Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 14 janvier 2013
N° CERTA-2012-INF-001-001

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : Dénis de service - Prévention et réaction

Gestion du document

Référence	CERTA-2012-INF-001-001
Titre	Dénis de service - Prévention et réaction
Date de la première version	27 janvier 2012
Date de la dernière version	14 janvier 2013
Source	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Introduction

Une attaque en déni de service provoque des dysfonctionnements ou paralyse complètement un ou plusieurs services de la victime.

Il est courant qu'une attaque de cette nature sollicite une ressource particulière du système d'information de la cible, jusqu'à « épuisement ». Cette ressource peut être la bande passante du réseau, la capacité de traitement globale d'une base de données, la puissance de calcul des processeurs, l'espace disque, etc.

La lutte contre les dénis de service est souvent une affaire de rapport de force. À défaut de pouvoir les empêcher, la victime potentielle doit prendre des dispositions pour en atténuer les effets.

L'agresseur peut n'utiliser qu'un seul ordinateur, mais en pratique cette situation est rare. Le plus souvent, il fait appel à un nombre important d'ordinateurs compromis, réunis dans un réseau de zombies (*botnet*). On parle alors de déni de service distribué, en anglais DDoS pour *Distributed Denial of Service*.

De plus, un élément d'un système d'information peut subir un déni de service dont il n'est pas la cible (effet collatéral). Ainsi, un site Web hébergé chez un prestataire peut souffrir des attaques visant un autre client du prestataire, dès lors qu'une partie de l'infrastructure est partagée (réseau, serveur, pare-feu...).

Cette note vise à donner des orientations pour se préparer à l'éventualité d'une attaque en déni de service et pour en amoindrir les impacts. Elle s'articule en plusieurs parties :

– des mesures techniques et organisationnelles à mettre en place avant d'être confronté à une attaque ;
– des mesures de réaction pour faire face à ces attaques ;

– à titre informatif, des causes d'indisponibilité connues, qui peuvent guider les techniciens lors de l'analyse et dans le mode de réaction.

Les mesures proposées dans ce document sont à décliner au regard des spécificités et de la politique de sécurité globale et à la politique de sécurité des systèmes d'information (PSSI) de chaque organisation. Cette PSSI peut contenir un plan de continuité d'activité (PCA) ou le volet informatique de ce plan. Cette PSSI sera le fruit d'une analyse de risques qui prendra en compte le degré d'indisponibilité acceptable des services et des systèmes potentiellement impactés.

2 Mesures de prévention

La prévention est à la fois organisationelle et technique.

2.1 S'organiser

Il convient de recenser :

– les acteurs techniques (internes et prestataires), hiérarchiques, juridiques, de communication amenés à intervenir et, pour chacun d'eux, leur rôle et leur limite de décision. Ces informations peuvent être regroupées dans un annuaire qui doit être tenu à jour ;
– les services offerts par les prestataires, en particulier les fournisseurs d'accès à l'Internet et les hébergeurs et faire compléter si besoin ces prestations dans une optique de lutte contre les dénis de service ;
– les services critiques, au sens des métiers, et les infrastructures informatiques sur lesquelles ils reposent ;
– les systèmes, critiques ou non, susceptibles d'être ciblés par des attaques en dénis de service ;
– les flux indispensables au fonctionnement de l'organisme et leur description technique (protocoles, direction de cheminement, parties du système d'information concernées, etc.) ;
– les procédures de signalement, de traitement des signalements, de réaction, de communication et de décision ;
– les procédures et les documentations d'exploitation technique, en particulier pour le déploiement des correctifs et pour les systèmes de filtrage, de supervision et de journalisation ;
– les documents d'architecture, à jour, des systèmes d'information.

Des contrôles et des exercices réguliers sont également des mesures préventives à mettre en oeuvre.

2.2 Prendre des mesures techniques

Les mesures organisationnelles débouchent en partie sur des mesures techniques appliquées avant que les attaques ne surviennent, dans le respect de la PSSI, comme :

– l'architecture adaptée aux contraintes d'un service critique. Ainsi, un serveur Web pourra être déporté sur un CDN (*Content Delivery Network*) pour avoir un premier niveau de résistance ;
– le cloisonnement des systèmes afin de permettre, par exemple, l'isolement d'un serveur ciblé par une attaque provenant de l'Internet, tout en permettant aux utilisateurs internes de continuer à s'y connecter : en effet, si par exemple le même accès Internet est utilisé pour le travail quotidien des utilisateurs et l'hébergement d'un serveur Web, une saturation de cet accès suite à une attaque DDoS visant le serveur Web peut perturber significativement le fonctionnement de l'organisme visé ;
– le recensement des systèmes, des briques logicielles et de leur niveau de mise à jour, pour les systèmes critiques et pour les systèmes exposés ;
– l'utilisation d'un outil de déploiement des correctifs de sécurité, de manière à limiter les possibilités de dénis de service par exploitation de vulnérabilités connues et corrigées ;
– la restriction des flux autorisés aux seuls flux utiles, au niveau des pare-feux et des équipements de filtrage ;
– la mise en place de moyens de secours, conformément au PCA, et des moyens de bascule, incluant les aspects sauvegarde, réseau, DNS, etc ;
– la mise en place de systèmes redondants (alimentations secourues, équipements réseau redondés) et/ou de capacité suffisante pour absorber des surcharges dans une limite acceptable et connue ;
– la gestion des ressources, comme la bande passante, de manière à limiter l'impact sur un service quand un autre est visé (exemple : faire en sorte qu'un DDoS sur le serveur Web ne paralyse pas la messagerie) ;
– la configuration restrictive des composants du système d'information, par inactivation, ou même désinstallation, des services inutilisés qui pourraient consommer beaucoup de ressources et offrir un point d'attaque ;

– la configuration restrictive des logiciels, comme la limitation des sessions venant d'une même adresse IP sur un serveur Web, la limitation de la réponse d'un annuaire LDAP en taille et en nombre d'entrées et du temps de recherche, la configuration empêchant un serveur Web de devenir un relais ouvert ;
– la supervision comprenant le suivi des consommations de ressources (bande passante, charge CPU, etc.) et la surveillance de disponibilité ;
– la préservation des traces telles que les journaux et les historiques de consommation des ressources système en fixant cependant des quotas relatifs à leurs volumes afin d'éviter un déni de service dû à une saturation de l'espace disque des machines ;
– la capacité à déployer des outils d'analyse permettant de caractériser le déni de service et ainsi de pouvoir prendre les mesures adaptées.

2.3 Détecter des dénis de service

Les mesures techniques (supervision, tests) et organisationnelles doivent faciliter la détection d'anomalies et d'attaques. Cela implique que les outils de supervision sont effectivement sous le contrôle permanent d'opérateurs humains, alertés de manière plus ou moins automatisée.

Parmi les indices classiques de ces attaques, on trouve :
– l'accroissement de la consommation de la bande passante, globale ou sur un ou plusieurs protocoles, ou depuis des sources particulières, ou vers des destinations particulières ;
– l'augmentation plus ou moins brutale de la consommation de ressources processeur, disque ou mémoire, sans explication légitime ;
– l'allongement des files d'attente des serveurs de messagerie ou le retard dans le temps de transit des messages ;
– des ruptures de communications sur délai de garde (*timeout*) ou signalées par message d'erreur (*host unreachable*) ;
– la présence dans les journaux de motifs nombreux et similaires voire identiques laissant penser à l'action de robots ou à des programmes qui sollicitent les ressources de manière systématique.

Le signalement de l'indisponibilité d'un service peut également provenir de l'extérieur (client, fournisseur, partenaire, CERT, etc.).

3 Mesures de réaction

La réaction doit se faire avec sang-froid et en menant une analyse rationnelle en relation avec les acteurs pertinents identifiés. Des actions irréfléchies peuvent aggraver l'impact du déni de service.

3.1 Analyser le déni de service

Cette analyse technique a deux objectifs : déterminer si la cause est accidentelle ou malveillante et prendre efficacement les mesures de réaction adaptées. En effet, les propriétés des technologies issues du monde de l'Internet (protocoles, adressage...) et des systèmes sont si variées que les dénis de service peuvent être multiformes.

Il est impératif de s'assurer que l'augmentation de la consommation d'une ressource n'est pas liée à une opération, peut-être rare ou ponctuelle, mais légitime.

L'analyse technique pourra également révéler qu'un dysfonctionnement (bogue, mauvaise configuration...) est la cause accidentelle du déni de service.

Il est important d'identifier quand cela est possible, entre autre :
– l'élément défaillant : s'agit-il d'un engorgement au niveau réseau qui entraîne une saturation des liens réseau (auquel cas il sera judicieux de se tourner vers son opérateur), d'un engorgement d'un service ou d'une application ne supportant pas une charge excessive ou encore d'une instabilité applicative due à du trafic anormal ;
– l'état de la cible : sollicitation élevée temporaire ou modification plus ou moins irréversible (destruction ou non de données, chiffrement malveillant du disque) ;
– le protocole utilisé : une requête HTTP donne l'IP de la source (cas des protocoles au-dessus de TCP en général), une requête DNS en UDP contient une adresse IP source indicative, donc rarement authentique lors des attaques (*spoofing*) ;
– la source (réseau interne, externe, IP unique, IP multiples, liaison utilisée en cas de multiplicité de FAI, accès WiFi) et compte tenu de l'item précédent, la fiabilité de cette information ;

– le discriminant : ce qui permet de distinguer le flux nuisible du trafic légitime inoffensif (forme de requête HTTP, User-Agent, champ MAILFROM du protocole SMTP) ;
– le mode de désignation de la cible : une IP, une plage complète, un ou plusieurs noms d'hôte, etc. ;
– la fonction de la ou des cibles : serveur Web, messagerie, DNS... ;

Les journaux des différents équipements réseau (routeurs, parefeux, etc.) ou système (serveur Web, proxy inverse, etc.) contiennent très souvent des éléments utiles à l'identification du problème et doivent être analysés en premier lieu.

L'utilisation d'analyseurs de flux (NetFlow, sFlow, IPFIX, etc.) peut également s'avérer utile pour diagnostiquer un DDoS (identification de la cible, des principales sources du trafic d'attaque, du service attaqué, etc.). Certains équipements réseau tels que les routeurs et parfois les commutateurs, disposent de fonctionnalités d'export des flux réseau vers des analyseurs de flux.

Dans tous les cas, les analyses doivent être conduites conformément à la réglementation en vigueur.

3.2 Prendre les dispositions organisationnelles

Selon les résultats de l'analyse, les mesures seront celles prévues dans la phase de préparation et qui seront confirmées au niveau décisionnel adéquat. Il est important de bien identifier les impacts associés à chacune des mesures prises (l'analyse des impacts pouvant judicieusement être réalisée en amont) et de ne pas agir de manière irréfléchie. En matière de mesures, il pourra s'agir :

– d'une notification du responsable, en cas de déni accidentel ;
– d'une notification de la cible, en cas de déni par effet collatéral ;
– d'un passage en mode dégradé ;
– l'activation des clauses d'un contrat de service avec le FAI, un CERT ou une société spécialisée ;
– du déclenchement du PCA ;
– de communications internes (vers le personnel), et externes (clients, grand public, partenaires, actionnaires) ;
– de décisions de nature juridique (report d'une échéance, dépôt de plainte...) ;
– ...

3.3 Cantonner l'attaque

Les mesure techniques de cantonnement seront extrêmement dépendantes de l'impact et de la technique utilisée par les attaquants et des choix faits dans la PSSI et par les instances de décision.

L'idée sous-jacente est d'arrêter le flux nuisible au plus près de la source et le plus finement possible. Cependant, des mesures générales peuvent être prises en urgence, puis remplacées par des mesures plus adaptées.

Par conséquent, les pistes indiquées ci dessous sont illustratives :

– si le flux hostile présente une caractéristique discriminante par rapport au flux normal, filtrer sur ce critère :
  – si la source se résume à un nombre d'IP réduit, bloquer ces IP au niveau des filtres (pare-feu, proxys inverses, antispams, gestionnaires de bande passante) ou chez le ou les FAI ;
  – si l'attaque vise un serveur par son adresse IP, modifier l'adresse IP et la résolution DNS de ce serveur ;
  – si l'attaque utilise un port particulier, bloquer ce port en entrée ou réduire la bande passante qui lui est allouée ;
  – si l'attaque congestionne le réseau interne et vise seulement quelques destinations internes (IP ou nom d'hôtes), blocage de ces destinations (IP ou noms d'hôtes) ;
– diminuer les durées de vie de résolution des hôtes ciblés (TTL) dans l'éventualité de changements dans les DNS. Ceci est déconseillé si les serveurs DNS sont eux-mêmes les cibles ;
– réduire les délais de rupture des connexions inactives (timeout) quand cela est pertinent (exemple : serveurs SMTP ou HTTP) ;
– durcir les limitations (nombre de connexions ouvertes à un instant donné par IP, volume des réponses, durée des recherches...) ;
– durcir les configurations des serveurs touchés selon le mode d'attaque observé (exemple : interdire des renégociations de session SSL, activer les protections par SYN cookies, etc.) ;
– adapter la capacité de journalisation ou de capture dans l'éventualité d'un dépôt de plainte (à moduler en fonction de l'impact technique de la journalisation) ;
– collecter les adresses d'origine, les traces horodatées, avec une estimation de leur fiabilité ;
– augmenter les ressources qui font défaut (duplication de serveurs et répartition de charge, allocation de bande passante...) ;

– réduire les ressources allouées aux services non essentiels ;
– installer les règles sur les systèmes de prévention des intrusions (IPS, Intrusion Prevention Systems) pour bloquer les flux indésirables ;
– déconnecter le réseau d'entreprise de l'Internet (ce qui peut être incompatible avec le besoin d'analyse et de traces). Cette option ne doit-être envisagée qu'en dernier recours et en ayant bien envisagé auparavant les effets de bord éventuels ;
– etc.

3.4 Reprendre le régime normal

Des agresseurs très motivés ont pu maintenir des dénis de service plusieurs jours durant. Dans les cas observés jusqu'à présent, ces attaques cessent d'elles-mêmes.

À la fin de l'attaque, il convient de reprendre les activités selon le PRA (plan de reprise d'activité).

À noter que certaines attaques en déni de service sont parfois utilisées par des attaquants à fin de diversion pour opérer à des vols de données ou à la mise en place de portes dérobées. Après chaque attaque subie en déni de service, il est important d'opérer un contrôle global des autres types d'attaques que les systèmes d'information de l'entreprise auraient pu subir.

3.5 Tirer les enseignements

Chaque incident est l'occasion de réaliser un retour d'expérience visant à apporter les modifications nécessaires des plans d'intervention, voire de modifier ou de durcir l'architecture, de revoir les contrats de prestation et d'améliorer l'organisation.

4 Causes possibles d'indisponibilité

Cette section donne des exemples de causes qui pourront éclairer l'analyse technique.

Une indisponibilité peut être due à de la malveillance mais aussi à des causes accidentelles. La première partie concerne les attaques tandis que la deuxième revient sur d'autres causes de déni de service.

4.1 Types d'attaques connues

Les techniques d'attaque évoluent sans cesse. L'utilisation de vulnérabilités (applicatives ou liées aux protocoles utilisés sur les réseaux) permet parfois de créer une asymétrie importante entre les ressources utilisées par l'agresseur et celles nécessaires pour les contrer.

La liste suivante indique des types d'attaques recensés ces dernières années :

– ICMP :
  – Smurf, rebond sur une addresse de *broadcast* (1998) ;
– UDP :
  – Rebond DNS ;
  – Rebond sur le protocole du jeu en réseau Quake3 (2011) ;
– TCP :
  – Sockstress/NKiller2, exploitation du *TCP Persist Timer* (2009, problème connu depuis 2005) ;
  – SYN flood ;
– HTTP :
  – Slowloris, requêtes incomplètes (2009) ;
  – Apache Killer, champs Range avec recouvrement multiples (2011) ;
  – Collision de condensés des requêtes sur PHP5, Java, ASP.NET, etc. (2011) ;
  – LOIC et HOIC ;
– SMTP :
  – NDR (Non delivery reports) ;
  – Sessions incomplètes.

Un déni de service peut également trouver sa source dans d'autres attaques :

– certaines attaques de type empoisonnement de caches DNS ;

– attaque d'une cible avec laquelle une infrastructure est partagée ;
– vague importante de pourriels ;
– ver ou virus qui saturent le réseau en tentant « bruyamment » de se répliquer.

4.2 Exemples de dénis de service accidentels

L'analyse technique ne peut exclure une cause accidentelle lorsqu'une indisponibilité est détectée. Les exemples ci-dessous sont illustratifs et non limitatifs :

– un accident matériel comme une perte d'énergie ou de climatisation, ou un arrachage de câble ;
– une opération de maintenance non signalée (interne, prestataire, opérateur) ;
– une erreur de programmation (bogue) qui provoque des boucles infinies ou remplit un disque ;
– une campagne de communication au lancement d'un serveur Web ou d'un service, qui provoque un pic de fréquentation qui dépasse les capacités prévue pour le régime « de croisière » ;
– un évènement ponctuel dont l'incidence est sous-estimée et qui provoque la saturation du service ou le ralentissement notable du système d'information (résultats financiers, évènement culturel, publication administrative) ;
– l'ajout de contenu lourd sur une page d'accueil (visite virtuelle en 3D) qui encombre le lien vers le FAI ;
– la mise à jour simultanée d'un logiciel sur des milliers de postes de travail, avec un programme volumineux et sans architecture de cache, qui sature des liens dans des services déconcentrés ;
– un publipostage électronique mal organisé qui occupe une passerelle antivirale à analyser des milliers de fois un même message, dont seul le destinataire change ;
– une simulation budgétaire lancée sur un serveur de partage bureautique qui en monopolise les ressources au détriment des autres utilisateurs internes.

Gestion détaillée du document

27 janvier 2012 version initiale.
14 janvier 2013 modifications mineures.