>, oct. 2013.

[20] J. Postel, « Internet Protocol ». RFC 791 (INTERNET STANDARD), sept. 1981. Updated by RFCs 1349, 2474, 6864.

[21] Agence nationale de la sécurité des systèmes d'information (ANSSI), « Recommandations de sécurité concernant l'analyse des flux HTTPS ». <http://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-concernant-lanalyse-des-flux-https/>, oct. 2014.

[22] Agence nationale de la sécurité des systèmes d'information (ANSSI), « Observatoire de la résilience de l'Internet français ». <http://www.ssi.gouv.fr/observatoire/>.

[23] W. Kumari et D. McPherson, « Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF) ». RFC 5635 (Informational), août 2009.

[24] D. Turk, « Configuring BGP to Block Denial-of-Service Attacks ». RFC 3882 (Informational), sept. 2004.

[25] ICANN, « Factsheet - root server attack on 6 february 2007 », mars 2007.

[26] R. Arends, R. Austein, M. Larson, D. Massey et S. Rose, « DNS Security Introduction and Requirements ». RFC 4033 (Proposed Standard), mars 2005. Updated by RFCs 6014, 6840.

[27] D. Farinacci, T. Li, S. Hanks, D. Meyer et P. Traina, « Generic Routing Encapsulation (GRE) ». RFC 2784 (Proposed Standard), mars 2000. Updated by RFC 2890.

[28] Vasco Asturiano, « The Shape of a BGP Update ». <https://labs.ripe.net/Members/vastur/the-shape-of-a-bgp-update>, fév. 2011.

[29] Rodney Joffe, « UltraDNS DDoS Attack Update ». <http://blog.neustar.biz/neustar-insights/ultradns-ddos-attack-update/>, mai 2014.

[30] Russ McRee, « UltraDNS DDOS ». <https://isc.sans.edu/diary/UltraDNS+DDOS/18051>, mai 2014.

[31] Xittel, « L'affaire Xittel : survivre aux DDoS ». <http://www.xittel.net/fr/residentiel/nouvelles/2013/10/l-affaire-xittel-survivre-aux-ddos.aspx>, oct. 2013.

[32] Agence nationale de la sécurité des systèmes d'information (ANSSI), « Dénis de service - Prévention et réaction ». <http://www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001/index.html>, jan. 2012.

[33] B. Claise, « Cisco Systems NetFlow Services Export Version 9 ». RFC 3954 (Informational), oct. 2004.

[34] B. Claise, B. Trammell et P. Aitken, « Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information ». RFC 7011 (INTERNET STANDARD), sept. 2013.

[35] Agence nationale de la sécurité des systèmes d'information (ANSSI), « Recommandations de sécurité pour la mise en oeuvre d'un système de journalisation ». <http://www.ssi.gouv.fr/fr/guides-et-bonnes-

pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-pour-la-mise-en-oeuvre-d-un-systeme-de.html>, déc. 2013.

[36] « Code des postes et des communications électroniques - Article D98-5 ». <http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=4AB8CBDD01BEF965466A599DA59F9FE0.tpdila10v_1?idArticle=LEGIARTI000025703451&cidTexte=LEGITEXT000006070987&categorieLien=id&dateTexte=20150210>, 2012.

[37] « Code de la défense - Article L1332-6-2 ». http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000028342867, déc. 2013.

[38] « Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique ». <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000875419>, jan. 1988.

[39] « Code pénal - Article 323-1 ». <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418316&cidTexte=LEGITEXT000006070719>, mars 2012.

[40] « Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation ». <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000026140136&categorieLien=id>, juil. 2012.

[41] Ministère de l'intérieur, « La brigade d'enquêtes sur les fraudes aux technologies de l'information ». <http://www.prefecturedepolice.interieur.gouv.fr/Nous-connaitre/Services-et-missions/Missions-de-police/La-direction-regionale-de-la-police-judiciaire/La-brigade-d-enquetes-sur-les-fraudes-aux-technologies-de-l-information>.

[42] Ministère de l'intérieur, « Une sous-direction pour organiser la lutte contre la cybercriminalité ». <http://www.police-nationale.interieur.gouv.fr/Actualites/L-actu-police/Une-sous-direction-pour-organiser-la-lutte-contre-la-cybercriminalite>.

[43] Ministère de l'intérieur, « La Division de lutte contre la cybercriminalité ». <http://www.gendarmerie.interieur.gouv.fr/pjgn/Organisation/Le-STRJD2/Cybercriminalite>.

[44] Ministère de l'intérieur, « Recherches et documentation (STRJD) ». <http://www.gendarmerie.interieur.gouv.fr/fre/Sites//Notre-Institution/Nos-missions2/Police-judiciaire/Recherches-et-documentation-STRJD>.

[45] Agence nationale de la sécurité des systèmes d'information (ANSSI), « Guide d'hygiène informatique ». <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/l-anssi-publie-la-version-finalisee-du-guide-d-hygiene-informatique.html>, jan. 2013.

[46] Prolexic Security Engineering & Response Team, « Prolexic Quarterly Global DDoS Attack Report Q1 2014 ». <http://www.stateoftheinternet.com/resources-web-security-2014-q1-global-ddos-attack-report.html>, avril 2014.

[47] Agence nationale de la sécurité des systèmes d'information (ANSSI), « Recommandations de sécurité relatives à un système GNU/Linux ». <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-relatives-a-un-systeme-gnu-linux.html>, juil. 2012.

[48] Karel Zak, « mount(8) - Linux manual page ». <http://man7.org/linux/man-pages/man8/mount.8.html>.

[49] Brad Spengler, « grsecurity ». <https://grsecurity.net/>.

[50] The PaX Team, « Homepage of The PaX Team ». <https://pax.grsecurity.net/>.

[51] Agence nationale de la sécurité des systèmes d'information (ANSSI), « Recommandations de sécurité relatives aux mots de passe ». <http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/mot-de-passe.html>, mai 2012.

[52] Jared Mauch, « Open Resolver Project ». <http://openresolverproject.org/>.

[53] Jared Mauch, « OpenNTPProject.org - NTP Scanning Project ». <http://openntpproject.org/>.

[54] Jared Mauch, « OpenSNMPProject.org - SNMP Scanning Project ». <http://opensnmpproject.org/>.

[55] Jared Mauch, « OpenSSDPProject.org - SSDP Scanning Project ». <http://openssdpproject.org/>.

[56] Team Cymru, « Secure NTP Template ». <http://www.team-cymru.org/secure-ntp-template.html>, 2015.

[57] Prolexic Security Engineering & Response Team, « Prolexic Quarterly Global DDoS Attack Report Q2 2014 ». <http://www.prolexic.com/knowledge-center-ddos-attack-report-2014-q2.html>, juil. 2014.

[58] Prolexic Security Engineering & Response Team, « Prolexic Issues Threat Advisory on itsoknoproblembro (BroDoS) Toolkit ». <http://www.prolexic.com/ddos-dispatch/five/itsoknoproblembro-brodos-ddos-toolkit-threat-advisory.html>, jan. 2013.

[59] Incapsula, « One of World's Largest Websites Hacked: Turns Visitors into "DDoS Zombies" ». <http://www.incapsula.com/blog/world-largest-site-xss-ddos-zombies.html>, avril 2014.

[60] Agence nationale de la sécurité des systèmes d'information (ANSSI), « Recommandations pour la sécurisation des sites web ». <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-des-applications-web/recommandations-pour-la-securisation-des-sites-web.html>, avril 2013.

[61] Paul Vixie et Vernon Schryver, « DNS Response Rate Limiting (DNS RRL) ». <http://ss.vix.su/~vixie/isc-tn-2012-1.txt>, avril 2012.

[62] Florian Maury, Mathieu Feuillet, « Démonstration d'un détournement possible de technologies anti-déni de service distribué (DDoS) ». <http://www.ssi.gouv.fr/fr/anssi/publications/publications-scientifiques/articles-de-conferences/demonstration-d-un-detournement-possible-de-technologies-anti-deni-de-service.html>, oct. 2013.

[63] P. Ferguson et D. Senie, « Network Ingress Filtering : Defeating Denial of Service Attacks which employ IP Source Address Spoofing ». RFC 2827 (Best Current Practice), mai 2000. Updated by RFC 3704.

À propos de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.
En vertu du décret n° 2009-834 du 7 juillet 2009 modifié par le décret n° 2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.
Pour en savoir plus sur l'ANSSI et ses missions, rendez-vous sur www.ssi.gouv.fr.

Mars 2015

Agence nationale de la sécurité des systèmes d'information
ANSSI - 51 boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
Sites internet : `www.ssi.gouv.fr` et `www.securite-informatique.gouv.fr`
Messagerie : communication [at] ssi.gouv.fr