Septembre, 2014

GROUPE DE TRAVAIL 5
Remédiation des attaques DDoS basées sur les serveurs
Rapport final

Table des matières

1 Résultats en bref

1.1 Résumé exécutif

Les secteurs des infrastructures critiques ont été attaqués par un barrage d'attaques DDoS, dont certaines émanaient de centres de données et de fournisseurs d'hébergement. [1] Les attaques DDoS provenant des centres de données et des fournisseurs d'hébergement sont particulièrement problématiques en raison de la bande passante et des ressources informatiques élevées dont dispose un attaquant. Cela rend la prévention, la détection et l'atténuation plus importantes, mais aussi plus difficiles. Ce groupe de travail a examiné et formulé des recommandations au Conseil concernant les meilleures pratiques au niveau du réseau et d'autres mesures que les fournisseurs de communications et la FCC peuvent prendre pour atténuer les effets des attaques DDoS provenant de grands centres de données et de sites d'hébergement. Ces recommandations comprennent des méthodes et des procédures techniques/opérationnelles visant à faciliter la mise en œuvre des recommandations par les parties prenantes. Bien que ce rapport soit axé sur les fournisseurs de communications, il convient de noter que des mesures devront être prises dans l'ensemble de l'écosystème Internet, notamment par les fournisseurs d'hébergement, les fournisseurs d'équipements, les propriétaires et les exploitants d'infrastructures critiques, les autres parties prenantes qui dépendent d'Internet, et même potentiellement les utilisateurs finaux eux-mêmes, pour réussir à atténuer les attaques DDoS. Le groupe de travail 5 reconnaît également que, bien qu'elles sortent largement du cadre du présent rapport, les attaques DDoS basées sur les serveurs ne sont pas seulement un problème national, mais mondial. En fin de compte, les mesures prises par l'écosystème Internet comprennent des considérations internationales.

Dans ce rapport final, le groupe de travail 5 a formulé des recommandations que les fournisseurs de communications peuvent suivre pour atténuer l'incidence et l'impact des attaques DDoS provenant des centres de données et des fournisseurs d'hébergement, en particulier celles qui visent les systèmes d'information des secteurs d'infrastructures critiques. [2] Les recommandations se présentent principalement sous la forme de meilleures pratiques (BP) d'atténuation des attaques DDoS basées sur les serveurs, qui figurent à l'annexe E. En outre, plusieurs recommandations applicables sont incluses ici pour faire avancer le travail de prévention, de détection et d'atténuation des attaques DDoS basées sur les serveurs.

Le groupe de travail 5 a également évalué le niveau d'effort des FAI dans la mise en œuvre des BP par rapport à l'impact de la mise en œuvre des meilleures pratiques spécifiques afin de déterminer le sous-ensemble des meilleures pratiques qui ont un impact élevé mais un niveau d'effort relativement faible à mettre en œuvre. Le groupe de travail s'est également attaché à identifier les obstacles à la mise en œuvre des BP en se fondant sur les enseignements tirés des études de cas des sous-groupes des FAI, des experts en sécurité Internet et de la communauté financière, ainsi que d'autres obstacles fondés sur les expériences réelles des membres en matière d'atténuation des attaques DDoS. Le groupe de travail a également élaboré une taxonomie à utiliser pour l'application des meilleures pratiques. Enfin, le groupe s'est penché sur les mesures d'efficacité potentielles visant à évaluer les résultats positifs des BP volontaires au niveau du réseau pour atténuer les attaques DDoS basées sur les serveurs.

2 Introduction

Ce rapport final documente les efforts entrepris par le groupe de travail 5 du CSRIC IV et fournit les meilleures pratiques que les fournisseurs de communications peuvent suivre pour atténuer les attaques DDoS basées sur les serveurs, lancées à partir de serveurs généralement basés dans des centres de données et des fournisseurs d'hébergement. Le rapport final fournit également des recommandations concernant les actions que la FCC peut prendre pour aider à atténuer les attaques DDoS.

1 http://www.eweek.com/security/ddos-attacks-on-major-banks-causing-problems-for-clients/
2 http://www.dhs.gov/critical-infrastructure-sectors

l'occurrence et l'impact des attaques DDoS basées sur les serveurs.

Le groupe de travail 5 a rassemblé une équipe de plus de 40 membres, dont des représentants de FAI, d'institutions financières, de fournisseurs d'hébergement, d'organisations à but non lucratif, d'associations, d'universités, de gouvernements fédéraux et d'États, ainsi que des experts en sécurité, pour accomplir la tâche du CSRIC IV. Les efforts du groupe de travail 5 du CSRIC IV ont permis de tirer parti et de compléter d'autres activités liées aux botnets, notamment :

- Recommandations du CSRIC II3 et du CSRIC III4 en matière d'atténuation des attaques DDoS
- Groupe de travail sur la messagerie, les logiciels malveillants et les dispositifs mobiles anti-abus (M3AAWG)[5]
- Groupe de travail anti-botnet de l'Online Trust Alliance (OTA)6
- Cloud Security Alliance (CSA) [7]
- Industry Botnet Group (IBG)[8]

Le groupe de travail 5 a examiné la structure de base d'une attaque DDoS typique et les différents types d'attaques DDoS observés dans les environnements de réseau actuels. La figure 1 illustre une attaque DDoS basée sur un serveur. Les récentes attaques DDoS ont exploité les vulnérabilités des sociétés d'hébergement web et d'autres grands centres de données pour lancer des attaques DDoS sur des systèmes informatiques et des sites web. Ces attaques peuvent avoir une origine nationale ou internationale et viser des cibles nationales ou internationales. La prévention, la détection et l'atténuation de ces attaques sont complexes et nécessitent une coopération et un partage d'informations entre les FAI et les opérateurs de réseau, les centres de données et les fournisseurs d'hébergement, les fabricants d'infrastructures (c'est-à-dire la chaîne d'approvisionnement) et les propriétaires et opérateurs d'infrastructures critiques. Le groupe de travail s'est basé sur l'interaction de l'écosystème décrite ci-dessus pour décider des études de cas à entreprendre et des meilleures pratiques industrielles à prendre en compte pour cette tâche d'atténuation des attaques DDoS basées sur les serveurs.

3 http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-conseil-ii
4 http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-conseil-iii
5 http://www.maawg.org/m3aawg-san-francisco-meeting-addresses-latest-messaging-security-ranging-mobile-malware-ddos-attacks
6 https://otalliance.org/resources/botnets
7 https://cloudsecurityalliance.org/
8 http://www.ustelecom.org/blog/industry-botnet-group-takes-multi-party-approach-fight-cybercriminalité

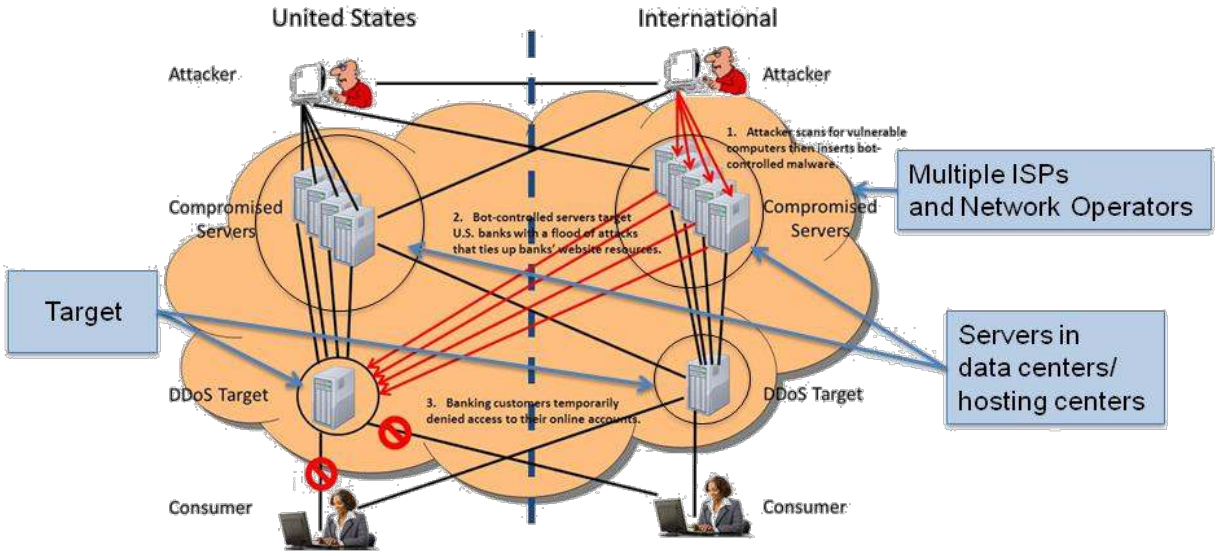


Figure 1 - Example of Server Based DDoS Attack

1

Le groupe de travail 5 a également effectué une analyse des lacunes afin de déterminer où les meilleures pratiques étaient manquantes, mais nécessaires, afin de s'aligner sur les phases du cycle de vie de la réponse aux incidents d'un FAI dans la protection et la réponse aux attaques DDoS basées sur les serveurs. Lorsque des lacunes ont été identifiées, le groupe de travail a formulé des recommandations pour de nouvelles meilleures pratiques.

Le groupe de travail 5 a appliqué le cycle de vie de la réponse aux incidents comme moyen de cartographier les meilleures pratiques et recommandations en matière de DDoS. Cette cartographie, ainsi que les recommandations classées par ordre de priorité dans chaque domaine, aideront les FAI à identifier les meilleures pratiques et les recommandations les plus importantes et les plus efficaces dans chaque domaine. Le groupe de travail a adapté le "cycle de vie d'un incident" d'Arbor Network aux "six phases de la préparation et de la réponse aux attaques DDoS" aux fins du présent rapport final, voir la figure 2 ci-dessous.

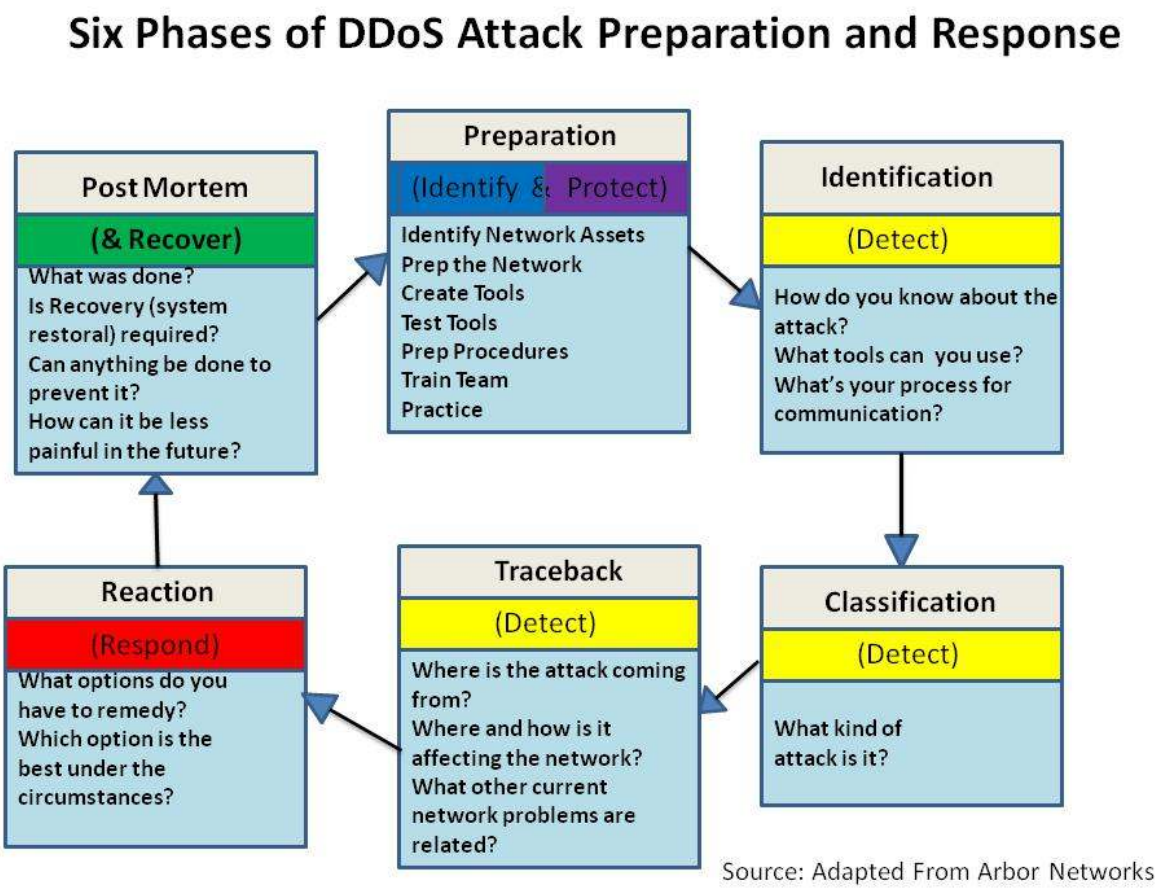


Figure 2. Six phases de préparation et de réponse à une attaque DDoS.

En conjonction avec le modèle en six phases, une taxonomie des activités (annexe A) a été créée afin de fournir des indications sur la manière dont les meilleures pratiques peuvent être utilisées dans chaque phase. Le modèle en six phases est une méthode de préparation et de réponse aux attaques conforme au cadre de cybersécurité du NIST. [9] Le modèle opérationnel des Six Phases est lié au cadre de cybersécurité du NIST de la manière suivante : La phase de préparation met en œuvre la fonction d'identification du NIST pour identifier les actifs du réseau à protéger et assure la fonction de protection du NIST en préparant le réseau et en créant des outils de détection et d'atténuation des DDoS. Les phases d'identification, de classification et de traçage sont liées à la fonction de détection du NIST. La phase de réaction est liée à la fonction de réponse du NIST, et la phase post-mortem à la fonction de récupération du NIST. Cette relation est illustrée ci-dessous dans la figure 3.

9 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

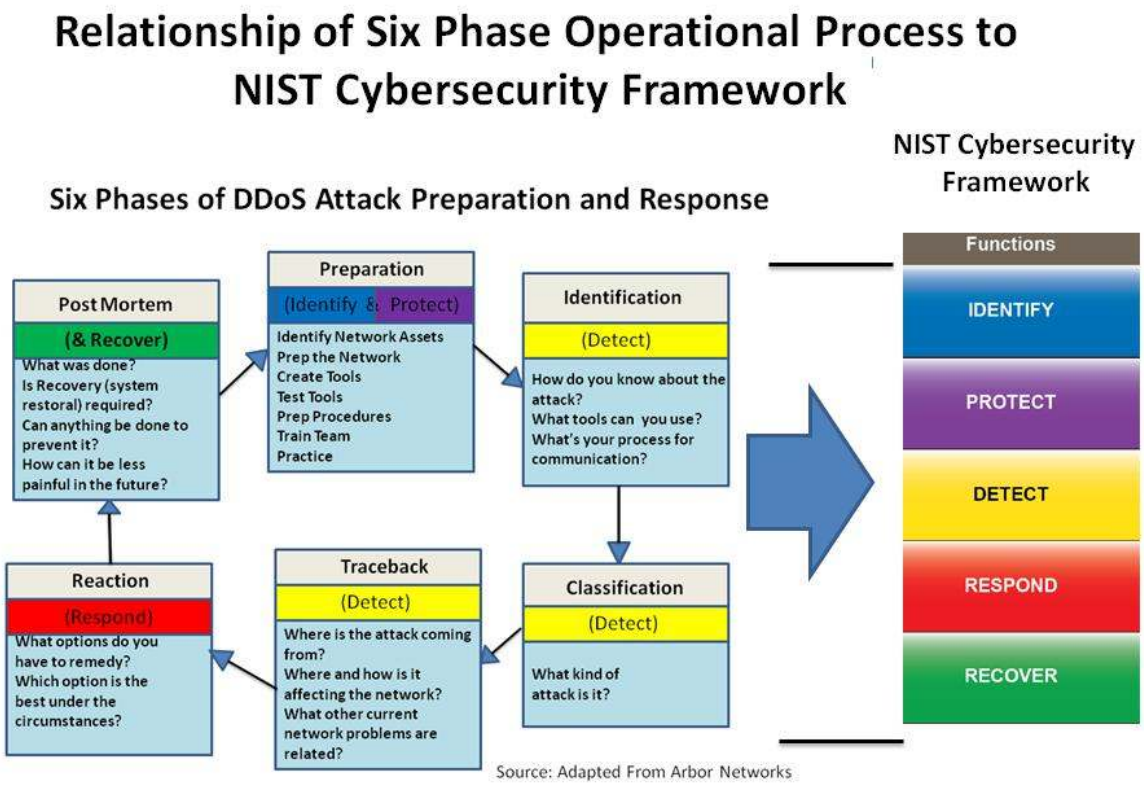


Figure 3. Relation entre le processus opérationnel en six phases et le cadre de cybersécurité du NIST.

Aux fins de l'analyse, le groupe de travail a utilisé la définition suivante d'une attaque DDoS : "une **attaque par déni de service (DoS)** ou par **déni de service distribué (DDoS)** est une tentative d'empêcher des utilisateurs légitimes d'accéder à des informations ou à des services10 (US-CERT)". Une attaque par déni de service distribué consiste en deux ou plusieurs systèmes ou attaquants engagés dans l'attaque en même temps vers la même cible. Les types d'attaques DDoS sont les suivants :

- Attaques volumétriques
  - Inondation directe de paquets
    - Des ordinateurs compromis et contrôlés à distance (bots) envoient du trafic d'attaque directement à la victime en essayant de remplir les circuits avec du mauvais trafic.
    - Des centaines, voire des dizaines de milliers de bots peuvent participer.
    - Les outils standard des FAI gèrent assez bien la plupart de ces types d'attaques.
    - Les paquets peuvent être soit usurpés, soit non usurpés.

  - Attaques d'amplification par réflexion
    - Les robots usurpent leur adresse IP source pour qu'elle corresponde à l'adresse IP de la victime.
    - Envoyez du trafic vers des services où la réponse sera bien plus importante que la question.

10 http://www.us-cert.gov/ncas/tips/ST04-015

        - Les serveurs DNS sont de grands amplificateurs pour ces types d'attaques.
        - Des facteurs d'amplification de plus de 200 fois sont possibles.
        - Les paquets doivent être usurpés.

- Attaques de la couche application
    - Les logiciels malveillants des bots sont conçus pour envoyer au serveur web ou à un autre serveur d'application un trafic qui semble provenir des ressources informatiques importantes d'un client et d'un consommateur légitimes.
    - Des volumes de trafic plus faibles.
    - Les attaquants doivent travailler davantage pour atteindre leurs objectifs.
    - Le trafic crypté est plus difficile à atténuer.
    - Une atténuation complète doit examiner les paquets non chiffrés. Une certaine atténuation peut se produire avec des paquets cryptés seulement.
    - Les paquets ne peuvent généralement pas être usurpés.
    - Attaques du service des noms de domaine (DNS)
        - Le DNS est l'un des deux services critiques de l'Internet, sans lequel presque toutes les applications Internet échouent (courrier, web, etc.). Le DNS est la page blanche de l'Internet.
        - Au lieu d'attaquer directement la victime, les attaquants s'en prennent aux services DNS du fournisseur d'accès Internet de la victime, ce qui interrompt le trafic de la victime.
        - L'attaque n'affecte pas seulement le trafic de la victime, mais peut aussi toucher de nombreux autres clients du FAI, même s'ils ne sont pas la cible de l'attaque.

- Attaques par épuisement de l'état
    - Les dispositifs qui conservent l'état des connexions tels que les serveurs, les pare-feu et les systèmes de détection/prévention des intrusions qui ont des capacités d'état limitées.
- Attaques du plan de contrôle
    - Les protocoles de routage tels que BGP (Border Gateway Protocol) et OSPF (Open Shortest Path First).

Le groupe de travail a utilisé les types d'attaques ci-dessus pour identifier les meilleures pratiques d'atténuation des attaques DDoS basées sur les serveurs et a discuté des outils et techniques d'atténuation généraux pour ces attaques afin de former un cadre pour les recommandations du groupe de travail.

2.1 Structure du CSRIC IV

Conseil de la sécurité, de la fiabilité et de l'interopérabilité des communications (CSRIC) IV									
Comité directeur du CSRIC									
Président ou Co-présidents : Travail Groupe 1	Président ou Co-présidents : Travail Groupe 2	Président ou Co-Présidents : Travail Groupe 3	Président ou co-président Présidents : Travail Groupe 4	Président ou Co-Présidents : Travail Groupe 5	Président ou co-président Présidents : Travail Groupe 6	Président ou Co-Présidents : Travail Groupe 7	Président ou Co-présidents : Travail Groupe 8	Président ou co-président Présidents : Travail Groupe 9	Président ou Co-Présidents : Travail Groupe 10
Travail Groupe 1 : Suivant Génération 911	Travail Groupe 2 : Sans fil Urgence Alertes	Travail Groupe 3 : EAS	Travail Groupe 4 : Cybersécurité Meilleures pratiques	Travail Groupe 5 : Serveur- Basé sur DDoS Attaques	Travail Groupe 6 : Long terme Internet de base Protocole Améliorations	Travail Groupe 7 : Héritage Best Pratique Mises à jour	Travail Groupe 8 : Sous-marin Câble Atterrissage Sites	Travail Groupe 9 : Infrastructure Partager Pendant Urgences	Travail Groupe 10 : CPE Alimentation du site

Tableau 1 - Structure du groupe de travail CSRIC IV.

2.2 Membres de l'équipe du groupe de travail 5

Le groupe de travail 5 est composé des membres énumérés ci-dessous.

Nom	Entreprise
Peter Fonash (coprésident)	DHS
Michael Glenn (coprésident)	CenturyLink
Paul Diamond (co-rédacteur en chef)	CenturyLink
Robert Thornberry (co-rédacteur en chef)	Bell Labs, Alcatel-Lucent
Vernon Mosley (liaison avec la FCC)	FCC
Jared Allison	Verizon
Don Blumenthal	Registre d'intérêt public
Chris Boyer	AT&T
Matt Carothers	Cox Communications
Roy Cormier	Nsight
Dave DeCoster	Shadowserver
John Denning	FSSCC
Roland Dobbins	Réseaux Arbor
Martin Dolly	ATIS
David Fernandez	Technologies Prolexic
Mark Ghassemzadeh	ACS
Darren Grabowski	NTT
Sam Grosby	Wells Fargo
Rodney Joffe	Neustar
John Levine	CAUCE
Gregory Lucak	Windstream
John Marinho	CTIA
Dan Massey	IEEE
Ron Mathis	Intrado
Bill McInnis	Identité sur Internet
Chris Morrow	Google
Michael O'Reirdan	MAAWG
Eric Osterweil	VeriSign, Inc.
Wayne Pacine	Conseil des gouverneurs de la Réserve fédérale
Glen Pirrotta	Comcast

R.H. Powell	Akamai
Nick Rascona	Sprint
Chris Roosenraad	Time Warner Cable
Craig Spiezle	Alliance pour la confiance en ligne
Joe St Sauver	Université de l'Oregon/Internet2
Kevin Sullivan	Microsoft
Bernie Thomas	CSG International
Matt Tooley	NCTA
Errol Weiss	FSSCC
Pam Witmer	Commission des services publics de PA

Tableau 2 - Liste des membres du groupe de travail 5.

3 Objectif, portée et méthodologie

3.1 Objectif

Ce groupe de travail a été chargé d'examiner et de faire des recommandations au Conseil concernant les meilleures pratiques au niveau du réseau et d'autres mesures visant à atténuer les effets des attaques DDoS provenant de grands centres de données et de sites d'hébergement. L'objectif du groupe de travail était d'organiser un groupe de travail avec un large éventail d'expérience et d'expertise, et d'inclure des participants du gouvernement et de l'industrie. Les 5 objectifs du groupe de travail11 sont les suivants :

Objectifs du GT5

Description :

Les secteurs des infrastructures critiques, y compris le secteur financier, ont été attaqués par un barrage d'attaques DDoS émanant de centres de données et de fournisseurs d'hébergement. Ce groupe de travail examinera et fera des recommandations au Conseil concernant les meilleures pratiques au niveau du réseau et d'autres mesures visant à atténuer les effets des attaques DDoS provenant de grands centres de données et de sites d'hébergement. Ces recommandations devraient inclure des méthodes et procédures techniques et opérationnelles pour faciliter la mise en œuvre par les parties prenantes de la ou des solutions recommandées.

Livrable :

Mesures recommandées que les fournisseurs de communications peuvent prendre pour atténuer l'incidence et l'impact des attaques DDoS provenant des centres de données et des fournisseurs d'hébergement, en particulier celles qui visent les systèmes d'information des secteurs critiques.

CSRIC

2

3.2 Portée

Depuis plusieurs années, on assiste à une augmentation rapide du volume, de la taille et de la portée des attaques DDoS, ce qui pose des problèmes aux fournisseurs d'accès à Internet en raison de l'augmentation du volume observé dans les domaines suivants

11 http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC_IV_Working_Group_Descriptions_5_7_14.pdf

leurs réseaux. Les attaques récentes se sont appuyées sur des locataires infectés au sein de grands centres d'hébergement de données. Afin d'aborder le problème des attaques DDoS basées sur les serveurs, le groupe de travail 5 a utilisé une approche holistique (par exemple, plusieurs parties prenantes représentées dans l'ensemble de l'écosystème) en se concentrant sur les actions que les opérateurs de réseau pourraient prendre pour prévenir et atténuer les attaques DDoS. L'approche holistique était nécessaire car, pour être efficace, les causes et les conséquences des attaques DDoS doivent être traitées par l'ensemble de l'écosystème des réseaux et de l'hébergement. La lutte contre ce vecteur d'attaque est devenue une priorité pour toutes les parties prenantes de l'écosystème.

L'approche du groupe de travail 5 était d'être aussi inclusive que possible sans répéter ou dupliquer les efforts entrepris par d'autres groupes traitant d'autres aspects du problème des attaques DDoS basées sur les serveurs. De plus, l'approche du groupe de travail 5 était de se concentrer sur les efforts qui résulteraient en des actions recommandées spécifiquement pour les attaques DDoS basées sur les serveurs, c'est-à-dire que de nombreuses meilleures pratiques examinées ont été reconnues comme étant valables, étaient de bonnes meilleures pratiques *en général*, mais n'étaient pas spécifiques aux attaques DDoS basées sur les serveurs et n'ont donc pas été incluses dans la portée de la tâche du groupe de travail 5. Une exception a été faite pour les recommandations visant à protéger contre les attaques par déni de service du système de nom de domaine (DNS). Les attaques DNS récentes et répétées ont été particulièrement flagrantes, et les meilleures pratiques d'atténuation ont donc été incluses dans les travaux du groupe de travail 5. [13]

3.3 Méthodologie

Le groupe de travail 5 a commencé par identifier des sous-groupes afin de se concentrer de manière appropriée sur des études de cas d'attaques DDoS basées sur des serveurs et sur l'analyse des meilleures pratiques de l'industrie. Les quatre sous-groupes suivants en sont issus : ISP, communauté financière, experts en sécurité Internet et sous-groupes des meilleures pratiques.

Le sous-groupe sur les meilleures pratiques a identifié les BP applicables aux attaques DDoS basées sur les serveurs, tandis que les sous-groupes sur les FAI, la communauté financière et les experts en sécurité Internet ont élaboré des études de cas représentatives des attaques DDoS basées sur les serveurs. L'ensemble du groupe de travail 5 a ensuite associé les meilleures pratiques au niveau du réseau à chaque domaine des sous-groupes ainsi que d'autres mesures visant à atténuer les effets des attaques DDoS provenant de grands centres de données et de sites d'hébergement.

Le groupe de travail 5 a organisé des conférences téléphoniques bihebdomadaires avec les membres de son groupe de travail pour accomplir cette tâche. En outre, les sous-groupes ont tenu des conférences téléphoniques bihebdomadaires pour solliciter des contributions et examiner les livrables de leurs études de cas. Le groupe de travail 5 a tenu une réunion en face-à-face de deux jours en janvier 2014 (Arlington, Virginie), et en avril 2014 (Longmont, Colorado), et une réunion finale en face-à-face en juillet 2014 (Arlington, Virginie), afin de faciliter la discussion sur les livrables.

Le groupe de travail 5 a examiné environ 600 BP de cybersécurité pour déterminer si elles entraient ou non dans le champ d'application de la mission du groupe de travail (c'est-à-dire les BP visant à atténuer les attaques DDoS basées sur les serveurs). Le groupe de travail a réduit la liste applicable à environ 30 BP saillantes. Le groupe de travail a effectué une analyse des lacunes en utilisant les Six Phases de la préparation et de la réponse aux attaques DDoS en parallèle avec le cadre de cybersécurité du NIST. Sur la base de cette analyse, le groupe de travail a également rédigé plusieurs nouvelles BP en vue de leur adoption volontaire par les communications.

12 http://www.darkreading.com/attacks-and-breaches/bank-attackers-used-php-websites-as-launch-pads/d/d-id/1107833 ?

13 http://www.pcworld.com/article/2040766/possibly-related-ddos-attacks-cause-dns-hosting-pannes.html

l'industrie.

Le groupe de travail a également identifié les obstacles à la mise en œuvre des BP en se basant sur les expériences résumées dans les études de cas des sous-groupes, ainsi que sur l'expérience des membres, et a examiné les mesures d'efficacité basées sur les résultats qui démontrent si les efforts volontaires contre les attaques DDoS basées sur les serveurs ont un effet favorable ou non. Le groupe de travail a également appliqué la taxonomie des six phases (annexe A) comme guide pour identifier les meilleures pratiques candidates à la mise en œuvre.

Enfin, le groupe de travail a formulé des recommandations quant aux mesures que la FCC peut prendre pour contribuer à atténuer les effets des attaques DDoS en permettant une adoption plus large des meilleures pratiques recommandées en matière de DDoS sur serveur.

3.3 Métriques

Les mesures du succès contre les attaques DDoS basées sur les serveurs sont essentielles pour déterminer l'efficacité du respect des meilleures pratiques recommandées dans ce rapport. Les membres du groupe de travail 5 reconnaissent qu'un accord sur une approche cohérente et uniforme pour mesurer l'efficacité du respect des BP recommandées jettera les bases pour déterminer si des actions volontaires supplémentaires sont nécessaires dans l'ensemble de l'écosystème afin de traiter de manière holistique les attaques DDoS basées sur les serveurs.

Le groupe de travail 5 reconnaît également que des mesures efficaces peuvent être difficiles à mettre en place. Les opérateurs de réseau ont chacun des méthodes différentes pour faire face aux attaques DDoS. Pour établir des mesures communes de réussite, il faut que les participants adoptent une approche uniforme pour la collecte, l'interprétation, l'analyse et la communication des mesures des attaques DDoS. Afin de mesurer l'efficacité du respect des BP recommandées pour les attaques DDoS basées sur les serveurs, les paramètres doivent être soigneusement choisis pour mesurer le résultat souhaité de manière significative, mesurable et reproductible. L'analyse minutieuse des mesures agrégées dans l'écosystème et la déduction de l'efficacité de la mise en œuvre des BP recommandées nécessitent la participation et la coopération de toutes les parties prenantes de l'écosystème qui contribuent à la collecte, à l'analyse, à la communication et à l'interprétation des mesures.

Afin d'impliquer les participants de l'écosystème plus large dans la formation d'une approche uniforme pour mesurer l'efficacité de la mise en œuvre des BP recommandées, le groupe de travail 5 a établi un partenariat avec le groupe de travail 4 du CSRIC IV, les meilleures pratiques en matière de cybersécurité, afin de tirer parti de leurs plus de 100 membres, pour aborder de manière holistique les paramètres pour mesurer l'efficacité de la mise en œuvre des BP recommandées, non seulement pour les attaques DDoS basées sur le serveur, mais aussi pour les autres BP recommandées en matière de cybersécurité. Les membres du groupe de travail 5 assureront la liaison avec les membres du groupe de travail 4 pour mener à bien cet effort de mesure holistique qui sera inclus dans le livrable du groupe de travail 4 en mars 2015.

Dans le cadre des efforts du groupe de travail 4 sur les mesures, le groupe de travail 5 recommandera des mesures potentielles d'attaques DDoS basées sur les serveurs qui pourraient être considérées comme des cas d'essai à prendre en compte par les participants de l'écosystème. Ces mesures que les membres du groupe de travail 5 indiqueront au groupe de travail 4 seront importantes pour mesurer l'efficacité du respect des BP recommandées pour les attaques DDoS basées sur les serveurs dans l'ensemble de l'écosystème et sont des mesures d'essai conceptuellement tenables.

pour qu'un processus d'examen discipliné soit établi par le groupe de travail 4.

3.4 Obstacles à la participation

Les sections suivantes traitent des efforts du groupe de travail 5 concernant les obstacles à la participation des opérateurs de réseau à l'adoption des meilleures pratiques recommandées présentées dans ce document. Ces sections sont largement adaptées du Guide de participation au code des FAI du CSRIC III [14], car les obstacles identifiés dans le suivi du code de conduite anti-bot volontaire américain pour les FAI recommandé par le groupe de travail 7 du CSRIC III sont applicables aux obstacles que les opérateurs de réseau peuvent rencontrer dans le suivi des BP des attaques DDoS basées sur le serveur recommandées par le groupe de travail 5. Outre les exploitants de réseaux, les fournisseurs d'hébergement, dans la mesure où les BP recommandées s'appliquent, peuvent également rencontrer des obstacles similaires. Les travaux antérieurs accomplis par le CSRIC III ont fourni des définitions et un cadre appropriés pour l'approche des barrières du groupe de travail 5.

Bon nombre des meilleures pratiques recommandées dans ce rapport final impliquent des niveaux d'engagement et de complexité variables. Il est entendu que les participants du secteur privé sont en concurrence interne pour les capitaux d'investissement et les ressources humaines, et que les décisions de prioriser ces investissements dépendent de plus en plus de la présentation d'une solide analyse de rentabilité aux décideurs.

Le guide des obstacles est conçu pour encourager une participation plus large en fournissant un ensemble structuré de ressources liées à des recommandations spécifiques, y compris les meilleures orientations disponibles sur la mise en œuvre.

3.4.1 Obstacles à la participation : Considérations

L'adoption des meilleures pratiques peut poser des obstacles dans la mesure où les activités requises ont un impact sur les méthodes et procédures existantes et sur les ressources de plusieurs organisations. Les opérateurs de réseau devront comprendre non seulement quels changements peuvent être nécessaires, mais aussi quelles organisations seraient touchées du point de vue des processus, des ressources et du budget. Il faut tenir compte de l'évolutivité et des niveaux d'intégration interdépartementale, ainsi que de tout soutien continu nécessaire pour mettre en œuvre une recommandation. En abordant les obstacles, des efforts ont été faits pour classer chaque obstacle identifié dans l'une des catégories suivantes :

3.4.1.1 Obstacles technologiques

Les obstacles technologiques sont des obstacles pour lesquels les solutions techniques actuelles peuvent être insuffisantes pour faire face aux menaces ou lorsque ces solutions peuvent avoir d'autres effets secondaires inacceptables. L'importance des solutions technologiques en tant qu'obstacles dépend de la mesure dans laquelle la technologie est nécessaire pour mettre en œuvre une recommandation spécifique. Certaines solutions peuvent nécessiter un minimum de ressources techniques (actifs et personnes), tandis que d'autres peuvent être plus exigeantes, notamment en termes d'intégration des systèmes. La mise en œuvre d'une recommandation est également susceptible de dépendre de la situation actuelle au sein d'un opérateur de réseau, notamment des capacités, ressources et priorités internes ou de l'accès à des ressources tierces. Les obstacles technologiques peuvent se traduire directement par des

14 http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%20201 3.pdf

obstacles. Une solution technique peut exister mais le coût de sa mise en œuvre chez l'opérateur de réseau peut être prohibitif.

3.4.1.2 Obstacles liés à la clientèle/au marché

Les obstacles liés aux clients ou au marché sont des obstacles qui découlent de la mise en œuvre de solutions qui peuvent être considérées par les clients comme inefficaces (par exemple, les clients choisissent de ne pas participer) ou indésirables (par exemple, la confidentialité, les conditions restrictives). Les activités des opérateurs de réseau peuvent également avoir des conséquences sur le marché en augmentant les coûts de leurs produits, le montant des investissements en capital qu'un opérateur de réseau est prêt à faire, la volonté des clients d'acheter la solution et d'autres considérations par rapport aux produits concurrents. La mise en œuvre de certaines bonnes pratiques proposées en tant que services de sécurité gérés sera une décision commerciale de l'opérateur de réseau. Il devra décider s'il souhaite offrir ces services et, le cas échéant, s'il souhaite les mettre en œuvre en interne ou par l'intermédiaire d'un tiers. Enfin, il devra décider de la portée, des caractéristiques, de la capacité et du prix de l'offre de services de sécurité gérés qui correspond le mieux au marché sur lequel il est en concurrence.

3.4.1.3 Obstacles opérationnels

Les obstacles opérationnels sont des obstacles qui pourraient avoir un impact inacceptable sur la mission et les ressources principales d'une organisation. Les organisations qui ont des responsabilités opérationnelles sont généralement tenues responsables par des mesures de performance bien définies. (par exemple, le temps moyen de transaction pour les représentants du service clientèle). Toute nouvelle pratique opérationnelle doit être mise en œuvre avec suffisamment d'attention pour :

- le développement et la mise à jour des méthodes et procédures opérationnelles ;
- la réaffectation de ressources existantes ou supplémentaires ;
- l'évolutivité des solutions ;
- les objectifs de performance opérationnelle, les facteurs critiques de réussite et la capacité à mesurer les résultats.

3.4.1.4 Obstacles financiers

Les obstacles financiers résultent de l'incapacité à quantifier les coûts ou les avantages liés à la mise en œuvre de recommandations spécifiques. Dans l'environnement économique actuel, l'absence d'une analyse de rentabilité spécifique à l'entreprise peut constituer un obstacle important à l'adoption. Les entreprises du secteur privé ont la responsabilité fiduciaire de prendre des décisions fondées sur une allocation prudente du capital. Lorsqu'il s'agit de déployer des investissements dans les technologies liées à la sécurité, la plupart des entreprises s'appuient sur des données quantifiables pour hiérarchiser et allouer les nouveaux investissements dans les systèmes, les processus et les ressources humaines.

3.4.1.5 Obstacles juridiques et politiques

Les lois qui découragent la collaboration et le partage d'informations entre les opérateurs de réseau, que ce soit aux États-Unis ou à l'étranger, peuvent servir de couverture aux acteurs malveillants. [15] Les acteurs malveillants ont la capacité de

[15] *Voir id.*

déguiser les botnets en trafic légitime, ce qui place les professionnels de la sécurité dans la position intenable de s'immiscer dans la vie privée d'un utilisateur final ou de permettre une activité criminelle dangereuse et coûteuse. En outre, les opérateurs de réseau ne sont pas toujours en mesure d'arrêter le trafic même s'il est reconnu comme malveillant. Par exemple, le trafic peut être mêlé à une activité commerciale, de sorte que le coût de l'atténuation serait supérieur au préjudice causé par le botnet. Les opérateurs de réseaux sont confrontés à un équilibre permanent entre la protection de leurs clients, la protection de la vie privée de ces derniers et le respect de l'autonomie attendue par les autres opérateurs de réseaux.

3.4.1.6 **Obstacles - Attaques DDoS basées sur le serveur**

Les attaques DDoS provenant des centres de données et des fournisseurs d'hébergement sont particulièrement problématiques en raison de la bande passante et des ressources informatiques élevées dont dispose un attaquant. Cela rend la prévention, la détection et l'atténuation plus importantes, mais aussi plus difficiles. Les attaques DDoS basées sur les serveurs nécessitent l'implication de l'écosystème, même à un degré plus élevé que d'autres types d'attaques. Ces aspects des attaques DDoS basées sur les serveurs entraînent des obstacles particuliers à la lutte contre ces attaques. Le présent rapport propose plusieurs nouvelles meilleures pratiques pour traiter ces aspects, ainsi que des meilleures pratiques existantes et actualisées. De manière générale, voici des déclarations sur les considérations particulières aux attaques DDoS basées sur les serveurs :

3.4.1.6.1 Considérations technologiques :

Certaines des meilleures pratiques identifiées dans ce document sont difficiles ou impossibles à mettre en œuvre sans impact dans certains réseaux, selon l'architecture du réseau. Certaines des meilleures pratiques décrites dans ce document dépendent en partie de la technologie disponible dans certaines plateformes de périphériques réseau, mais pas dans d'autres.

3.4.1.6.2 Considérations relatives au client/marché :

Certaines meilleures pratiques, bien que très efficaces, sont des services supplémentaires que les clients doivent acheter et configurer. Les contrôles d'atténuation des attaques peuvent très bien interférer avec le trafic légitime, ce qui peut être jugé inacceptable par un client.

3.4.1.6.3 Considérations opérationnelles :

Si de nombreuses bonnes pratiques ne sont pas difficiles à mettre en œuvre en soi, leur mise en œuvre à l'échelle de milliers de clients introduit une complexité importante en termes de gestion de la configuration et de systèmes de back-office. Certaines techniques d'atténuation pourraient causer des dommages collatéraux à d'autres clients dans le même centre de données, ce qui pourrait être jugé inacceptable par les opérateurs de centres de données. Bon nombre des recommandations de changements opérationnels nécessitent une coordination entre les opérateurs de réseau et leurs clients pour éviter les pannes. Il s'agit d'un investissement en temps important qui peut également entraîner des problèmes de fidélisation des clients si ces derniers ne bénéficient pas directement de la mise en œuvre.

3.4.1.6.4 Considérations juridiques/réglementaires/politiques :

[16] *Voir généralement*, Can We Beat Legitimate Cyber Behavior Mimicking Attacks from Botnets, IEEE (2012).

Le partage de données entre fournisseurs peut être plus difficile dans certains pays où les lois locales sur la protection de la vie privée sont strictes. Des problèmes de responsabilité peuvent également se poser en cas de partage de données inexactes lors d'une attaque.

3.4.1.6.5 Considérations financières :

Un grand nombre des meilleures pratiques présentées dans ce document dépendent de capacités spécifiques et d'ensembles de fonctionnalités qui ne sont pas omniprésentes parmi les routeurs. Leur mise en œuvre peut nécessiter l'achat de nouveaux équipements par les opérateurs de réseau, les fournisseurs d'hébergement ou les clients.
La mise en œuvre de certaines des meilleures pratiques identifiées peut avoir un impact sur les performances des équipements de réseau ou des serveurs. Cela peut à son tour nécessiter des appareils plus puissants ou plus nombreux, rendant les services plus coûteux pour tous les clients.

4 Contexte

Les CSRIC précédents ont recommandé des meilleures pratiques qui pourraient être utilisées pour atténuer les attaques DoS et DDoS. Le CSRIC II a approuvé les recommandations du groupe de travail 8 dans son rapport final intitulé *ISP Network Protection Practices:*[17]

- Meilleures pratiques recommandées dans les domaines de la prévention, de la détection, de la notification, de l'atténuation et de la protection de la vie privée.
- Se sont concentrés sur les BP pour les ISP qui fournissent des services aux consommateurs sur des réseaux résidentiels à large bande, mais ont noté que beaucoup des meilleures pratiques identifiées dans le rapport seraient également des pratiques précieuses à appliquer dans des contextes de réseaux non résidentiels et non destinés aux consommateurs.
- Il est également recommandé que, à une date ultérieure, la FCC examine si un travail supplémentaire sur les meilleures pratiques serait utile dans le contexte non résidentiel.

Le CSRIC II a également approuvé les recommandations du groupe de travail 2A dans leur rapport final sur *les meilleures pratiques en matière de sécurité cybernétique:*[18]

- Mise à jour des meilleures pratiques en matière de cybersécurité reflétant l'environnement technologique actuel dans le secteur des communications, et références connexes :
  - Analyser les meilleures pratiques existantes en matière de cybersécurité (NRIC, NIST, SANS, IEEE, etc.).
  - recommander des modifications et des suppressions de ces meilleures pratiques existantes.
  - Identifier les nouvelles meilleures pratiques en matière de cybersécurité pour les technologies existantes et relativement nouvelles dans le secteur de la communication.

Le CSRIC III a approuvé les recommandations du groupe de travail 7 dans son rapport final intitulé *U.S. Anti-Bot Code of Conduct for ISPs (ABCs for ISPs):*[19]

- L'accent est mis sur la menace des réseaux de zombies provenant des dispositifs résidentiels à large bande.
- Actions volontaires recommandées par la PSI dans les domaines de l'éducation, de la détection, de la notification, de la remédiation et de la collaboration.

17 http://www.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf
18 http://www.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf
19 http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf

- a en outre recommandé que la FCC, en partenariat avec d'autres agences gouvernementales fédérales et l'industrie, facilite la création d'études de cas sur les activités d'atténuation des botnets.

Le CSRIC III a approuvé les recommandations du groupe de travail 4 de leur rapport final *DNS Best Practices:*[20]

- Se concentre sur les meilleures pratiques pour sécuriser le DNS et le système de routage pour l'Internet pendant la période précédant la mise en œuvre du DNSSEC.

Le CSRIC III a également approuvé les recommandations du groupe de travail 5 de leur rapport final sur les *pratiques de mise en œuvre des DNSSEC pour les ISP:*[21]

- Examiner les meilleures pratiques pour le déploiement et la gestion des extensions de sécurité des systèmes de noms de domaine (DNSSEC) par les fournisseurs de services Internet (ISP).
- Recommander des métriques et des mesures appropriées qui permettent d'évaluer l'efficacité du déploiement des DNSSEC par les FAI.

Les récentes attaques DDoS ont exploité les vulnérabilités des sociétés d'hébergement web et d'autres grands centres de données pour lancer des attaques DDoS sur les systèmes informatiques et les sites web. Le CSRIC IV a reconnu que le travail dans ce domaine est à la fois opportun et important afin d'avoir un impact sur ces dernières menaces DDoS. Sur la base des progrès réalisés dans les CSRIC précédents axés sur les réseaux résidentiels, le groupe de travail 5 du CSRIC IV a été chargé de recommander des mesures que les fournisseurs de communications peuvent prendre pour atténuer l'incidence et l'impact des attaques DDoS provenant des centres de données et des fournisseurs d'hébergement, en particulier celles qui visent les systèmes d'information des secteurs d'infrastructures critiques.

5Analyse, constatations et conclusions

5.1 Analyse

Les études de cas ont porté sur un certain nombre d'attaques DDoS basées sur des serveurs. Une attaque peut impliquer plusieurs FAI et plusieurs centres de données et d'hébergement.

- Anatomie d'une attaque DDoS basée sur un serveur

Comme le montre la figure 3, un attaquant peut prendre le contrôle d'un centre de données et de serveurs d'hébergement et tirer parti des ressources de calcul et de réseau considérables pour lancer une attaque DDoS sur une entreprise victime. Il convient de noter que la cible peut également faire partie de l'infrastructure des FAI. Cette attaque submerge l'accès à la cible, empêchant les utilisateurs légitimes d'y accéder et causant des problèmes de sécurité.

---

20 http://www.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.p df

21 http://www.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG5_Report_March_%202013.p df

22 http://www.darkreading.com/attacks-and-breaches/bank-attackers-used-php-websites-as-launch-pads/d/d-id/1107833 ?

des dommages collatéraux en affectant d'autres parties le long du chemin du trafic DDoS. L'atténuation de ce type d'attaque nécessite l'intervention de toutes les parties concernées :

- Plusieurs FAI
- Fournisseurs d'hébergement / Centres de données / Revendeurs
- Infrastructure cible
- Infrastructure du FAI de l'attaquant d'origine

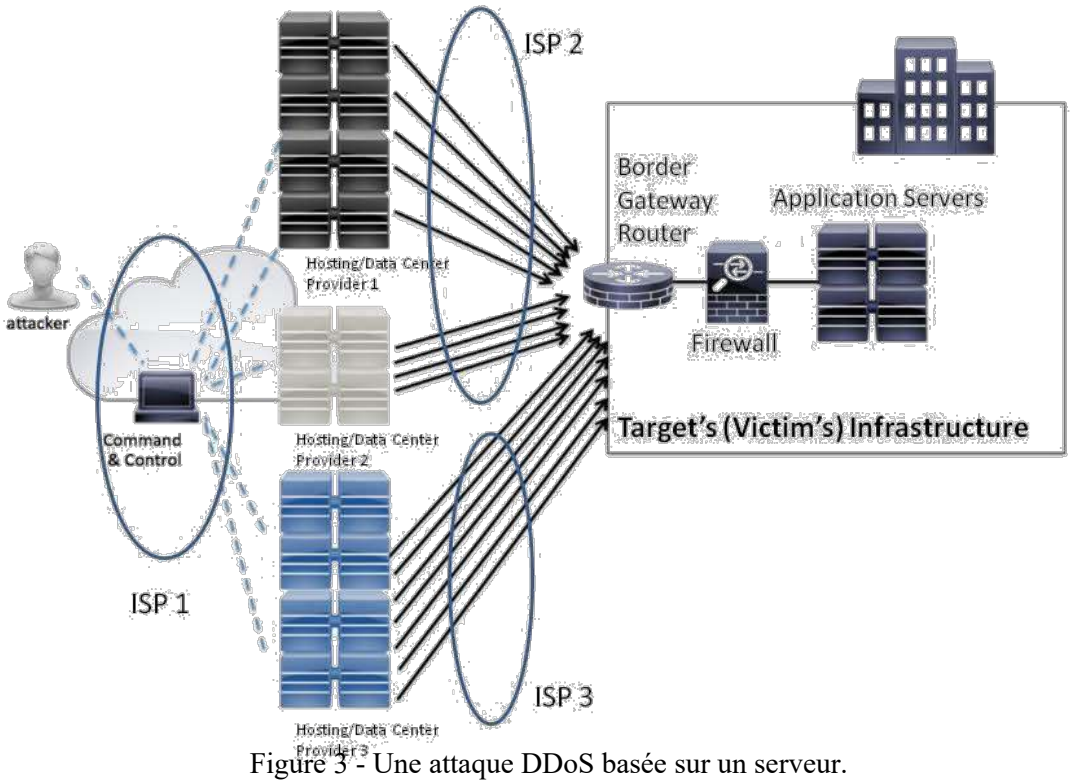


Figure 3 - Une attaque DDoS basée sur un serveur.

Source :
http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html#_Toc374453043

- Taxonomie des attaques - Une taxonomie des types d'attaques DDoS basées sur les serveurs a été créée afin de déterminer l'étendue des défenses qui seraient nécessaires pour atténuer les attaques. La taxonomie des attaques figure à l'annexe C.

- Études de cas
  - Le groupe de travail 5 a identifié trois sous-groupes chargés de se concentrer sur les études de cas d'attaques DDoS basées sur les serveurs des parties prenantes et un quatrième sous-groupe chargé de réaliser une analyse des meilleures pratiques de l'industrie. Ces sous-groupes étaient les suivants ISPs, Financiers

Les sous-groupes Communauté, Experts en sécurité Internet et Meilleures pratiques.
- Le sous-groupe des meilleures pratiques a identifié les BP applicables aux attaques DDoS basées sur les serveurs, tandis que les sous-groupes des FAI, des financiers et des experts en sécurité Internet ont élaboré des études de cas représentatives des attaques DDoS basées sur les serveurs. Ces études de cas figurent à l'annexe D.

- Meilleures pratiques recommandées
  - Les meilleures pratiques sont incluses dans l'annexe E

5.2 Constatations

Principales conclusions des études de cas :

1. Les attaques DDoS deviennent suffisamment importantes pour dépasser la capacité d'absorption d'un seul FAI.
2. Les attaques basées sur les serveurs exploitent les ressources informatiques et de réseau des centres de données pour organiser des attaques DDoS d'un volume sans précédent.
3. En raison de l'augmentation du volume des attaques DDoS, les dommages collatéraux (impacts sur d'autres personnes non ciblées par l'attaque DDoS) sont courants - perte de paquets, retards, latence élevée pour le trafic Internet des parties non impliquées dont le trafic traverse simplement les réseaux saturés par ces attaques.
4. Les attaques DDoS sont utilisées non seulement pour perturber les services, mais aussi pour détourner les ressources de sécurité pendant que d'autres attaques sont tentées, par exemple des transactions frauduleuses.
5. Les attaques DDoS adaptatives sont très répandues. Les attaquants modifient le trafic d'attaque à la volée pour éviter d'être identifiés et pour défier et confondre les stratégies d'atténuation.
6. Les attaques par réflexion et par amplification sont encore courantes. Elles tirent parti d'une mauvaise configuration du DNS, du NTP et d'autres ressources du réseau, avec la possibilité d'usurper (falsifier) les adresses IP sources (cibles).
7. L'architecture des réseaux de zombies est de plus en plus sophistiquée et difficile à retracer. Les systèmes de commande et de contrôle (^{C2}) sont de plus en plus hiérarchisés et utilisent des serveurs proxy et des réseaux peer to peer pour masquer l'emplacement du système qui exécute les commandes. En outre, certains réseaux de zombies ont la capacité d'endommager un système compromis après avoir mené à bien une attaque.
8. Les dispositifs sont de plus en plus dispersés dans le monde entier, ce qui rend la coordination de la mise hors service de ces systèmes difficile, car les pays ont souvent des lois différentes et parfois contradictoires.
9. Le trafic DDoS se développe rapidement, de sorte que des capacités d'atténuation automatisées sont nécessaires pour protéger l'infrastructure.
10. Afin de soutenir les capacités d'atténuation automatisées, il convient de suivre une taxonomie normalisée pour exprimer les informations nécessaires à l'atténuation des attaques DDoS basées sur les serveurs.
11. Les technologies anti-spoofing (anti-forging) doivent être plus largement déployées pour se protéger des attaques par amplification.
12. La capacité d'atténuation des attaques DDoS doit être déployée sur l'ensemble du réseau, car il est difficile de prévoir d'où viendra l'attaque.
13. L'atténuation des DDoS nécessite de multiples outils. Les FAI ont besoin d'une capacité de filtrage des trous noirs de destination pour protéger leurs réseaux, sachant que le filtrage des trous noirs complète le processus d'atténuation des DDoS.

attaque DDoS à la cible. Les atténuateurs d'attaques ont besoin de plusieurs types de capacités moins intrusives pour minimiser l'efficacité des attaques DDoS.

14. Les attaques DDoS doivent être traitées par l'ensemble de l'écosystème des réseaux, et pas seulement par les opérateurs de réseaux. Cela inclut les fournisseurs de centres d'hébergement et de centres de données, les cibles des attaques DDoS, les fournisseurs de logiciels, les organisations open source, ainsi que les fabricants d'équipements (toute la chaîne d'approvisionnement).
15. L'atténuation des attaques DDoS nécessite une coopération étroite entre les cibles, les fournisseurs d'hébergement et les opérateurs de réseau. À mesure que les nouvelles techniques d'atténuation des DDoS deviennent plus efficaces, les attaquants continueront d'adapter leurs techniques pour trouver de nouveaux moyens d'attaquer leurs cibles.
16. L'élaboration de mesures de réussite potentielles pour déterminer l'efficacité du respect des meilleures pratiques volontaires en matière d'attaques DDoS basées sur les serveurs doit être abordée non seulement par les opérateurs de réseau, mais aussi par les parties prenantes de l'écosystème Internet au sens large, afin de fournir des interprétations significatives et holistiques de l'efficacité.

5.3 Conclusions

Dans ce rapport final, le groupe de travail 5 a documenté ses conclusions, formulé des recommandations, suggéré des meilleures pratiques pour faire face aux attaques DDoS basées sur les serveurs, abordé les obstacles à la mise en œuvre et suggéré une voie à suivre pour aborder de manière holistique les mesures d'efficacité pour suivre les BP recommandées. Nous concluons dans ce rapport final que des mesures devront être prises, non seulement par les opérateurs de réseau, mais par l'ensemble de l'écosystème des parties prenantes touchées par les attaques DDoS basées sur les serveurs, afin de prévenir, détecter et atténuer les attaques.

6 Recommandations

1- La FCC encourage les FAI à envisager la mise en œuvre volontaire, selon un ordre de priorité, des meilleures pratiques recommandées et des nouvelles recommandations (annexe E) pour faire face aux attaques DDoS basées sur les serveurs, en faisant la promotion de la sensibilisation et des avantages de ces meilleures pratiques.

2- La FCC encourage le développement de meilleures pratiques pour les fournisseurs d'hébergement afin de promouvoir des pratiques informatiques sûres, de réduire les vulnérabilités et de réduire la menace d'exploitation des vulnérabilités, réduisant ainsi l'incidence des attaques DDoS basées sur les serveurs.

3- La FCC encourage les relations volontaires du secteur privé, dans la mesure où elles n'existent pas déjà, entre pairs pour collaborer sur les meilleures pratiques de réponse aux DDoS et le soutien à l'atténuation.

4- La FCC encourage le développement d'un centre d'échange volontaire d'informations sur l'atténuation des attaques DDoS au sein de la structure existante de partage d'informations du DHS, qui peut être une ressource pour les FAI, les fournisseurs d'hébergement, les cibles, les organisations d'intervention (CERTS et ISAC) et les gouvernements pour atténuer les attaques DDoS en temps réel.

5- La FCC encourage les acteurs de l'écosystème à partager les informations relatives aux attaques DDoS basées sur les serveurs entre eux ou par le biais d'un centre d'échange centralisé utilisant une taxonomie normalisée, telle que la Structured Threat Information eXpression (STIX)[23] ou une construction similaire, afin de contribuer à l'atténuation automatisée des attaques.

6- La FCC encourage le partage des meilleures pratiques en matière d'atténuation des DDoS, des menaces et des vulnérabilités, et les actions de réponse aux incidents parmi les opérateurs de réseau dans le Comm-ISAC.

23 https://stix.mitre.org/

7 Remerciements

Ce rapport final reflète les contributions inestimables de tous les membres du groupe de travail. Les coprésidents du groupe de travail 5, Michael Glenn de CenturyLink et Peter Fonash du DHS, tiennent à exprimer leur reconnaissance à tous les membres du groupe de travail 5 pour leur travail acharné, leur temps et leurs efforts considérables qui ont abouti à ce rapport final. Les coprésidents tiennent à souligner les efforts inlassables des rédacteurs, Paul Diamond de CenturyLink et Robert Thornberry de Bell Labs, Alcatel Lucent, pour leur dévouement exceptionnel dans l'élaboration des rapports provisoire et final. Les coprésidents tiennent également à remercier les personnes suivantes qui ont dirigé les efforts des importants sous-groupes :

- FAI - Jared Allison de Verizon et Chris Boyer de AT&T
- Finances - John Denning de la Bank of America et Errol Weiss du Conseil de coordination du secteur des services financiers (CCSSF)
- Internet - Roland Dobbins de Arbor Networks
- Meilleures pratiques - Robert Thornberry des Bell Labs, Alcatel-Lucent

Les coprésidents souhaitent remercier Vernon Mosley de la Federal Communications Commission pour les efforts considérables qu'il a déployés afin de faciliter la production du rapport. Les coprésidents souhaitent également remercier les hôtes des réunions en face à face, CenturyLink et Intrado. Enfin, les coprésidents tiennent à remercier John Levine, de CAUCE, pour la création et la maintenance du wiki et du serveur de liste du GT5.

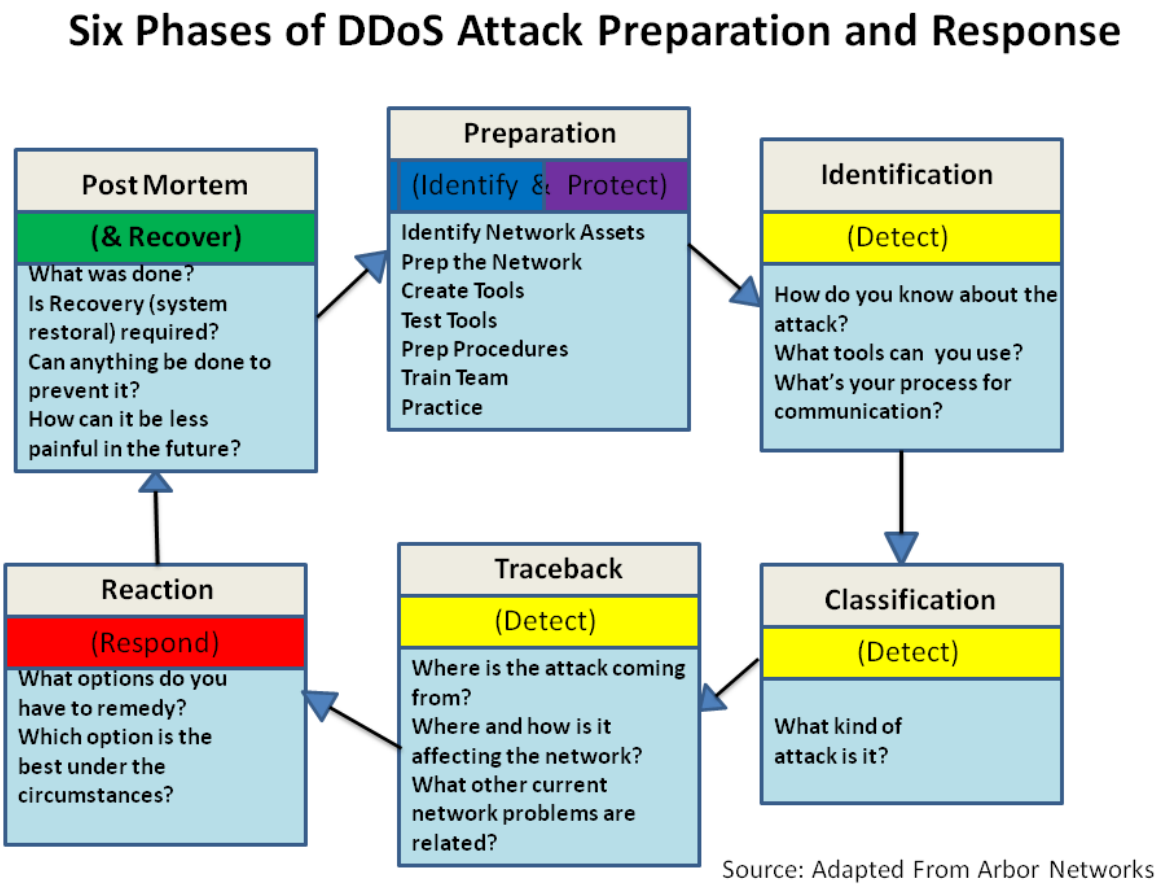
Les membres du groupe de travail 5 tiennent à souligner le leadership exceptionnel des coprésidents, Michael Glenn et Peter Fonash, qui ont permis au groupe de travail de rester concentré et de créer un environnement d'équipe très performant pour contribuer aux recommandations sur l'atténuation des attaques DDoS basées sur les serveurs.

8 Annexes

Annexe A : Taxonomie des six phases de préparation et de réponse aux attaques DDoS
Annexe B : Glossaire des DDoS basés sur les serveurs
Annexe C : Taxonomie des attaques DDoS
Annexe D : Études de cas sur l'atténuation des attaques DDoS
Annexe E : Meilleures pratiques en matière d'atténuation des DDoS sur les serveurs

Annexe A : Taxonomie des six phases de préparation et de réponse aux attaques DDoS

.



Préparation

- Communication
  - ISP et Pure Play DDoS Société d'atténuation (PP)
    - ISP/PP à ISP/PP
    - ISP/PP vers l'hébergement
    - ISP/PP à la victime
    - ISP/PP à la coordination centrale
    - Centre
  - Hébergement
    - Hébergement vers un ISP
    - D'hébergement à hébergement
    - Accueil de la victime
    - Hébergement vers la coordination centrale
    - Centre
  - Cible
    - De la victime à l'ISP
    - De la victime à l'hôte
    - De victime à victime
    - Cible de la coordination centrale
    - Centre
- Suivi et visibilité
  - ISP
    - Netflow
    - Niveaux de trafic
    - Niveaux de ressources de l'infrastructure du serveur
    - Détournement d'itinéraire
    - Journaux des FW, routeurs et serveurs
  - Hébergement
    - Netflow
    - Niveaux de trafic
    - Niveaux de ressources de l'infrastructure du serveur
    - Signalisation des attaques des ISP
    - Journaux des FW, routeurs et serveurs
  - Cible
    - Niveaux de ressources de l'infrastructure du serveur
    - Signalisation des attaques des ISP
    - Journaux des FW, routeurs et serveurs

Prévention		
	ISP	
		Techniques anti-spoofing Réduire les surfaces réfléchissantes Limites de débit / Blocage du trafic
	Hébergement	
		Techniques anti-spoofing Réduire les surfaces réfléchissantes Limites de débit / Blocage du trafic Plan de minimisation des ressources du serveur et procédures
	Cible	
		Plan de minimisation des ressources du serveur et procédures
Déployer et configurer Outils d'atténuation		
	ISP et Pure Play DDoS Société d'atténuation Filtrage	
		Filtrage CDN (attaques du trafic Web) BGP Flowspec Black Hole Filtering (Source et Destination) Nettoyage des données du réseau
	Filtrage de l'hébergement	
		Nettoyage des données sur site
	Filtrage des cibles	
		Nettoyage des données sur site

Capacité et ressources		
	ISP	
		Serveur DNS Capacité du réseau DNS Lien, routeur et état BGP Protection
	Hébergement	
		Serveur DNS Capacité du réseau DNS Lien, routeur et état BGP Protection Largeur de bande des liaisons montantes du centre de données FWs, IDS/IPS, capacités des commutateurs
	Cible	
		Liaisons montantes pour serveurs et réseaux FWs, IDS/IPS, capacités des commutateurs Capacités des ressources du serveur
Minimiser le service d'attaque		
	ISP	
		Fermer Ouvrir Résolveurs DNS Limitation du débit des requêtes DNS Limitation du débit des protocoles ouverts (NTP, Echo, etc) Désactiver les protocoles inutiles sur infrastructure du réseau
	Hébergement	
		Fermer Ouvrir Résolveurs DNS Limitation du débit des requêtes DNS Limitation du débit des protocoles ouverts (NTP, Echo, etc) Désactiver les protocoles inutiles sur infrastructure du réseau Désactiver les protocoles inutiles sur serveur et infrastructure virtuelle
	Cible	

Désactiver les protocoles inutiles sur serveur et infrastructure virtuelle

Peering et Upstream
Coopérative ISP
accords d'atténuation

Formel et informel
accords d'atténuation
Identification de 24/7
contacts opérationnels à
pairs ou des FAI en amont pour
atténuation des attaques
assistance

Identification

Suivi et visibilité

ISP

- Netflow (avec routeur et interface information)
- Niveaux de trafic
- Infrastructure du serveur
- Détournement d'itinéraire
- Journaux des FW, routeurs et serveurs
- Capture et analyse complètes des paquets

Hébergement

- Netflow (avec routeur et interface information)
- Niveaux de trafic
- Charges du système
- Signalisation des attaques des ISP
- Journaux des FW, routeurs et serveurs
- Capture et analyse complètes des paquets

Cible

- Charges du système
- Signalisation des attaques des ISP
- Journaux des FW, routeurs et serveurs
- Capture et analyse complètes des paquets

Confirmer avec la cible (client) que le le trafic est une véritable attaque trafic.

Classification

Type d'attaque

Attaque volumétrique ?

- Envoi direct de paquets
- Réflexion/Amplification

Attaque de la couche d'application ?
État ou ressource
Attaque d'épuisement ?

Attaque de l'avion de contrôle ?

Attaque spécifique Ipv6 ?

Traceback

Identification de la source
IPs

Identification de l'entrée
interfaces de routeur

Identification des DDoS
Chemins de paquets

Charges de trafic intermédiaires

Identification de la réflexion
Surface (routeurs, serveurs, etc)

Identification du routeur d'entrée
Interfaces pour les réflecteurs
usurpés
paquets

Réaction

Déterminer le meilleur outil ou ensemble d'outils pour atténuer les attaque

Analyser le trafic résiduel va à la cible de la mise au point des filtres d'atténuation et l'évolution du trafic d'attaque et méthodes

Surveillance des méthodes de filtrage pour minimiser les faux positifs erreurs de circulation

Avez-vous besoin de l'aide de vos pairs ? ou des fournisseurs en amont pour atténuer l'attaque ?

Post Mortem

A quelle vitesse le
attaque identifiée et
classé ?

Les outils ont-ils été efficaces ?
pour atténuer l'attaque ?

Y a-t-il d'autres
mesures préventives
qui peuvent être mis en place pour
prévenir les attaques futures ?

Y a-t-il d'autres
les mesures d'atténuation qui
peuvent être mises en place pour
plus efficace pour atténuer
des attaques futures ?

Étaient les communications
opportun et efficace ?

Étaient des ISP mutuels
accords d'assistance
nécessaire ? Efficace ?

Annexe B : Glossaire de la DDoS basée sur le serveur du CSRIC IV WG5

(Ce glossaire combine les glossaires des rapports finaux du CSRIC III WG7 comme base de référence).

I. Conditions :

1. Filtrage des trous noirs / Routage des trous noirs

Technique utilisée pour éliminer le trafic réseau en fonction de l'adresse IP source ou destination. Le filtrage/routage des trous noirs est généralement utilisé pour atténuer une attaque DoS ou DDoS par un opérateur de réseau. Cette technique peut être déployée au niveau des routeurs de périphérie, de frontière ou centraux afin d'éliminer efficacement le trafic d'attaque à proximité des points d'entrée du réseau pour minimiser les effets d'une attaque sur le réseau ou le trafic d'autres clients.

2. Bot

Un "bot" malveillant (ou potentiellement malveillant) (dérivé du mot "robot", ci-après simplement appelé "bot") désigne un programme installé sur un système afin de permettre à ce système d'exécuter automatiquement (ou semi-automatiquement) une tâche ou un ensemble de tâches, généralement sous le commandement et le contrôle d'un administrateur distant (souvent appelé "bot master" ou "bot herder").

Les systèmes informatiques et autres dispositifs d'utilisateur final qui ont été "botté" sont aussi souvent appelés "zombies".

Les robots malveillants sont généralement installés subrepticement, sans le consentement de l'utilisateur ou sans que celui-ci comprenne parfaitement ce que son système pourrait faire une fois le robot installé.

Les bots sont souvent utilisés pour envoyer des courriers électroniques indésirables ("spam"), pour reconnaître ou attaquer d'autres systèmes, pour écouter le trafic réseau ou pour héberger des contenus illégaux tels que des logiciels piratés, du matériel d'exploitation des enfants, etc.

De nombreuses juridictions considèrent l'infection involontaire des hôtes des utilisateurs finaux comme un exemple d'intrusion informatique illégale.

3. Botnet

Les botnets sont des réseaux d'appareils informatiques d'utilisateurs finaux connectés à l'internet et infectés par des logiciels malveillants, qui sont contrôlés à distance par des tiers à des fins malveillantes.
Un botnet est sous le contrôle d'un "botherder" ou "botmaster" donné. Un réseau de zombies peut compter une poignée d'hôtes zombifiés ou des millions.

4. Fournisseur de communication

Les fournisseurs de communications sont constitués de fournisseurs de services Internet, de fournisseurs de services, d'opérateurs de réseaux, d'opérateurs de centres d'hébergement, d'opérateurs de centres de données et de l'écosystème de fabricants qui soutient ces fournisseurs.

5. Client (ou "Client direct")

La partie qui passe un contrat avec un ISP pour un service. Distinguez le "client" de l'"utilisateur autorisé" : par exemple, un café peut acheter un service Internet à un ISP. Le café serait le client du FSI. Le café peut choisir d'offrir l'utilisation gratuite de sa connexion (si elle est autorisée).

6. Centre de données

Une installation dédiée à l'hébergement de grandes quantités de ressources informatiques et de réseau dans un environnement offrant des capacités d'alimentation et de réseau à haute disponibilité.

7. Nettoyage des données

Acheminement du trafic d'attaque DoS ou DDoS vers un système ou un service qui tente de différencier le "bon" trafic réseau du trafic d'attaque et de laisser tomber le trafic d'attaque tout en laissant passer le bon trafic. Les épurateurs de données peuvent être déployés dans les réseaux des opérateurs de réseau ou dans les locaux des clients. Pour un trafic d'attaque supérieur à la bande passante vers les locaux du client, des laveurs de données basés sur le réseau sont nécessaires pour atténuer efficacement l'attaque.

8. Attaque par déni de service (DoS) ou déni de service distribué (DDoS)

A Une attaque par déni de service (DoS) ou déni de service distribué (DDoS) est une tentative d'empêcher des utilisateurs légitimes d'accéder à des informations ou à des services24 (US-CERT)". Une attaque par déni de service distribué consiste en deux ou plusieurs systèmes ou attaquants engagés dans l'attaque en même temps vers la même cible.

9. Détection

La détection est le processus par lequel un fournisseur de services ou un utilisateur final prend conscience qu'un système ou un appareil particulier a été infecté par un logiciel malveillant. Un fournisseur de services peut détecter qu'un système a été infecté de différentes manières, notamment en recevant des plaintes de tiers concernant des spams, des analyses de réseau ou des attaques provenant de ce système. Les utilisateurs finaux peuvent détecter les infections du système au moyen d'outils logiciels ou d'autres moyens.

10. Écosystème

Ce terme est souvent utilisé pour décrire les relations entre les différents participants à l'internet, à savoir les fabricants de matériel, les développeurs de logiciels, les fournisseurs d'accès à Internet et les fournisseurs de contenu, d'applications et de services internet qui permettent à l'internet de fonctionner et d'être utile aux utilisateurs finaux.

L'écosystème Internet comprend des fournisseurs de systèmes d'exploitation, des organisations axées sur l'utilisateur final, des fournisseurs de contenu, d'applications et de services Internet, des FAI, des fournisseurs de recherche, des utilisateurs finaux, des services informatiques, des sociétés d'hébergement, des fournisseurs de blogs, des fournisseurs de sécurité, des chercheurs, des gouvernements, des sociétés de services financiers et d'autres parties.

L'économie dite "souterraine" est aussi souvent décrite comme un "écosystème", avec de multiples participants remplissant divers rôles spécialisés. Par exemple, certains participants peuvent se spécialiser dans l'écriture de logiciels malveillants, tandis que d'autres peuvent "récolter" des adresses électroniques à partir de pages Web et de listes de diffusion, et d'autres encore peuvent se spécialiser dans la distribution de logiciels malveillants à ces adresses électroniques récoltées. L'écosystème des logiciels malveillants comprend aussi normalement la population des victimes potentielles ciblées et les organismes chargés de l'application de la loi qui luttent contre la cybercriminalité.

[24] http://www.us-cert.gov/ncas/tips/ST04-015

11. Utilisateur final

Utilisateur final : dans un contexte informatique et de réseau, l'utilisateur final est la personne qui, en fin de compte, fait un usage autorisé d'un produit ou d'un service.

L'utilisateur final n'est souvent pas la même personne que celle qui a acheté le produit ou le service. Par exemple, le propriétaire d'un café peut acheter de la connectivité pour ses clients ; dans ce cas, ce sont les clients du café, et non le propriétaire, qui sont les véritables "utilisateurs finaux", même s'ils n'ont pas passé de contrat direct avec un FSI pour la connectivité qu'ils utilisent.

Une partie, telle qu'un hacker/cracker qui utilise un produit ou un service sans l'autorisation de l'acheteur, serait normalement considérée comme un cyber-intrus et non comme un "utilisateur final" en soi.

12. Centre d'hébergement / Fournisseur d'hébergement

Les centres d'hébergement offrent différents types de services d'hébergement qui peuvent aller de l'hébergement géré utilisant des ressources informatiques, de réseau et de gestion fournies par l'opérateur du centre d'hébergement, à l'hébergement en colocation qui permet aux locataires de fournir leur propre équipement logé dans les racks de l'opérateur d'hébergement.

13. ISP

Un fournisseur d'accès à Internet (FAI) est une entreprise qui fournit un accès au détail à Internet pour les membres du public, ou pour les entreprises et autres organisations. Ces connexions peuvent se faire par câble, DSL, satellite, sans fil, par ligne commutée ou par d'autres technologies. Les FAI sont parfois aussi appelés "fournisseurs d'accès".
Une entreprise qui fournit un accès à l'Internet uniquement à ses propres employés ne serait normalement pas considérée comme un FSI. De même, un transporteur de réseau qui ne fournit qu'un accès en gros à l'Internet pour d'autres FSI serait normalement considéré comme un fournisseur de services de réseau (FRS), plutôt qu'un FSI.

14. Logiciels malveillants

"Malware" est l'abréviation de "logiciel malveillant".

Les robots malveillants sont un type de logiciels malveillants. Les autres formes de logiciels malveillants comprennent des catégories de logiciels connues sous le nom de virus, chevaux de Troie, vers, rootkits, crimeware, enregistreurs de frappe, composeurs, logiciels espions, logiciels publicitaires, etc. Les facteurs qui distinguent ces différents types de logiciels malveillants sont moins importants que la compréhension des raisons pour lesquelles les logiciels malveillants peuvent être considérés comme "malveillants".

Les logiciels malveillants violent souvent un ou plusieurs des principes fondamentaux suivants :

(a) Consentement : Un logiciel malveillant peut être installé même si l'utilisateur ne l'a pas demandé sciemment.
(b) Honnêteté : Les logiciels malveillants peuvent prétendre faire une chose, alors qu'ils font en réalité quelque chose de complètement différent.
(c) Vie privée-Respect de la vie privée : Les logiciels malveillants peuvent violer la vie privée d'un utilisateur, par exemple en capturant ses mots de passe ou ses informations de carte de crédit.

(d) Non-intrusivité : Les logiciels malveillants peuvent gêner les utilisateurs en faisant apparaître des publicités, en changeant la page d'accueil du navigateur, en rendant les systèmes lents ou instables et en les rendant susceptibles de tomber en panne, ou en interférant avec les logiciels de sécurité déjà installés.
(e) Inoffensivité : Les logiciels malveillants peuvent être des logiciels qui nuisent aux utilisateurs (par exemple, des logiciels qui endommagent notre système, envoient des spams ou désactivent les logiciels de sécurité).
(f) Respect de la gestion des utilisateurs : Si l'utilisateur tente de supprimer le logiciel, celui-ci peut se réinstaller ou passer outre les préférences de l'utilisateur.
Les utilisateurs peuvent installer des logiciels malveillants à leur insu en ouvrant une pièce jointe contaminée reçue par courrier électronique ou en visitant une page web au contenu malveillant. Les systèmes peuvent également être infectés directement par un attaquant à distance, ce dernier ayant ciblé une vulnérabilité connue qui peut être exploitée à distance, ou par l'utilisateur qui monte un CD, un DVD ou une clé USB infectés.

15. Atténuation

L'atténuation est le processus de gestion ou de contrôle des effets associés à un bot. Par exemple, si un système est infecté par un bot de spam et qu'il envoie des courriers électroniques commerciaux indésirables, l'atténuation peut consister à filtrer le spam émis par ce dispositif.

L'atténuation peut également consister à bloquer, à limiter l'accès ou à limiter le débit des services sur les appareils qui peuvent être utilisés dans une attaque DDoS réfléchie.

Notez que l'atténuation n'implique généralement pas la correction de la condition sous-jacente (ce serait la "remédiation") ; l'atténuation gère simplement les symptômes associés à une condition.

16. Opérateur de réseau

Une organisation qui fournit des services de réseau pour l'accès à l'Internet dans le domaine câblé ou sans fil. Les FAI, les sociétés de télécommunications, les câblo-opérateurs et les fournisseurs d'hébergement peuvent être des exemples d'opérateurs de réseau s'ils fournissent ces services.

17. Notification

La notification est un processus par lequel les FAI communiquent avec leurs utilisateurs finaux concernant l'infection possible de l'appareil de l'utilisateur final par un bot malware ou la manière dont un abonné peut prévenir ou identifier une telle infection. La notification peut également impliquer un processus par lequel les utilisateurs finaux sont dirigés vers des outils qui leur permettront de découvrir eux-mêmes les infections par des robots. La notification peut prendre différentes formes, notamment une notification directe par le FAI à l'utilisateur final, ou une notification indirecte par le biais des outils d'autodécouverte disponibles ou d'un tiers. La notification peut être effectuée via plusieurs canaux potentiels, notamment (mais pas exclusivement) le courrier électronique, le courrier postal, un appel téléphonique, une notification dans le navigateur, un outil d'autodécouverte en ligne ou un message SMS.

18. Prévention

La prévention consiste à renforcer un système ou un service afin qu'il soit moins vulnérable à la compromission et à l'exploitation. Par exemple, sur de nombreux systèmes, la prévention peut impliquer :

- Mise à jour du système d'exploitation et de toutes les applications avec les correctifs de sécurité disponibles.

- Installation ou activation d'un pare-feu
- Utilisation d'un logiciel anti-virus
- S'assurer que le système est régulièrement sauvegardé
- Utiliser des mots de passe forts
- Désactiver ou empêcher l'accès aux services réseau inutiles
- Encourager les utilisateurs à utiliser les services Internet en toute sécurité (par exemple, le courrier électronique, la navigation sur Internet, etc.)

19. Attaque DDoS réfléchie

Une attaque DDoS qui falsifie l'adresse source des paquets IP d'attaque avec l'adresse IP de la victime et envoie les paquets IP à des hôtes intermédiaires. Lorsque l'hôte intermédiaire répond à ces paquets, les paquets de réponse sont envoyés à l'adresse IP de la victime, inondant celle-ci de trafic en provenance des hôtes intermédiaires. En général, dans ce type d'attaque, on utilise des hôtes et des protocoles intermédiaires où le paquet de réponse est plus grand que le paquet de demande, ce qui amplifie le trafic réseau envoyé à la victime.

20. Assainissement

La remédiation est le processus que suit l'utilisateur final pour nettoyer un ordinateur infecté afin qu'il ne le soit plus. Dans les cas simples, il s'agit d'installer et d'exécuter un produit anti-virus. Dans les cas plus difficiles, la remédiation peut impliquer une intervention plus substantielle allant jusqu'à "atomiser et paver" le système - le formater et le réinstaller à partir de zéro, ou au moins à partir de la dernière sauvegarde propre connue. Une fois que le système est propre ou qu'il a été réinstallé, il est normalement renforcé pour le protéger contre la réinfection.

21. Serveur

Un serveur de réseau est un ordinateur conçu pour traiter les demandes et fournir des données aux ordinateurs clients sur un réseau local ou sur Internet. Les serveurs des centres de données et des centres d'hébergement sont généralement dotés de connexions à large bande passante vers le réseau et disposent d'importantes ressources informatiques pour traiter un grand nombre de demandes dans un court laps de temps.

22. Spam

Courriel non désiré et non demandé, souvent de nature commerciale, envoyé normalement à un grand nombre de destinataires sous une forme sensiblement identique. Le spam est souvent envoyé par des "affiliés" qui sont payés par la personne qui gère le programme d'affiliation lorsque les destinataires achètent le produit annoncé par le spam.

II. Le cycle de vie de l'infection :

1. Propre : Aux fins du code de conduite anti-botnet volontaire des FAI, un ordinateur ou un autre dispositif en réseau sera considéré comme "propre" lorsqu'il (a) ne présente aucun symptôme d'infection perceptible de l'extérieur (tel que l'envoi de pourriels, la participation à une attaque par déni de service distribué ou le contact avec un hôte de commande et de contrôle connu), et (b) qu'un examen de l'ordinateur ou d'un autre dispositif en réseau à l'aide d'un programme anti-virus commercial ou gratuit/ouvert généralement accepté (utilisant les définitions disponibles les plus récentes) ne révèle aucune infection, et (c) que l'ordinateur ou tout autre dispositif semble fonctionner normalement à tous égards. Un système nouvellement acheté est présumé démarrer dans un état propre "hors de la boîte", sauf preuve du contraire.

2. Vulnérable : Un ordinateur ou un autre dispositif en réseau est considéré comme "vulnérable" lorsqu'il présente une ou plusieurs failles ou configurations erronées qui le rendent potentiellement susceptible d'être compromis, infecté ou utilisé comme support réfléchissant dans une attaque DoS ou DDoS. Un exemple courant de dispositif vulnérable est un dispositif qui n'a pas été corrigé ou qui utilise un mot de passe facile à deviner pour l'accès. Notez qu'un système peut être "propre" et "vulnérable" simultanément, comme dans le cas où un système vulnérable est protégé par un contrôle compensatoire (tel qu'un pare-feu), permettant ainsi au système d'éviter d'être infecté ou compromis malgré la présence d'une ou plusieurs vulnérabilités.

3. Infecté : Un ordinateur ou un périphérique réseau infecté est un ordinateur sur lequel un logiciel ou un micrologiciel malveillant a été installé sans autorisation préalable. Ce logiciel malveillant ou microprogramme malveillant peut être appelé virus, cheval de Troie, ver, rootkit, enregistreur de frappe, composeur, logiciel criminel, logiciel espion, logiciel publicitaire, etc. Une définition complète de
Le terme "malware" se trouve dans le glossaire figurant à l'annexe A du document "ABCs for ISPs" du CSRIC de la FCC.

4. Isolé : Un système infecté ou compromis peut être isolé pour l'empêcher de générer un trafic Internet indésirable. Les hôtes isolés sont souvent placés dans des "jardins clos" où ils ne peuvent accéder qu'à un ensemble strictement limité de ressources nécessaires à la remédiation, ou ne sont autorisés qu'à accéder à des services de sécurité (tels que le service de téléphonie VoIP pour les urgences).

5. Hors ligne : Un système hors ligne est un système où aucun accès au réseau n'est autorisé vers/depuis cet hôte. D'un point de vue conceptuel, pensez à un hôte connecté à un réseau Ethernet dont le câble Ethernet a été déconnecté (ou le port du commutateur Ethernet a été désactivé), bien que des processus techniques différents soient évidemment utilisés dans le cas de connexions par modem câble, DSL, etc.
connexions, accès sans fil, accès par modem, etc.

6. Désinfecté : Un système est considéré comme "désinfecté" lorsque, après avoir été infecté, il a été ramené à un état "propre" (comme défini précédemment). La première étape de la désinfection d'un système consiste souvent à installer et à exécuter un produit antivirus (s'il n'était pas déjà installé et à jour). Dans certains cas, il peut être nécessaire de formater et de réinstaller le système depuis le début pour venir à bout de logiciels malveillants persistants particulièrement bien cachés.

7. Durci : Un système durci est un système qui a été systématiquement configuré de manière à éliminer les vulnérabilités (ou les vulnérabilités potentielles) du système. Par exemple, entre autres choses, un système renforcé est doté de correctifs à jour, tous les services inutiles sont désactivés, tout le trafic réseau sensible doit être crypté, un système de sécurité fort est utilisé. des mots de passe ou une authentification multifactorielle, effectuera une journalisation sécurisée vers un hôte de journalisation hors système, etc.

8. Réinfection : Un système qui a été désinfecté mais PAS durci sera souvent réinfecté rapidement.

9. Compromis : Alors que de nombreux systèmes vulnérables peuvent être compromis à la suite d'une infection par un logiciel malveillant, d'autres systèmes vulnérables peuvent être compromis à la suite de mots de passe faibles ou d'une mauvaise configuration (comme des fichiers critiques qui peuvent être modifiés involontairement par des parties non autorisées). Un système compromis n'est pas digne de confiance.

10. Géré : Un "hôte géré" est un hôte qui est administré de manière centralisée, plutôt que d'être autonome.

administré par le ou les utilisateurs du système. Les hôtes gérés sont couramment utilisés dans les grandes entreprises et les agences gouvernementales.

11. Surveillé : Un hôte surveillé est un hôte qui est continuellement (ou au moins périodiquement) scruté pour des choses comme un trafic réseau anormal ou des modifications non autorisées de fichiers système critiques. La surveillance peut s'effectuer via des systèmes de sécurité réseau, tels que Snort, ou via des systèmes basés sur l'hôte, tels que Tripwire.

12. Remplacé : Si la plupart des utilisateurs tentent de désinfecter et de renforcer un système infecté, certains peuvent choisir de le remplacer par un nouveau système. Le système précédent peut alors être vendu ou donné à un tiers, qui peut obtenir le système et les logiciels malveillants qui y sont installés.

13. Partagé : Un système partagé est un système qui est utilisé par plusieurs personnes. Un exemple courant de dispositif partagé serait un dispositif familial utilisé par un ou plusieurs parents ainsi que par les enfants ou d'autres membres de la famille. Un dispositif partagé semble souvent plus sujet aux infections (ou autres problèmes de sécurité) qu'un système utilisé par une seule entité.

14. Orphelins : Un dispositif ou un programme orphelin est un dispositif ou un programme ancien pour lequel le fournisseur ne publie plus de correctifs de sécurité/stabilité, même critiques. Les systèmes ou programmes orphelins ne peuvent généralement pas être renforcés.

III. Rôles des écosystèmes

1. Client : Dans le contexte de l'ABC des FAI, la personne qui paie un FAI pour un service Internet.

2. Propriétaire du système : la personne qui possède un ordinateur ou un autre dispositif donné.

3. Utilisateur du système : une personne que le propriétaire du système autorise intentionnellement à utiliser son ordinateur ou un autre appareil.

4. Personne de soutien : Pour les ordinateurs résidentiels, une personne de soutien peut être un membre de la famille ou un ami qui aide le propriétaire ou l'utilisateur du système à utiliser et à entretenir son ordinateur. Il peut également s'agir d'un spécialiste commercial de l'assistance informatique engagé à cette fin par le propriétaire ou l'utilisateur de l'ordinateur.

5. ISP Security/Abuse Team : La personne ou le groupe d'un fournisseur de services Internet qui traite les plaintes concernant un client.

6. Vendeur : La société qui a fabriqué et commercialisé un système informatique ou un logiciel. On peut parler d'un fournisseur de système d'exploitation, d'un fournisseur de logiciels d'application, d'un fournisseur de matériel informatique ou d'un fournisseur de logiciels antivirus, par exemple.

7. Application de la loi : Un agent de police, un shérif, un agent fédéral ou toute autre personne assermentée ayant le pouvoir d'enquêter sur des crimes, de rassembler des preuves et de procéder à des arrestations.

8. Régulateur : Un fonctionnaire d'État ou fédéral chargé de gérer les pratiques commerciales ou toute autre activité de manière à garantir une équité fondamentale ou le respect des réglementations. Un exemple de régulateur serait la Commission fédérale du commerce des États-Unis. Les régulateurs ont généralement recours à des sanctions civiles (telles que des amendes administratives ou des poursuites civiles) plutôt qu'à des sanctions pénales (telles que l'arrestation ou l'incarcération).

9. Utilisateur non autorisé : une personne qui utilise un ordinateur ou un autre dispositif sans l'autorisation intentionnelle de l'utilisateur. L'autorisation du propriétaire du système, ou une personne qui utilise un accès autorisé au-delà de son autorisation.

10. Auteur du logiciel malveillant : Le programmeur ou l'équipe de programmation qui conçoit et code un logiciel malveillant, tel qu'un robot.

11. Botmaster : Un botmaster est une personne qui exploite un réseau d'ordinateurs bots, qu'elle utilise souvent pour envoyer du spam ou attaquer d'autres ordinateurs. Le botmaster envoie normalement des commandes à "ses" bots via un hôte de commande et de contrôle, par exemple un serveur sous son contrôle.

12. Affilié : Dans ce contexte, un affilié est une personne qui contribue à la commercialisation d'un produit ou d'un service particulier en échange d'une rémunération, généralement par le biais de modèles de paiement par impression, de paiement par clic, de paiement par installation ou de partage des revenus :
(a) Paiement à l'impression (PPI) : les affiliés sont généralement des propriétaires de sites web qui sont payés en fonction du nombre de fois qu'une bannière de site web ou une autre publicité est montrée aux visiteurs.
(b) Le paiement au clic : dans ce modèle, les affiliés sont payés lorsque quelqu'un clique effectivement sur une publicité.
(c) Paiement à l'installation : dans ce modèle, les affiliés sont payés lorsqu'un programme qui leur a été fourni est installé sur un nouveau système, soit subrepticement, soit avec le consentement éclairé de l'utilisateur (peut-être dans le cadre d'une offre d'"accès sponsorisé" pour un programme ou un site qui devrait autrement être acheté).
(d) Partage des revenus : dans ce modèle, les affiliés reçoivent un pourcentage des ventes associées aux clients qu'ils ont référés.

13. Vendeur de listes : Un vendeur de listes est une personne qui compile et distribue des listes d'adresses électroniques. Par exemple, un spammeur qui souhaite faire de la publicité pour un casino en ligne illégal peut acheter une liste d'adresses électroniques connues pour être associées à des joueurs en ligne.

14. Société d'hébergement à l'épreuve des balles : Une société d'hébergement à l'épreuve des balles est une société qui accepte d'héberger un site web ou une autre présence en ligne malgré les plaintes qui peuvent résulter de cette activité, généralement en échange du paiement d'un prix supérieur par la partie hébergée. Les sociétés d'hébergement à l'épreuve des balles peuvent être utilisées pour héberger des sites Web de spam, des logiciels malveillants, des documents relatifs à la maltraitance des enfants ou tout autre contenu susceptible d'être inacceptable pour les sociétés d'hébergement ordinaires.

15. Bureaux d'enregistrement de noms de domaine à l'épreuve des balles : Un bureau d'enregistrement de noms de domaine à l'épreuve des balles est un bureau qui permet à un spammeur ou à un autre cybercriminel d'enregistrer un nom de domaine et de le conserver, malgré les plaintes qui peuvent être associées à ce nom de domaine. Ce service est normalement fourni moyennant une prime par rapport aux tarifs d'enregistrement de noms de domaine du marché.

16. Processeur de paiement : Lorsqu'un affilié réalise une vente, le paiement est normalement effectué par carte de crédit. L'entité qui traite cette transaction par carte de crédit est appelée "processeur de paiement".

17. Expéditeur direct : Un expéditeur direct est une entité qui gère l'exécution des commandes pour un programme d'affiliation. Par exemple, un expéditeur direct spécialisé dans les produits pharmaceutiques illégaux peut emballer et expédier des commandes obtenues par un spammeur de pilules.

18. Échangeur de devises en ligne : Certains affiliés peuvent être payés à l'aide d'une devise en ligne plutôt que par un chèque envoyé par la poste ou un dépôt direct. Les échangeurs de devises en ligne permettent à certains d'acheter une devise en ligne en échange d'espèces, ou vice versa.

19. Rapporteur d'abus : tierce partie signalant un incident d'abus à un FAI, ou par l'intermédiaire d'un centre d'échange (tel qu'une équipe de réponse aux incidents de sécurité informatique).

Annexe C : Taxonomie des attaques DDoS

1 Attaques DDoS - Attaquer la disponibilité

1.1 Définition des attaques DDoS

Aux fins de l'analyse, le groupe de travail a utilisé la définition suivante d'une attaque DDoS : "une **attaque par déni de service (DoS)** ou par **déni de service distribué (DDoS)** est une tentative d'empêcher des utilisateurs légitimes d'accéder à des informations ou à des services25 (US-CERT)". Une attaque par déni de service distribué consiste en deux ou plusieurs systèmes ou attaquants engagés dans l'attaque en même temps vers la même cible.

1.2 1.2 Objectifs des attaques DDoS

1.2.1 Attaques contre les capacités

1.2.2 Attaques contre l'État

1.3 Outils d'attaque DDoS

1.3.1 Les botnets

1.3.1.1 Botnets clients

1.3.1.2 Les botnets de serveurs

1.3.1.3 Botnets participatifs

1.3.1.4 Autres botnets

1.3.2 Harnais d'attaque

1.3.3 Applications de génération de trafic

2 Attaques DDoS IPv4 & IPv6

2.1 Attaques DDoS volumétriques

2.1.1 Inondation directe par paquets

2.1.1.1 ICMP et ICMPv6

2.1.1.2 UDP

2.1.1.3 TCP

2.1.1.3.1 SYN-Flood (inondation)

2.1.1.3.2 RST-Inondation

2.1.1.3.3 ACK-Inondation

2.1.1.3.4 RST-Inondation

2.1.1.3.5 Inondation nulle

2.1.1.3.6 Inondation SYN/ACK

2.1.1.3.7 Inondation de l'arbre XMAS

2.1.1.3.8 Invalidité de la combinaison de drapeaux Flood

2.1.1.3.9 Inondation du port 0

2.1.1.4 Paquets fragmentés

2.1.1.4.1 UDP

2.1.1.4.2 TCP

2.1.1.5 Protocole 0

2.1.1.6 Inondation par GRE (General Routing Encapsulation)

2.1.1.7 Inondation ESP (IPsec Encapsulating Security Payload)

2.1.1.8 Inondation du RTP

2.1.1.9 Autres protocoles "non standard" inondation

2.1.2 Réflexion/Amplification

2.1.2.1 Réflexion/amplification UDP

[25] http://www.us-cert.gov/ncas/tips/ST04-015

Annexe D : Études de cas sur l'atténuation des attaques DDoS

Études de cas du sous-groupe ISP

I. Contexte

Depuis plusieurs années, les fournisseurs d'accès à Internet (FAI) s'emploient activement à atténuer les *attaques par déni de service distribué (DDoS)*[26] . Dans les premières versions les plus courantes de l'attaque, les ordinateurs personnels connectés à des services domestiques à large bande commençaient à être infectés par des logiciels malveillants qui transformaient les machines en *zombies (*désormais appelés *bots*). En utilisant des serveurs compromis séparément pour le contrôle, les attaquants pouvaient alors commander de grands groupes de bots pour envoyer des volumes de données à une victime, généralement un site web. Le site Web est alors submergé par les données entrantes et est incapable de traiter les demandes normales autorisées.

De 1999 à 2011 environ, les volumes de données visant l'infrastructure de la plupart des FAI et l'habileté avec laquelle ces volumes de données ont été élaborés par les adversaires sont restés dans des limites gérables. Au *cours de cette période de douze ans, très peu d'attaques majeures ayant un impact sur les services ont été menées sur une partie de l'infrastructure des grands FAI*. Cela inclut les attaques contre l'infrastructure des services de noms de domaine des principaux FAI de niveau 1. Les attaques au cours de cette période étaient généralement de l'ordre de plusieurs gigabits par seconde.

En outre, au cours de cette même période, certains fournisseurs de services Internet ont développé de nouveaux services de sécurité gérés pour les entreprises afin de les aider à atténuer les attaques DDoS sur leur propre infrastructure. Plusieurs institutions financières américaines sont actuellement abonnées à ces services qui impliquent généralement une détection en temps réel des attaques basée sur des solutions volumétriques ou applicatives. Par exemple, une attaque DDoS peut être détectée de manière volumétrique en fonction des pics de trafic à l'aide d'outils de collecte de données, puis le trafic est redirigé à l'aide du protocole BGP (border gateway protocol) vers des pare-feu spécialement conçus pour filtrer l'attaque. Le trafic épuré est ensuite "tunnelisé" vers le site du client via l'infrastructure du FAI.

Fin 2012, les FAI ont commencé à voir des attaques à plus grande échelle par des adversaires créant un volume entrant suffisant pour potentiellement dépasser la capacité d'entrée de l'infrastructure d'épuration de certains FAI. En outre, le botnet à l'origine de l'attaque était unique en ce sens qu'il utilisait des serveurs sur des connexions réseau souvent importantes comme bots, plutôt que des PC compromis sur des connexions haut débit grand public. Plus tard au cours du troisième trimestre, ce même adversaire a lancé une série d'"attaques télégraphiées" sur des sites Web bancaires, dont les avertissements étaient régulièrement publiés sur *pastebin*. Ces attaques ont atteint une taille sans précédent, ciblant souvent à nouveau les DNS. En réaction, les FAI ont procédé à plusieurs ajustements en temps réel pour renforcer leur infrastructure, leurs plates-formes de scrubbing et la capacité des sites DNS27.

Cette étude de cas a pour but de fournir une explication et de proposer des pratiques que les FAI peuvent adopter.

---

[26] Une **attaque par déni de service (DoS)** ou par **déni de service distribué (DDoS)** est une tentative d'empêcher des utilisateurs légitimes d'accéder à des informations ou à des services26 (US-CERT).

[27] Il s'agit d'un processus continu d'ingénierie du trafic. De nombreux FAI surveillent en permanence les flux de trafic pour garantir une capacité adéquate. Ce même processus s'applique aux liaisons de données vers l'infrastructure d'épuration DDoS des FAI.

en réponse à des attaques DDoS de grande envergure à l'avenir.

II. Taxonomie simplifiée des attaques DDoS pour les ISP

Alors que le groupe de travail élargi a développé une taxonomie détaillée des attaques DDoS, le sous-groupe ISP a estimé qu'il était nécessaire de développer une version simplifiée pour l'étude de cas. Le sous-groupe a également discuté d'un modèle permettant de classer les attaques DDoS en deux dimensions :

1. Type d'attaque - volumétrique ou d'application
2. Direction de l'attaque - soit du *nord au sud*, soit *de l'est à l'ouest*.
    a. Une attaque *Nord-Sud* est une attaque qui provient de l'extérieur du réseau du FAI et qui vise un client ou une infrastructure du FAI à l'intérieur du réseau du FAI.
    b. *Une attaque sud-nord est une attaque qui prend naissance à l'intérieur du réseau du FAI et qui vise une entité ou une infrastructure externe à l'intérieur du réseau du FAI.*
    c. *East-to-West* représente une attaque qui part d'un client et vise un autre client.

Exemples :

1. L'infrastructure du client ou du FAI est frappée de l'extérieur - du nord au sud.
2. Les clients avec des passerelles domestiques boguées inondent les serveurs DNS des FAI - du sud au nord
3. Les clients inondent les paquets vers une cible externe - également du sud au nord.
4. Les clients s'attaquent les uns aux autres - d'est en ouest

Le sous-groupe a suggéré que nous distinguions les clients qui s'attaquent les uns aux autres des clients qui attaquent des infrastructures ou des cibles externes, car cela nécessite parfois des stratégies de détection et d'atténuation différentes. Par exemple, si deux clients d'une même région s'attaquent l'un à l'autre, le trafic peut ne traverser aucun des routeurs à partir desquels les FAI collectent les données de flux, et il n'atteindra pas les centres d'épuration à la périphérie de l'échange de trafic du FAI.

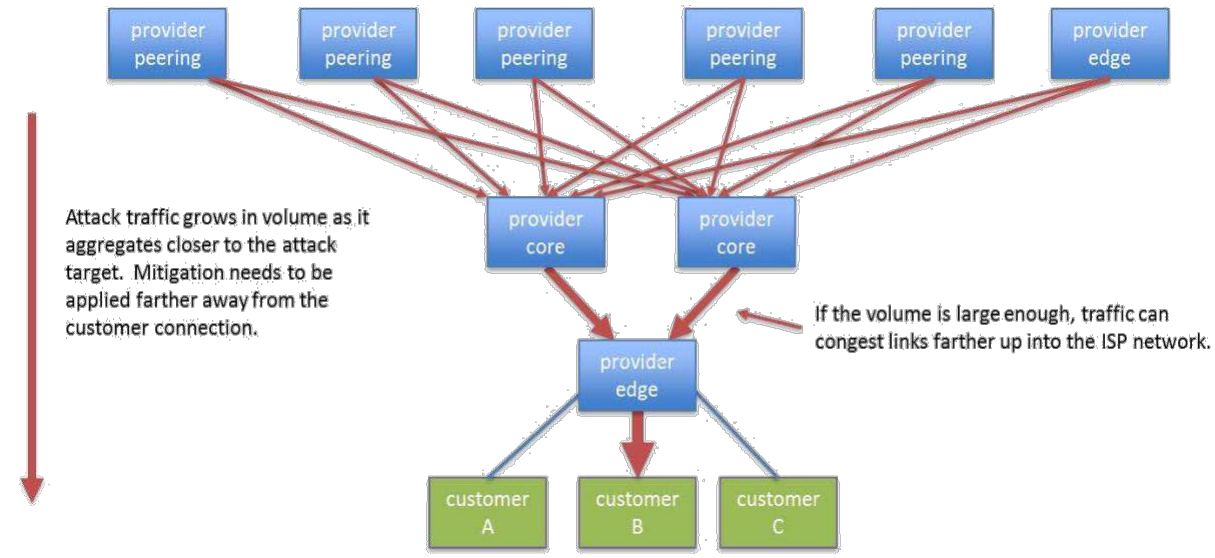
III. Exemples d'attaques DDoS subies par les FAI

A. Attaque DoS volumétrique basée sur un serveur contre un gros client

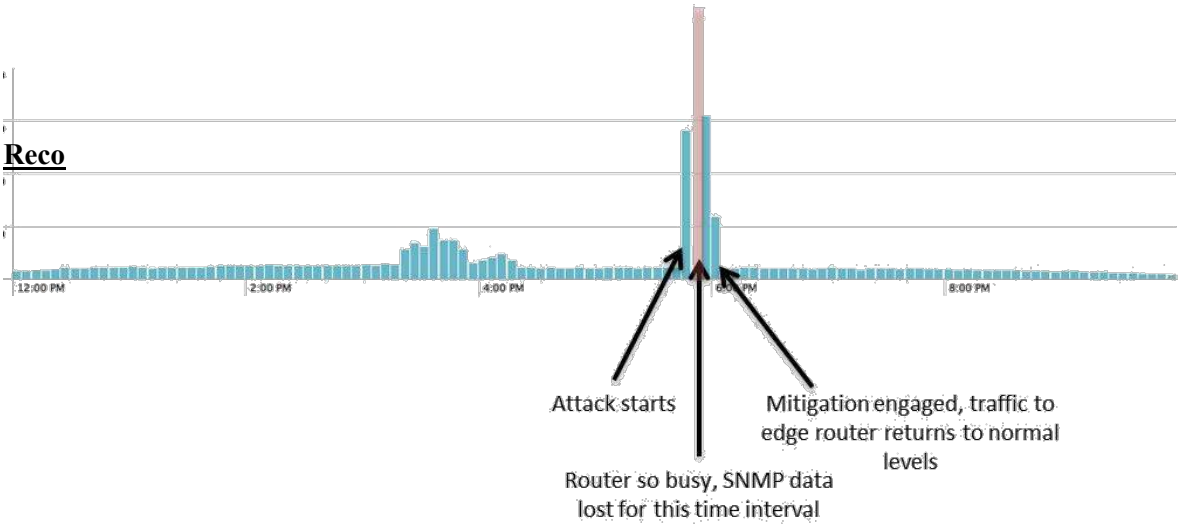
Contexte : Cette attaque a utilisé des paquets UDP/80 (trafic poubelle) en grand volume pour épuiser la bande passante de la cible. L'attaque a pris environ 10 minutes pour atteindre un volume maximal de plus de 70 Gbps. À l'époque, il s'agissait de l'une des plus grandes attaques observées sur le réseau du FAI. Les adresses IP attaquantes se comptaient par milliers.

Mesures d'atténuation :

1. L'attaque a été identifiée avec une adresse IP cible par le service de détection de déni de service du client.
2. Le client a fait appel au service d'atténuation des attaques, le trafic a été réacheminé vers les centres d'atténuation des attaques. Le trafic d'attaque a été abandonné et le trafic légitime a été livré.



Dans le cas d'attaques plus importantes (10 à 100 Gbps), il existe un risque d'impact collatéral sur les clients non visés par l'attaque. Les dommages collatéraux peuvent souvent être évités si l'attaque est détectée et atténuée rapidement.



Pratiques recommandées :

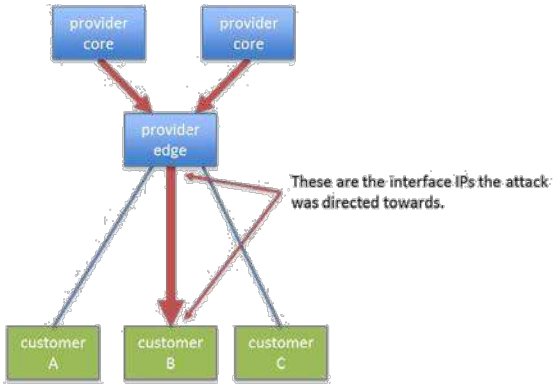
1. Le routage par trou noir doit être configuré sur les routeurs des FAI en cas d'attaque d'un client qui n'est abonné à aucun service d'atténuation des attaques de type DoS.
2. L'instrumentation du réseau et les alarmes basées sur le polling SNMP, le netflow, les sondes ou une technologie similaire sont essentielles pour détecter rapidement (15 minutes ou moins) les problèmes de saturation de la bande passante.
3. La collecte de flux nets ou une technologie similaire doit être déployée pour identifier les cibles d'attaque et les protocoles cibles.
4. Les fournisseurs qui proposent des services d'atténuation des attaques et de nettoyage doivent concevoir l'infrastructure. de sorte que le trafic d'attaque ne soit pas concentré dans une seule zone ou un seul centre d'épuration. La capacité de ces centres doit être dimensionnée de manière appropriée.

B. Attaque dirigée vers les IP des ISP et des infrastructures des clients

Contexte : Cette attaque a de nouveau utilisé des paquets UDP/80 (trafic poubelle) en grand volume pour épuiser la bande passante de la cible. Cependant, dans ce cas, l'attaque était d'abord dirigée vers l'interface IP du routeur du client, puis vers celle du FAI.

Mesures d'atténuation :

1. L'attaque a été identifiée avec une IP cible via un flux net.
2. Le sous-réseau /30 entre le FAI et le client a été mis sur liste noire.
3. Des filtres ont ensuite été appliqués sur les routeurs frontaliers des FAI pour limiter le trafic destiné à l'infrastructure des FAI.



Pratiques recommandées :

- Limitez autant que possible le trafic à l'infrastructure point à point du FAI, que ce soit par filtrage ou par routage.
- N'utilisez pas les IP de l'infrastructure point à point pour le NAT, la terminaison des tunnels ou tout autre trafic qui exige que les IP soient annoncées et acheminées alors qu'elles n'auraient pas besoin de l'être.
- Mettez en œuvre la détection comme suggéré dans l'étude de cas 1 afin que ces attaques puissent être identifiées rapidement. Notez que lorsqu'une adresse ISP est la cible de l'attaque, le client ne verra jamais le trafic.

Défis potentiels :

- Le filtrage à chaque point d'entrée du FAI peut s'avérer peu pratique.
- La réadaptation d'un réseau à un espace qui n'est pas acheminé peut être une tâche difficile et fastidieuse.

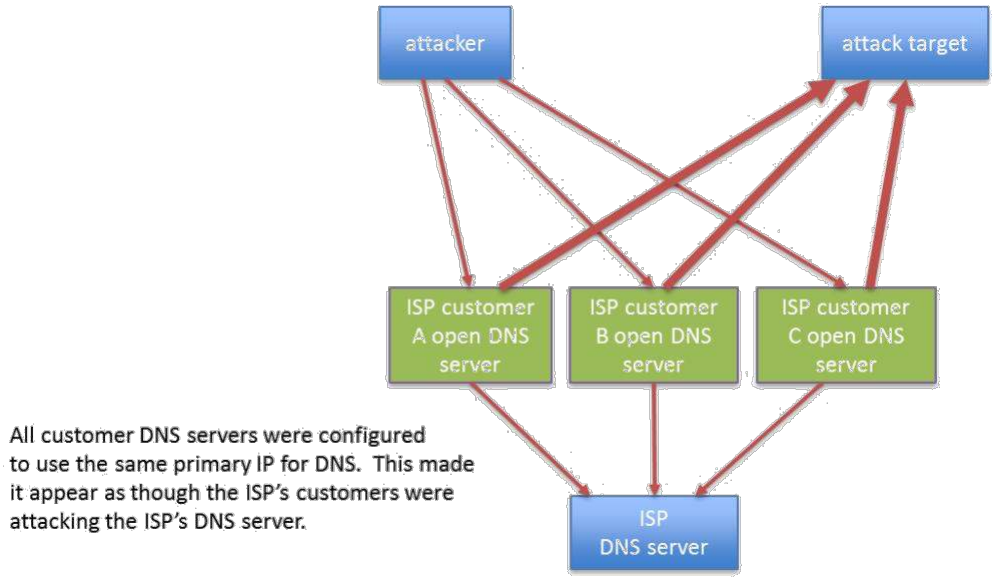
C. Dommages collatéraux de l'attaque par réflexion du DNS

Contexte : Cette attaque a de nouveau utilisé des paquets UDP/53 usurpés (requêtes DNS) en grand nombre vers des serveurs DNS récursifs non filtrés pour amplifier l'attaque et épuiser la bande passante de la cible. Dans ce cas, le fournisseur d'accès Internet risquait de subir un impact négatif, même si l'attaque n'était pas du tout dirigée contre lui.

Mesures d'atténuation :

1. L'attaque a été identifiée avec une IP cible via le flux net ainsi que la journalisation configurée sur le serveur DNS.
2. Les requêtes des clients étaient acheminées par un service d'atténuation des failles de sécurité.

3. Le fournisseur d'accès a ensuite assuré le suivi pour que l'équipement du client soit correctement filtré.



Pratiques recommandées :

- Configurer des services d'atténuation des attaques pour les infrastructures critiques comme les services DNS. Les exemples de mesures d'atténuation comprennent l'épuration du trafic et la limitation du débit des services.
- Augmenter la capacité d'atténuation selon les besoins des services d'infrastructure.
- Distribuez les services essentiels en utilisant des technologies telles que le anycast ou les réseaux de distribution de contenu lorsque cela est possible.
- Assurer la gestion hors bande des infrastructures critiques de manière à ce qu'une attaque n'empêche pas l'accès aux équipements nécessaires pour atténuer l'attaque.
- Limitez l'exposition des services aux seules personnes qui ont besoin d'y accéder (par exemple, DNS, NTP, etc.).
- Évitez d'utiliser des équipements configurés avec des services non protégés tels que des DNS non filtrés et des chaînes de communauté SNMP connues.
- Appliquez des contrôles anti-spoofing là où c'est possible et pratique, par exemple dans les réseaux résidentiels et les centres d'hébergement.

Défis potentiels :

- Le provisionnement de la capacité d'atténuation peut être une "course aux armements" avec les attaquants.
- Certains services ne peuvent être filtrés efficacement sans un impact collatéral inacceptable.
- L'anti-spoofing (BCP 38) n'est pas possible pour de nombreux clients du transit.

D. Home Gateway/Router Originated DDoS

- **Contexte :** Un fournisseur particulier de passerelles domestiques avait un bogue qui l'obligeait à inonder de requêtes DNS le débit de la ligne lorsque le modem en face d'elle redémarrait. Le fournisseur d'accès à Internet a augmenté la vitesse de la bande passante sur son marché le plus important, ce qui a nécessité le redémarrage des modems. Environ 250 passerelles domestiques ont commencé à inonder les requêtes DNS, mettant hors service le cluster DNS du FAI.

- •

- Problèmes découverts :

- Pas de capacité d'atténuation des DDOS aussi profondément dans le réseau du FAI. Les centres d'épuration des données se trouvent à la périphérie du réseau du FAI.

- Les serveurs DNS renvoyaient des informations d'autorité supplémentaires et facultatives avec chaque réponse, ce qui provoquait un effet d'amplification.
- Les fonctions de limitation de débit n'étaient pas utilisées sur les équilibreurs de charge du FAI.
- L'ISP avait des difficultés à gérer les serveurs DNS par le biais des interfaces de requête, qui étaient saturées en raison de l'inondation DNS du modem à large bande.

- Mesures d'atténuation :

1. Utilisation d'outils de sécurité hors bande qui capturent les paquets DNS. Configuré les outils pour compter le nombre de paquets vus sur une période donnée et générer des alertes sur les clients dépassant ces seuils.
2. Introduire les alertes dans le système de gestion des abus existant et mettre les clients hors ligne.
3. Automatiser le processus pour une utilisation future

Recommandations :

- Pour un service donné, veillez à ce qu'il renvoie le moins d'informations possible afin qu'il ne puisse pas être facilement utilisé comme amplificateur.
- Assurez-vous que les serveurs restent joignables en cas d'attaque en séparant les interfaces de gestion des interfaces de service.
- Utiliser les fonctions de sécurité (telles que la limitation du débit) disponibles dans le matériel de réseau existant.
- L'atténuation peut être réalisée hors ligne à l'aide de moniteurs passifs qui signalent à d'autres outils de prendre certaines mesures.

E. Null Routing

Contexte : Le routage nul est la forme la plus simple d'atténuation des DDOS, mais aussi celle qui entraîne le plus de dommages collatéraux. C'est un marteau qui laisse tomber tout le trafic destiné à une adresse IP donnée.

Pour :

- Simple et rapide à mettre en œuvre
- Abandon du trafic à la périphérie du réseau sur les liens les plus importants.

Cons :

- Supprime tout le trafic vers une IP donnée et pas seulement le trafic malveillant.

Cas d'utilisation :

- Client résidentiel (ou autre IP dynamique) attaqué. Le FAI peut simplement supprimer tout le trafic destiné à l'IP cible et en donner une nouvelle au client.
- Attaque sortante. Si une adresse IP d'un autre FAI fait l'objet d'une attaque et que ce dernier indique que nos clients n'ont aucun besoin légitime de l'atteindre, le premier FAI peut supprimer les paquets avant qu'ils ne quittent son réseau. Exemple : le routeur d'un autre ISP est attaqué. Les clients du premier ISP n'ont aucune raison d'envoyer des paquets directement à ce routeur, donc ils ne routent pas son IP sur notre réseau.

IV. Techniques d'atténuation des FAI (outils/contrôles techniques)

La réponse aux attaques DDoS comporte deux phases principales :

Phase 1 : Détection

Les attaques DDoS peuvent être détectées par les FAI en utilisant des méthodes volumétriques ou basées sur les applications. Par exemple, dans le cas des solutions volumétriques, les FAI établissent une base de référence par rapport à laquelle les anomalies du trafic d'attaque peuvent être déterminées. Un autre moyen de détecter les attaques est de s'adresser directement aux clients qui, souvent, observent eux-mêmes une augmentation progressive des volumes de trafic d'entrée et contactent les FAI en conséquence.

Détection :

Type	Du nord au sud	Du sud au nord	D'est en ouest
Volumétrique	- • Basé sur le flux net solutions - • Utilisation suivi de - • Appel de la victime	- • Basé sur le flux net solutions - • Appel de la victime	- • Appel de la victime
Application28	- • Basé sur le DPI solutions - • Basé sur l'hôte solutions - • Appel de la victime	Solutions basées sur le - • DPI Solutions basées sur - • l'hôte - • Appel de la victime	- • Appel de la victime

Phase 2 : Atténuation

La phase d'atténuation de l'activité de réponse aux DDOS a pour objectif de contrer les effets de l'action malveillante. L'atténuation prend généralement la forme (1) d'un filtrage du mauvais trafic, ou (2) d'une réduction de l'intensité de l'attaque en dégradant la source du botnet. Cette deuxième action peut être réalisée de diverses manières, par exemple en contactant les propriétaires de PC et de serveurs infectés avant, pendant et après une attaque. Ainsi, l'objectif principal des activités de sécurité DDoS des FAI implique toutes les tentatives possibles pour réussir à bloquer, détourner, filtrer et ralentir le trafic d'attaque intégré dans le flux normal du trafic d'entrée destiné à un site victime. Étant donné que la plupart des attaques DDOS varient considérablement (contrairement aux récentes attaques bancaires, qui suivaient une cadence plus routinière), le processus de décision peut être très dynamique et dépend généralement d'une analyse en temps réel.

Atténuation :
D'une manière générale, on préfère souvent la technique d'atténuation la plus simple qui résoudra le problème. Du point de vue des services, cependant, les techniques d'atténuation plus spécifiques sont préférées à celles qui sont plus brutales et ont un impact plus important sur le trafic légitime. Comme indiqué précédemment, l'action appropriée dans une situation donnée dépend des spécificités de l'attaque et de la cible.

Les routes de trou noir sont la solution préférée dans le cas où le service ou le client sous

[28] Les attaques DDoS au niveau de la couche applicative peuvent être plus difficiles à détecter et, dans certains cas, nécessiter des outils plus intrusifs que les outils volumétriques traditionnels, comme l'utilisation de l'inspection approfondie des paquets (DPI), et peuvent également être compliquées par l'utilisation du cryptage SSL ou autre.

L'attaque ne subira aucune dégradation ou coupure en perdant tout le trafic vers la cible. Par exemple, dans le cas où l'adresse cible n'a jamais besoin de recevoir de trafic en provenance d'Internet, une route en trou noir de cette IP est la réponse la plus simple. En outre, une attaque sortante peut également être atténuée par le routage en trou noir de la cible de l'attaque. Si des services sont requis pour l'adresse cible, mais que l'attaque utilise un protocole ou un service différent, un filtre de paquets tel qu'un routeur ACL peut être efficace. Les attaques volumétriques non triviales, c'est-à-dire celles qui visent des services nécessaires, nécessitent souvent des services d'épuration plus spécialisés ou des solutions d'IAP. Ces services sont conçus pour permettre à la plupart du trafic légitime de passer tout en bloquant la plupart du trafic d'attaque.

Type	Du nord au sud	Du sud au nord	D'est en ouest
Volumétrique	- • Frottage centre/hors-rail - • route du trou noir - • routeur ACL - • BGP Flowspec	- • Suspendre l'attaquant service - • Contrôle des autres dispositifs, comme le blocage les ports d'un modem - • route du trou noir - • routeur ACL	• Suspendre le service de l'attaquant • Contrôle d'autres dispositifs, comme le blocage des ports d'un modem. • route du trou noir • routeur ACL
Application	- • Frottage centre/hors-rail - • Basé sur le DPI solutions - • Basé sur l'hôte solutions	- • Solutions basées sur le DPI - • Solutions basées sur l'hôte - • Suspendre l'attaquant service - • Contrôle des autres dispositifs, comme le blocage les ports d'un modem	• Suspendre le service de l'attaquant • Contrôle d'autres dispositifs, comme le blocage des ports d'un modem. • Solutions basées sur l'hôte

V. Recommandations supplémentaires

- Les FAI examinent l'ensemble de recommandations *ABCs for ISPs* pour l'atténuation des logiciels malveillants publié par le CSRIC III en 2012, étant donné que de nombreuses attaques DDoS ont émané d'utilisateurs finaux infectés.
- Des meilleures pratiques similaires doivent être développées pour les fournisseurs d'hébergement en termes de bureau des abus et de processus de notification pour alerter les locataires infectés des centres d'hébergement en cas d'attaques basées sur les centres de données.
- Les FAI examinent le PCA 38 et d'autres alternatives pour gérer potentiellement l'usurpation d'adresse IP.

Étude de cas du sous-groupe financier

Étude de cas :

De la fin 2012 à la mi-2013, les institutions financières américaines (USFI) ont subi des attaques continues de déni de service distribué (DDoS) contre leurs réseaux. L'analyse indique que certaines de ces attaques proviennent d'un acteur de la menace d'un État-nation. Ces attaques montrent des signes de planification préalable et leur complexité continue d'évoluer.

On pense que les attaques DDoS contre les USFI font partie d'une stratégie d'attaque plus vaste et laissent présager des attaques plus graves. Les USFI visées représentent une composante importante de l'activité économique américaine, sont emblématiques de la stabilité économique des États-Unis et, si elles sont compromises, elles pourraient représenter un risque systémique pour le secteur financier. Les groupes qui s'en attribuent le mérite ont menacé de lancer d'autres attaques.

Qu'est-ce qu'une attaque DDOS ?
Une attaque DDoS est une cyberattaque coordonnée visant à perturber la disponibilité d'un ou de plusieurs systèmes de traitement de l'information ou d'une ou de plusieurs applications en consommant la bande passante du réseau ou en submergeant le système cible de connexions de données simultanées provenant de plusieurs sources autonomes. Le modèle distribué a donné naissance aux botnets, qui sont des collections d'hôtes infectés par des logiciels malveillants et capables de lancer des attaques DDoS au gré de l'adversaire qui les contrôle afin de modifier considérablement la vitesse des attaques.

Types de DDoS utilisés :

- Inondation UDP
- Flooding TCP
- Attaques de la fonction de recherche
- Fichier volumineux GET
- Attaques au niveau des infrastructures
- Attaques des portails d'authentification

Les étapes de l'attaque :

- Port 80 SYN Flood avec un peu d'UDP pour saturer la bande passante du réseau si possible.
- Attaquer les serveurs DNS avec des paquets UDP/TCP malformés.
- Attaquer les ports DNS des serveurs web.
- Attaquer les connexions SSL.
- Les URL (dernière tactique) passent du site principal aux sites secondaires.
- HTTP/HTTPS Post attaques (fonctions de recherche).
- Ports 80/443/53

Outils :

- Les attaquants utilisent des scripts d'attaque personnalisés qui envoient du trafic vers les ports 80, 443, 53, 1800.

Techniques adaptatives :

- Volume important (bande passante/packets), morphing constant (port/protocole).

- Personnalisation à la volée des attaques pour répondre à l'atténuation.
- Capacité à compromettre puis à utiliser des serveurs infectés par des logiciels malveillants avec des connexions à large bande passante.
- Possibilité d'ajouter aux bots et d'ajouter de nouveaux clients pour échapper aux filtres IP et aux listes noires.

Alors que les attaques de 2012-2013 étaient principalement axées sur la bande passante (couches 3 et 4), les acteurs de la menace ont modifié et fait évoluer leurs capacités pour mener des attaques plus complexes sur la couche 7. À l'aide de SSL, les acteurs de la menace ont conçu des attaques de manière à ce que le trafic d'attaque ressemble à du trafic légitime afin de camoufler leurs activités néfastes et de tromper les défenses du réseau. En outre, les attaques sont passées de cibles uniques, les attaquants "s'attardant" sur une cible pendant des heures ou des jours, à des attaques contre plusieurs USFI simultanément ou en succession rapide.

Contrôles techniques :

1. Limitation du débit du protocole de porteuse
2. Blocage de l'IP source du transporteur
3. Filtrage par trou noir de l'adresse IP ou du protocole de destination.
4. Filtrage des équilibreurs de charge à l'aide de scripts personnalisés
5. Pare-feu d'applications web sur site
6. Nettoyage de données BGP par un tiers
7. Nettoyage des données basé sur le DNS d'un tiers
8. Règles IPS
9. Blocs réseau basés sur les caractéristiques des couches 3 ou 4
10. Équipement de détection/atténuation des DDoS sur site
11. Blocage des transporteurs sur la base de la géographie de l'IP source
13. Limitation du débit de connexion
15. Filtrage sur place des paquets/sessions en fonction du temps de survie (TTL)
16. Filtrage des protocoles/ports sur place

Tendances émergentes

- L'architecture des réseaux de zombies est de plus en plus sophistiquée et difficile à repérer. Les systèmes de commande et de contrôle (C2) sont de plus en plus hiérarchisés et utilisent des serveurs proxy pour masquer l'emplacement du système qui exécute les commandes.
- Les dispositifs sont de plus en plus dispersés dans le monde entier, ce qui rend la coordination de la mise hors service de ces systèmes difficile, car les pays ont souvent des lois différentes et parfois contradictoires.
- Les réseaux de zombies sont de plus en plus sophistiqués, et certains ont la capacité d'effacer tout le disque dur d'un système compromis après avoir mené une attaque.
- Les outils DDoS sont et seront de plus en plus sophistiqués, avec des capacités multitâches et multithreads qui permettront de lancer des attaques sur plusieurs cibles et services simultanément.
- Les médias sociaux tels que Twitter pourraient potentiellement être utilisés pour rediriger et configurer les zombies comme de nouveaux vecteurs d'attaque.
- Avec la prolifération des appareils mobiles, les adversaires vont compromettre et installer des botnets et les utiliser pour mener des attaques DDoS.

- Les attaquants ont développé la capacité de surveiller activement les actions défensives et d'adapter continuellement leurs attaques pour tenter de déjouer les mesures d'atténuation. Les attaquants ont démontré leur capacité à enrichir les bots, en ajoutant de nouveaux clients pour échapper aux filtres et aux listes noires d'adresses IP.

Études de cas du sous-groupe des experts en sécurité Internet

Étude de cas n° 1 : attaque DDoS sortante/transversale lancée par des serveurs dans un centre de données Internet (IDC)

Serveurs compromis dans un IDC en raison de versions vulnérables de logiciels ; pas de root, pas de trafic usurpé.

- Vecteurs d'attaque multiples et changeants - HTTP, HTTP/S, inondations de requêtes DNS malformées ; GET via HTTP et HTTP/S consommant la bande passante de transit sortante sur les réseaux cibles. Impact collatéral sur les utilisateurs légitimes des serveurs, les opérateurs IDC, les opérateurs de réseaux de transit.

- Nombre élevé de paquets par seconde (pps) / bits par seconde (bps) par source

Étude de cas n° 2 : attaque par réflexion/amplification DNS exploitant des récurseurs DNS ouverts.

L'attaquant usurpe l'adresse IP de la cible de l'attaque, en envoyant des requêtes DNS pour de grands enregistrements DNS pré-identifiés (enregistrements ANY, grands enregistrements TXT, etc.) soit à des serveurs DNS récursifs ouverts abusifs, soit directement à des serveurs DNS faisant autorité.

L'attaquant choisit le port UDP qu'il souhaite cibler - avec le DNS, il est généralement limité à UDP/53 ou UDP/1024-65535. Le port de destination est UDP/53

Les serveurs "répondent" soit directement à la cible de l'attaque, soit aux serveurs récursifs DNS ouverts intermédiaires avec des réponses DNS volumineuses. La cible de l'attaque verra des flux de réponses DNS non sollicitées décomposées en fragments initiaux et non initiaux.

La taille de la réponse est généralement comprise entre 4096 et 8192 octets (elle peut être plus petite ou plus grande) et est divisée en plusieurs fragments.

La taille des paquets reçus par la cible de l'attaque est généralement de ~1500 octets en raison des MTU Ethernet courantes - et il y en a beaucoup.

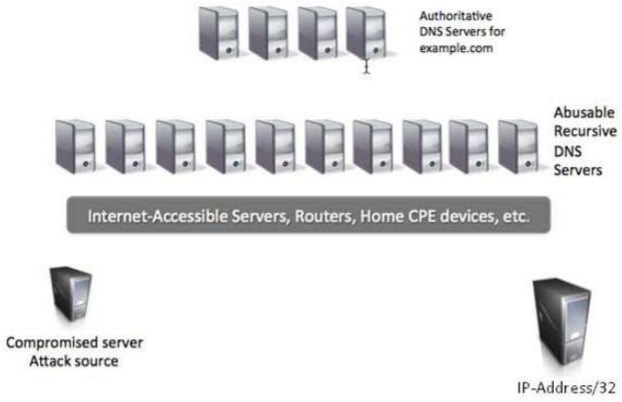
Lorsque ces multiples flux de réponses DNS fragmentées convergent, le volume de l'attaque peut être énorme - la plus grande attaque vérifiée de ce type à ce jour est de ~200gb/sec. Les attaques de 100gb/sec sont monnaie courante.

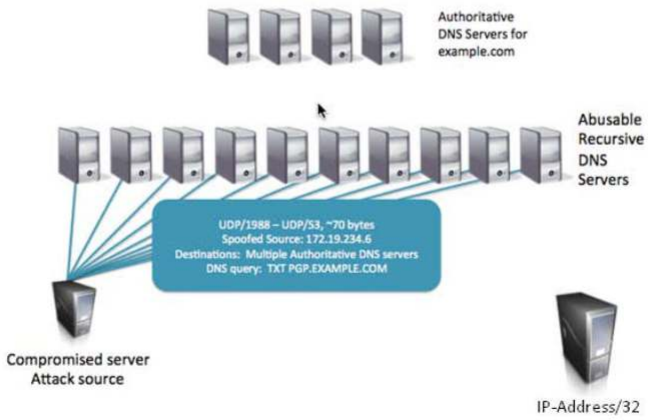
La bande passante de transit Internet de la cible, ainsi que la bande passante principale des pairs/upstreams de la cible, ainsi que la bande passante principale des réseaux intermédiaires entre les différents services DNS utilisés de manière abusive et la cible, sont saturées.

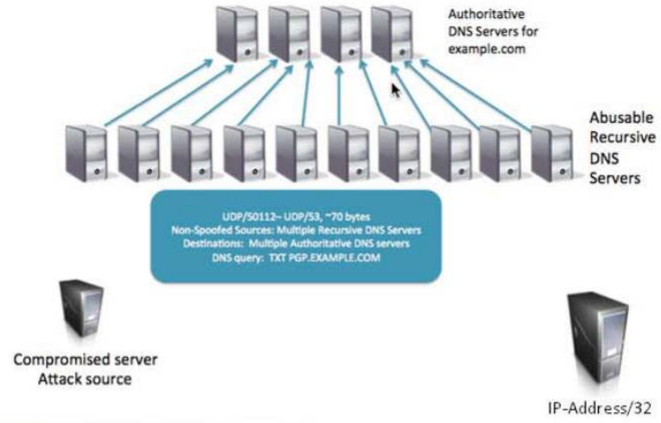
Dans la plupart des attaques impliquant des serveurs DNS récursifs ouverts intermédiaires sont des réflecteurs, entre ~20 000 et 30 000 DNS récursifs abusifs sont exploités par les attaquants. Jusqu'à 50 000 serveurs DNS récursifs ouverts abusifs ont été observés dans certaines attaques.

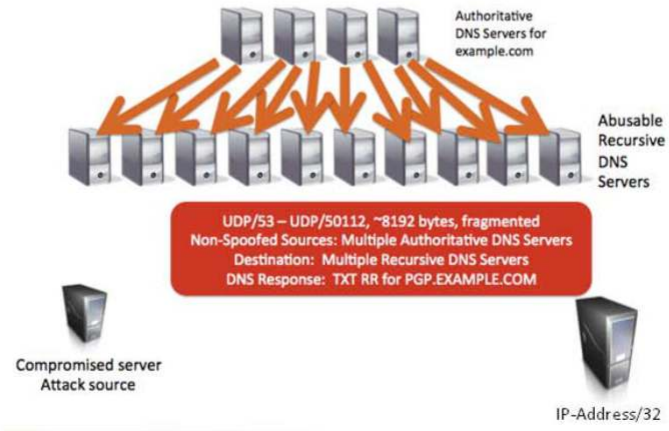
Dans les attaques exploitant directement les serveurs DNS faisant autorité, des centaines ou des milliers de ces serveurs sont utilisés par les attaquants.

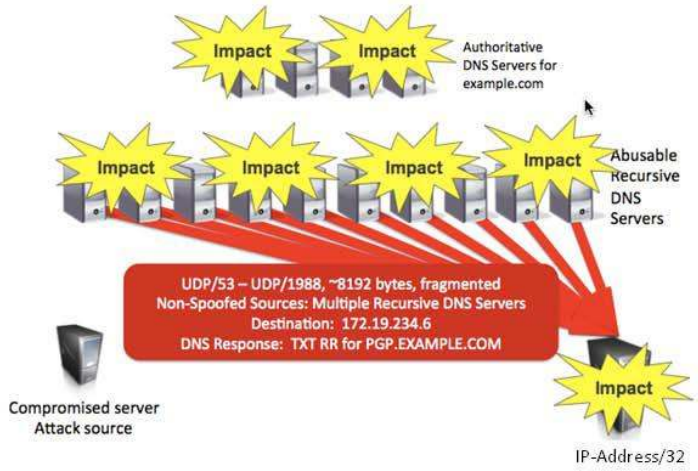
De nombreux serveurs DNS faisant autorité et bien connus sont "anycasted", avec de multiples instances déployées sur Internet.






Authoritative
DNS Servers for
example.com
Abusable
Recursive
DNS
Servers
UDP/50112– UDP/53, ~70 bytes
Non-Spoofed Sources: Multiple Recursive DNS Servers
Destinations: Multiple Authoritative DNS servers
DNS query: TXT PGP.EXAMPLE.COM
Compromised server
Attack source
IP-Address/32


Authoritative
DNS Servers for
example.com
Abusable
Recursive
DNS
Servers
UDP/53 – UDP/50112, ~8192 bytes, fragmented
Non-Spoofed Sources: Multiple Authoritative DNS Servers
Destination: Multiple Recursive DNS Servers
DNS Response: TXT RR for PGP.EXAMPLE.COM
Compromised server
Attack source
IP-Address/32



Etude de cas n°3 : Serveur Web d'un réseau d'entreprise ciblé par une attaque par réflexion/amplification ntp.

L'attaquant usurpe l'adresse IP de la cible de l'attaque, envoie monlist, showpeers ou d'autres requêtes administratives NTP de niveau 6/-7 à plusieurs services NTP abusifs fonctionnant sur des serveurs, des routeurs, des dispositifs CPE domestiques, etc.

L'attaquant choisit le port UDP qu'il souhaite cibler - généralement UDP/80 ou UDP/123, mais il peut s'agir de n'importe quel port de son choix - et l'utilise comme port source. Le port de destination est UDP/123.

Les services NTP "répondent" à la cible de l'attaque avec des flux non usurpés de paquets de 468 octets provenant de UDP/123 vers la cible ; le port de destination est le port source choisi par l'attaquant lors de la génération des requêtes NTP monlist/showpeers/etc.

Lorsque ces multiples flux de réponses NTP non usurpées convergent, le volume d'attaque peut être énorme.
- La plus grande attaque vérifiée de ce type jusqu'à présent est de plus de 400gb/sec. Les attaques à 100gb/sec sont monnaie courante.

En raison du volume des attaques, la bande passante de transit Internet de la cible, ainsi que la bande passante principale des pairs/amonts de la cible, de même que la bande passante principale des réseaux intermédiaires entre les divers services NTP utilisés abusivement et la cible, sont saturées par le trafic d'attaque non usurpé.

Dans la plupart des attaques, les attaquants exploitent entre ~4 000 et ~7 000 services NTP abusifs. Jusqu'à 50 000 services NTP ont été observés dans certaines attaques.

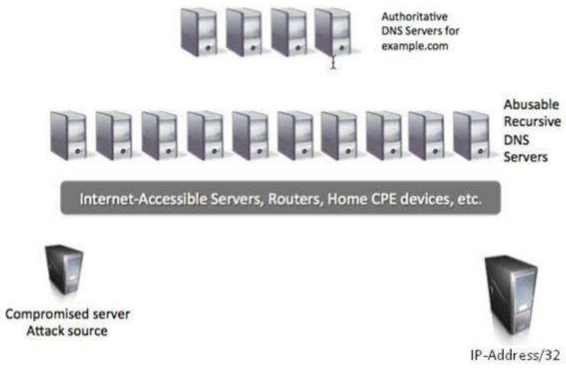
Les serveurs, les services, les applications, l'accès à l'Internet, etc. sur le réseau cible sont submergés et rendus indisponibles par le simple volume de trafic - des dizaines ou des centaines de gigaoctets par seconde fréquemment.

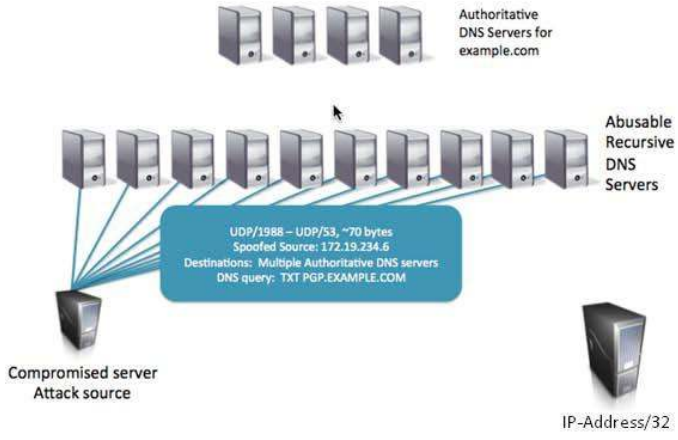
Saturation complète des liens de peering/transit du réseau cible.

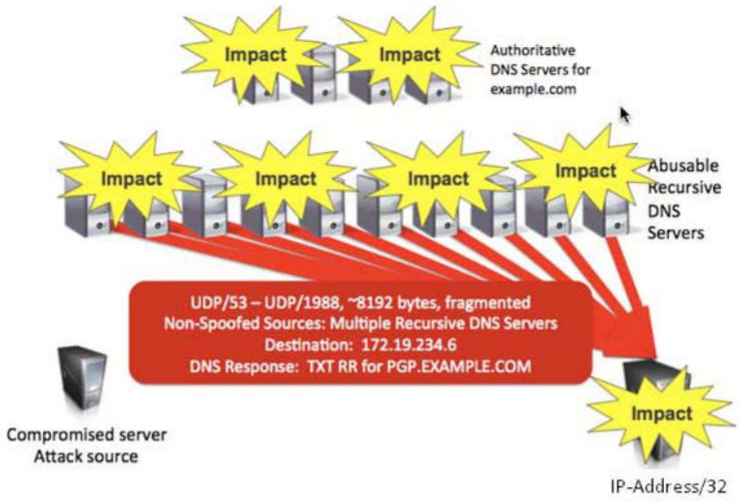
Saturation totale ou quasi-totale des liaisons de peering/liaisons de transit/liaisons de base des réseaux intermédiaires entre les réflecteurs/amplificateurs NTP et le réseau cible - y compris les réseaux des pairs/fournisseurs de transit directs du réseau cible.

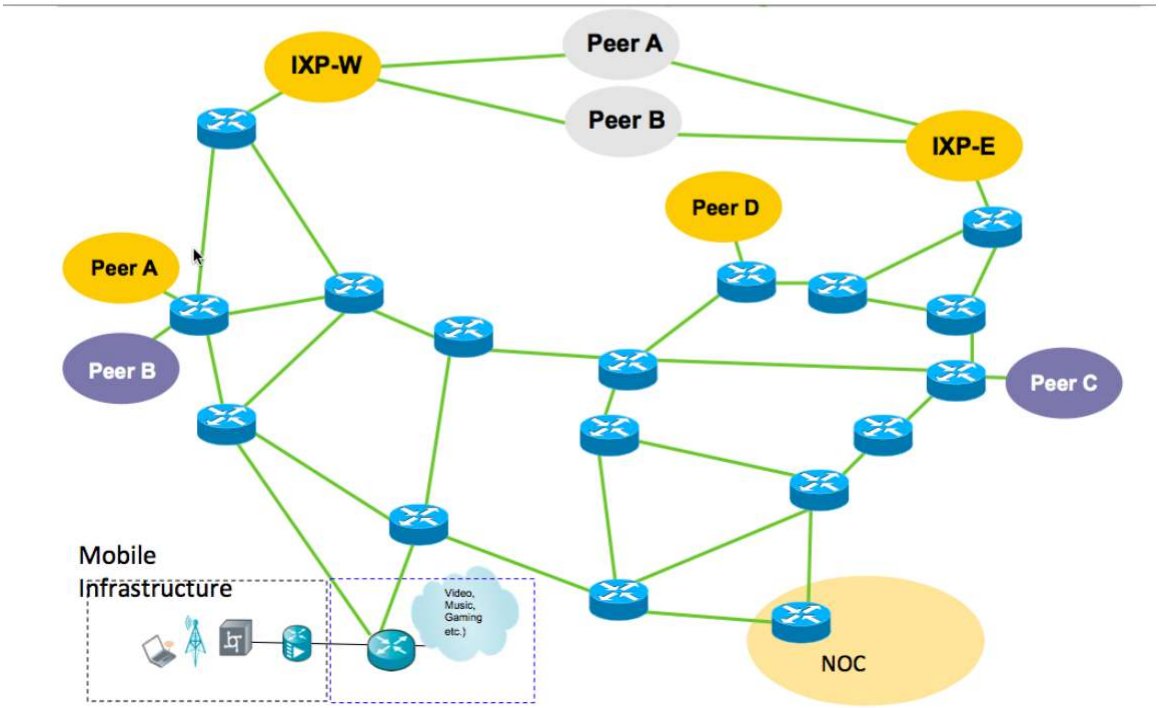
Dommages collatéraux généralisés - perte de paquets, retards, forte latence pour le trafic Internet des parties non impliquées qui se trouvent simplement à traverser des réseaux saturés par ces attaques.

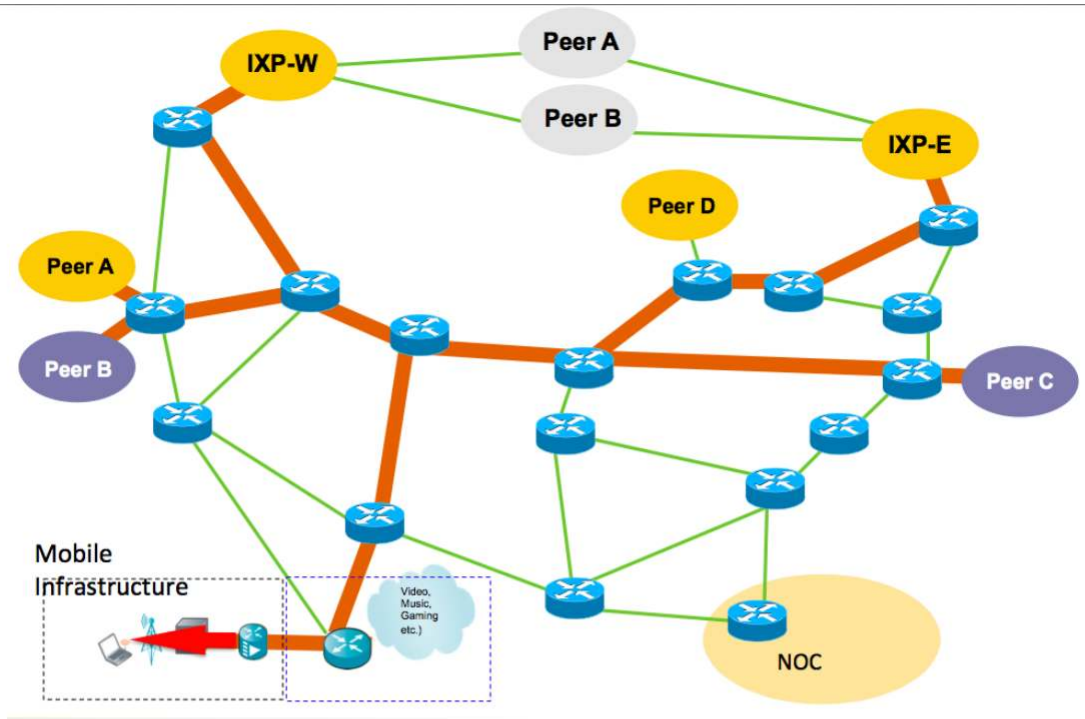
Indisponibilité des serveurs/services/applications, accès à l'Internet pour les spectateurs topologiquement proches du réseau cible.

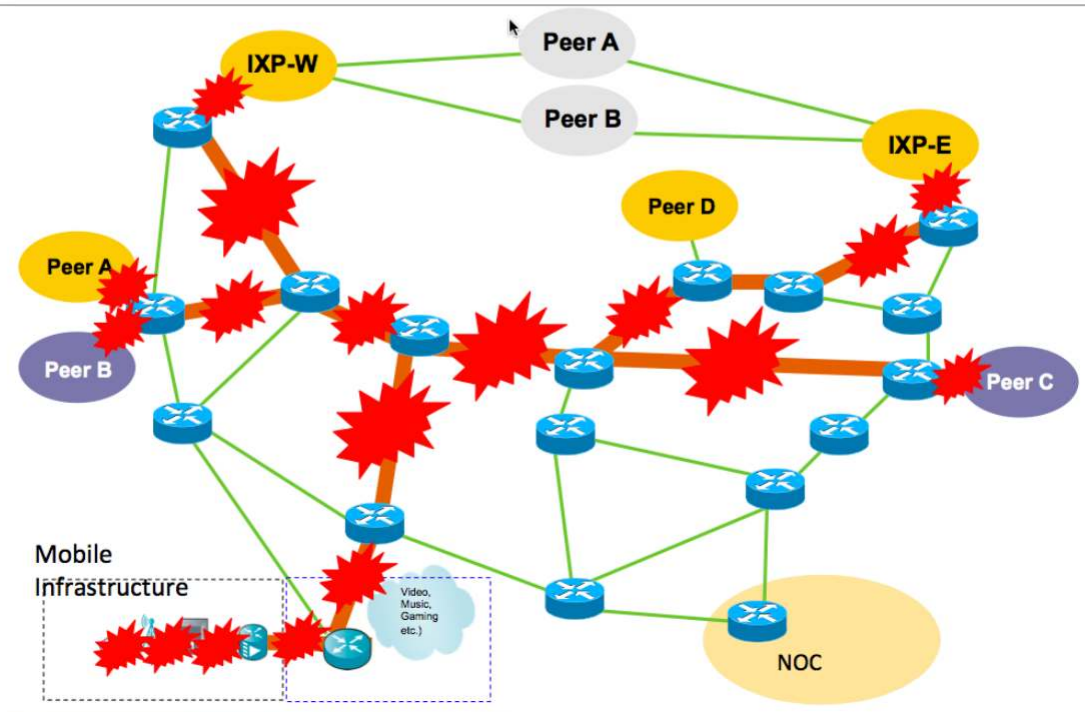

Authoritative
DNS Servers for
example.com
Abusable
Recursive
DNS
Servers
Internet-Accessible Servers, Routers, Home CPE devices, etc.
Compromised server
Attack source
IP-Address/32


Authoritative
DNS Servers for
example.com
Abusable
Recursive
DNS
Servers
UDP/1988 – UDP/53, ~70 bytes
Spoofed Source: 172.19.234.6
Destinations: Multiple Authoritative DNS servers
DNS query: TXT PGP.EXAMPLE.COM
Compromised server
Attack source
IP-Address/32


Impact
Impact
Authoritative DNS Servers for example.com
Impact
Impact
Impact
Impact
Abusable Recursive DNS Servers
UDP/53 – UDP/1988, ~8192 bytes, fragmented
Non-Spoofed Sources: Multiple Recursive DNS Servers
Destination: 172.19.234.6
DNS Response: TXT RR for PGP.EXAMPLE.COM
Impact
IP-Address/32
Compromised server
Attack source


IXP-W
Peer A
Peer B
IXP-E
Peer D
Peer A
Peer B
Peer C
Mobile Infrastructure
Video, Music, Gaming etc.)
NOC


IXP-W
Peer A
Peer B
IXP-E
Peer D
Peer A
Peer B
Peer C
Mobile
Infrastructure
Video,
Music,
Gaming
etc.)
NOC


IXP-W
Peer A
Peer B
IXP-E
Peer D
Peer A
Peer B
Peer C
Mobile
Infrastructure
Video,
Music,
Gaming
etc.)
NOC

Annexe E : Meilleures pratiques

Introduction aux meilleures pratiques

Les meilleures pratiques sont des déclarations qui décrivent les conseils que l'industrie se donne à elle-même pour trouver la meilleure approche pour répondre à une préoccupation. Elles résultent d'une coopération sans précédent de l'industrie qui engage une vaste expertise et des ressources considérables. L'objectif principal des meilleures pratiques est de fournir des conseils à partir de l'expertise et de l'expérience de l'ensemble de l'industrie. La mise en œuvre des meilleures pratiques est censée être volontaire. La décision de mettre en œuvre ou non une meilleure pratique spécifique doit être laissée à l'organisation responsable (par exemple, le fournisseur de services, l'opérateur de réseau ou le fournisseur d'équipement). En outre, l'applicabilité de chaque meilleure pratique dans une circonstance donnée dépend de nombreux facteurs qui doivent être évalués par des personnes ayant une expérience et une expertise appropriées dans le même domaine que celui visé par la meilleure pratique.

Les meilleures pratiques recommandées par le groupe de travail 5 du CSRIC IV sont destinées à donner des conseils. La décision de mettre en œuvre ou non une meilleure pratique spécifique doit être laissée à l'organisation responsable (par exemple, le fournisseur de services, l'opérateur de réseau ou le fournisseur d'équipement). La mise en œuvre obligatoire de ces meilleures pratiques n'est pas conforme à leur intention. L'application appropriée de ces bonnes pratiques ne peut être faite que par des personnes ayant une connaissance suffisante de l'architecture de l'infrastructure réseau spécifique à l'entreprise pour comprendre leurs implications. Bien que les meilleures pratiques soient rédigées de manière à être facilement comprises, leur signification n'est souvent pas évidente pour ceux qui n'ont pas cette connaissance et cette expérience préalables. Une application appropriée nécessite la compréhension de l'impact des meilleures pratiques sur les systèmes, les processus, les organisations, les réseaux, les abonnés, les opérations commerciales, les questions de coûts complexes et d'autres considérations. Compte tenu de ces considérations importantes concernant l'utilisation prévue, les parties prenantes de l'industrie craignent que les autorités gouvernementales ne les imposent de manière inappropriée en tant que règlements ou ordonnances judiciaires. Étant donné que ces meilleures pratiques ont été développées grâce à une large coopération de l'industrie qui engage une vaste expertise et des ressources volontaires considérables, une telle utilisation abusive de ces meilleures pratiques pourrait mettre en péril la volonté de l'industrie de travailler ensemble pour fournir de telles orientations à l'avenir. [29]

[29] Ces principes sont issus des travaux du groupe de discussion 3B de la NRIC VII, Rapport final sur la fiabilité du réseau public de données, sections 2.3.2 et 3.4.2.

Le WG5 a identifié les catégories suivantes pour les meilleures pratiques visant à atténuer les risques liés aux serveurs.
Les attaques DDoS :

Préparation
Identification
Classification
Traceback
Réaction
Post-mortem et récupération

Les meilleures pratiques suivantes concernent les attaques DDoS basées sur les serveurs.

Opérateurs de réseaux

Préparation

Numéro BP : Nouveau BP2
Filtrage par trou noir basé sur la destination / Filtrage par trou noir basé sur la destination déclenché à distance :
Les opérateurs de réseau doivent déployer un filtrage des trous noirs (BHF) basé sur la destination afin de protéger leurs réseaux des attaques DDoS. Les opérateurs de réseau doivent, dans la mesure du possible, fournir un filtrage des trous noirs à destination déclenché à distance (RTBHF) pour l'espace IP d'un client.
Référence BP/Commentaires :
La RFC 4778 est utile comme réponse initiale afin de contrôler l'attaque tout en vérifiant son impact et en reconfigurant le réseau.
Notez qu'une fois que le filtrage Black Hole est en place, il complète l'attaque DDoS en supprimant tout le trafic vers la destination. Le trafic vers la cible peut être repris en attribuant de nouvelles adresses IP à la cible et en annonçant les nouveaux enregistrements DNS .
Phase : Préparation (déploiement d'outils d'atténuation, opérateur réseau, filtrage de l'hébergement)
Orientation de la mise en œuvre : Efficacité (H/M/L) : H
Difficulté de mise en œuvre : (H/M/L) : M

Numéro BP : Nouveau BP8
Déployer des technologies anti-spoofing :
Les opérateurs de réseau et les fournisseurs d'hébergement doivent, dans la mesure du possible, déployer des technologies anti-spoofing pour empêcher le trafic usurpé de provenir de leurs réseaux.
Référence BP/Commentaires :
Relatif à la BP 9-7-0408
Notez que le déploiement peut ne pas être réalisable sur certains réseaux multi-hommes en raison de la nécessité d'un routage asymétrique.
Phase : Préparation (protéger, opérateur de réseau, fournisseurs d'hébergement)

Guide de mise en œuvre : Efficacité (H/M/L) :
Réseaux de maisons individuelles : H
Réseaux multi-accueils : M à L

Difficulté de mise en œuvre : (H/M/L) :
Réseaux de maisons individuelles : L
Réseaux multi-hommes : H

Numéro BP : Nouveau BP16
Déployer l'épuration des données du réseau :
Les opérateurs de réseau devraient employer, dans la mesure du possible, des centres de nettoyage des données du réseau pour filtrer le trafic d'attaque DDoS. Pour ce faire, ils peuvent "dévier" le trafic DDoS suspecté d'être une attaque vers un centre de nettoyage du réseau où le trafic d'attaque peut être filtré et "réacheminer" le trafic légitime vers la cible.

Référence BP/Commentaires :

Il est important de dimensionner la capacité du réseau et des centres d'épuration pour qu'ils puissent accueillir le trafic d'attaque, afin de minimiser les dommages collatéraux potentiels causés par de fortes hausses de trafic. Phase : Préparation (déploiement des outils d'atténuation, opérateur réseau)

Orientation de la mise en œuvre : Efficacité (H/M/L) : H

Difficulté de mise en œuvre : (H/M/L) : H

Numéro BP : 9-8-8047

Protéger contre les attaques par déni de service DNS (Domain Name System) :

Les opérateurs de réseau doivent fournir une protection DoS DNS en assurant une défense en profondeur pour prévenir les attaques qui rendraient le DNS indisponible en mettant en œuvre des techniques de protection telles que :

1) Augmenter la résilience du DNS par la redondance et des connexions réseau robustes, par exemple, déployer plusieurs serveurs avec une connectivité réseau diversifiée pour chaque service de sorte qu'un serveur ou un site n'affecte pas les autres. Déployer anycast pour améliorer la redondance de leurs serveurs DNS. Anycast peut être utilisé pour fournir un service DNS à partir d'une seule adresse IP DNS en utilisant plusieurs serveurs DNS dans le réseau, ce qui améliore la résilience du DNS. Notez qu'Anycast adresse la redondance du réseau et ne fournit pas d'équilibrage de charge entre les nœuds DNS.
2) Disposez de serveurs de noms distincts pour le trafic interne et externe ainsi que pour les infrastructures critiques, telles que les réseaux OAM&P et de signalisation/contrôle,
3) Dans la mesure du possible, séparez les serveurs DNS de mise en cache ou récursifs des serveurs DNS faisant autorité,
4) Protégez les informations DNS en protégeant les serveurs de noms maîtres à l'aide de règles de filtrage/pare-feu configurées de manière appropriée, en mettant en place des maîtres secondaires pour toutes les résolutions de noms et en utilisant des listes de contrôle d'accès pour limiter les demandes de transfert de zone aux parties autorisées.
5) Configurer l'instrumentation du réseau pour alerter les équipes d'exploitation des fournisseurs en cas de volumes de trafic anormaux.
6) Concevoir le filtrage du réseau DNS dans les architectures DNS pour permettre le filtrage au niveau du réseau et de l'application d'un trafic DNS spécifique (domaines, types de requêtes, IP sources, taux de requêtes, etc.) pendant une attaque ; ceci doit être configuré à l'avance. Cette configuration doit minimiser les interférences avec le trafic DNS légitime.
7) Disposez d'une connectivité de gestion hors bande pour les serveurs DNS afin de pouvoir gérer les serveurs pendant une attaque.
8) Séparez les serveurs DNS de mise en cache des serveurs faisant autorité.
9) N'utilisez pas de serveurs DNS tournés vers l'Internet pour les opérations du réseau interne, les systèmes d'administration, de maintenance et d'approvisionnement.
10) Fournir un serveur DNS robuste et une capacité de bande passante supérieure au trafic maximal de la connexion réseau.

Référence BP/Commentaires :

RFC-2870, ISO/IEC 15408, ISO 17799, US-CERT "Securing an Internet Name Server" (http://www.cert.org/archive/pdf/dns.pdf).

Phase : Préparation (capacité et ressources, opérateur de réseau)

Orientation de la mise en œuvre : Efficacité (H/M/L) : H

Difficulté de mise en œuvre : (H/M/L) : H

Numéro BP : 9-8-8753A - Nouveau BP (anciennement BP 9-8-8563)
Mis à jour à :
Gestion des vulnérabilités - Notification :

Lorsqu'une vulnérabilité ou un exploit DoS ou DDoS est découvert, les opérateurs de réseau, les fournisseurs d'hébergement et les vendeurs de matériel/logiciels doivent informer les propriétaires/opérateurs des systèmes concernés du problème afin de s'assurer que les logiciels, les configurations ou les équipements sont mis à jour pour remédier à la vulnérabilité. Si une correction à court terme n'est pas possible, les propriétaires/exploitants doivent envisager des mesures d'atténuation du système ou du réseau afin de minimiser la probabilité d'exploitation d'une attaque DDoS.

Référence BP/Commentaires :

Institut Sans, "Vulnerability Management : Tools, Challenges and Best Practices". 2003. Pg. 12 - 13.
Préparation (Protect) BP
Phase : Préparation (protéger, opérateur de réseau, fournisseurs d'hébergement)
Orientation de la mise en œuvre : Efficacité (H/M/L) : H
Difficulté de mise en œuvre : (H/M/L) : H

Numéro BP : 9-9-8068

Les fournisseurs de services, les opérateurs de réseaux, les fournisseurs d'hébergement, les services de sécurité publique et les fournisseurs d'équipements doivent élaborer et mettre en pratique un plan de communication dans le cadre d'un plan d'intervention plus large en cas d'incident, en identifiant les acteurs clés et en incluant autant d'éléments suivants que nécessaire : noms des personnes à contacter, numéros de téléphone professionnels, numéros de téléphone à domicile, numéros de téléavertisseur, numéros de fax, numéros de téléphone portable, adresses à domicile, adresses Internet, numéros de pont permanents, etc. Les plans de notification doivent être élaborés avant qu'un événement/incident ne se produise, si nécessaire. Le plan doit également prévoir des canaux de communication alternatifs (p. ex. téléavertisseurs alpha, Internet, téléphones satellites, VOIP, lignes privées, téléphones intelligents) en mettant en balance la valeur de toute méthode alternative et les risques de sécurité et de perte d'information introduits.

Référence BP/Commentaires :

Une autre voie de communication à large bande pour la coordination et la gestion.
Phase : Préparation (communication, opérateur de réseau, fournisseur d'hébergement)
Orientation de la mise en œuvre : Efficacité (H/M/L) : H
Difficulté de mise en œuvre : (H/M/L) : L

Numéro BP : 9-8-8753
Mis à jour à :
Gestion des vulnérabilités :

Les opérateurs de réseau, les fournisseurs d'hébergement et les vendeurs de matériel/logiciels doivent s'assurer qu'ils peuvent gérer les vulnérabilités de sécurité dans les produits qu'ils gèrent ou maintiennent pour les clients. Cette gestion peut être passive, comme la simple tenue d'une liste des clients auxquels ils ont distribué le produit, ou active, comme l'analyse et le signalement des vulnérabilités. En outre, les produits, services, matériels et logiciels doivent être testés pour détecter les vulnérabilités avant les déploiements importants.

Référence BP/Commentaires :

Institut Sans, "Vulnerability Management : Tools, Challenges and Best Practices". 2003. Pg. 12 - 13.

Préparation (Protect) BP

Phase : Préparation (protéger, opérateur de réseau, fournisseurs d'hébergement)

Orientation de la mise en œuvre : Efficacité (H/M/L) : H

Difficulté de mise en œuvre : (H/M/L) : H

Numéro BP : 9-8-8912

Communiquer la mise en œuvre de la connaissance de la situation et des mesures de protection avec les autres opérateurs de réseau :

Les opérateurs de réseau doivent faire des efforts raisonnables pour communiquer avec les autres opérateurs et les fournisseurs de logiciels de sécurité, en envoyant et/ou en recevant des rapports d'abus par des méthodes manuelles ou automatisées. Ceci est particulièrement important dans le cas d'attaques DDoS afin d'informer les sources de trafic DDoS de leur participation à l'attaque. Ce partage d'informations et cette collaboration sont nécessaires pour aider à prévenir de futures attaques. Ces efforts peuvent inclure des informations telles que la mise en œuvre de "mesures de protection" comme le signalement d'abus (par exemple, le spam) via des boucles de rétroaction (FBL) utilisant des formats de message standard tels que le format de signalement des abus (ARF). Dans la mesure du possible, les opérateurs de réseau doivent s'engager dans des efforts avec d'autres participants de l'industrie et d'autres membres de l'écosystème Internet dans le but de mettre en œuvre un partage d'informations plus robuste et normalisé dans le domaine de la détection des botnets entre les fournisseurs du secteur privé.

Référence BP/Commentaires :

Il convient de noter que la création de mécanismes de communication avec d'autres opérateurs de réseau doit avoir lieu avant l'attaque afin que des canaux de communication soient disponibles pendant l'attaque si nécessaire.

Voir le document suivant pour plus d'informations :

http://www.maawg.org/sites/maawg/files/news/CodeofConduct.pdf

Les vulnérabilités peuvent être signalées de manière standardisée en utilisant les informations fournies à l'adresse suivante

http://nvd.nist.gov/

http://puck.nether.net/mailman/listinfo/nsp-security

https://ops-trust.net/

https://www2.icsalabs.com/veris/

https://stix.mitre.org/

Phase : Préparation (communication, opérateur de réseau)

Post-mortem et récupération

Guide de mise en œuvre : Efficacité (H/M/L) : M

Difficulté de mise en œuvre : (H/M/L) : M

Notez que les meilleures pratiques de ce groupe s'adressent principalement aux ISP qui fournissent des services aux utilisateurs finaux sur des réseaux résidentiels à large bande, mais qu'elles peuvent également s'appliquer à d'autres utilisateurs et réseaux.

Numéro BP : 9-8-8917

Notification aux utilisateurs finaux :

Les opérateurs de réseaux et les fournisseurs d'hébergement devraient développer et maintenir des méthodes de notification critiques pour communiquer à leurs clients que leur ordinateur, leurs serveurs et/ou leur réseau a probablement été infecté par un logiciel malveillant. Ces méthodes devraient inclure une gamme d'options afin de s'adapter à un groupe diversifié de clients et de technologies de réseau. Une fois qu'un opérateur de réseau a détecté un problème de sécurité probable chez l'utilisateur final, des mesures doivent être prises pour informer l'internaute qu'il peut avoir un problème de sécurité. Un opérateur de réseau ou un fournisseur d'hébergement doit décider de la ou des méthodes les plus appropriées pour fournir une notification à ses clients ou utilisateurs d'Internet, et doit utiliser des méthodes supplémentaires si la méthode choisie n'est pas efficace. L'éventail des options de notification peut varier en fonction de la gravité et/ou de la criticité du problème.

Des exemples de différentes méthodes de notification peuvent inclure, sans s'y limiter, l'email, l'appel téléphonique, le courrier postal, la messagerie instantanée (IM), le service de messagerie courte (SMS) et la notification par navigateur web.

Référence BP/Commentaires :

Une décision de l'opérateur de réseau et du fournisseur d'hébergement sur la méthode ou le moyen le plus approprié. des méthodes pour fournir une notification à un ou plusieurs de leurs clients ou utilisateurs d'Internet dépend d'une série de facteurs, depuis les capacités techniques de l'opérateur de réseau, aux attributs techniques du réseau de l'opérateur de réseau, aux considérations de coût, les ressources disponibles du serveur, les ressources organisationnelles disponibles, le nombre de probables d'hôtes infectés détectés à un moment donné, ainsi que la gravité des menaces éventuelles, parmi les suivantes de nombreux autres facteurs. L'utilisation de plusieurs méthodes de notification simultanées est raisonnable. Pour un opérateur de réseau mais peut être difficile pour un faux fournisseur d'anti-virus. Notez que le
l'utilisation de notifications aveugles, c'est-à-dire de notifications sans suivi, s'est avérée être moins efficace que les méthodes qui vérifient ou exigent une action de l'utilisateur. La meilleure pratique 9-8-8921 prévoit des informations sur la manière de traiter l'infection par le logiciel malveillant.
https://otalliance.org/best-pratiques/meilleures pratiques de l'industrie
Vous trouverez de plus amples informations à l'adresse suivante
https://otalliance.org/system/files/files/resource/documents/ota_botnet_notification_whitepaper2012.pdf
Phase : Préparation (communication, opérateur de réseau, fournisseur d'hébergement)

Guide de mise en œuvre : Efficacité (H/M/L) : L
Difficulté de mise en œuvre : (H/M/L) : M

Notez que les meilleures pratiques de ce groupe s'adressent principalement aux ISP qui fournissent des services aux utilisateurs finaux sur des réseaux résidentiels à large bande, mais qu'elles peuvent également s'appliquer à d'autres utilisateurs et réseaux.

Numéro BP : 8-9-8074
Mise à jour de
Attaque par déni de service (DoS) - Cible :

Dans la mesure du possible, les opérateurs de réseaux, les fournisseurs d'hébergement, les réseaux cibles et les équipements des fournisseurs d'équipements doivent être en mesure de survivre à des augmentations significatives du nombre de paquets et de l'utilisation de la bande passante. Dans la mesure du possible, les fournisseurs d'équipements et de logiciels doivent développer des fonctions efficaces de survie aux attaques DoS/DDoS pour leurs gammes de produits.

Les infrastructures supportant les services critiques doivent être conçues pour faire face à des augmentations significatives du volume de trafic et doivent inclure des dispositifs de réseau capables de filtrer et/ou de limiter le débit du trafic. Les ingénieurs réseau doivent comprendre les capacités de ces dispositifs et savoir comment les utiliser de manière optimale. Dans la mesure du possible, les systèmes essentiels à la mission doivent être déployés dans une configuration en grappe permettant l'équilibrage de la charge du trafic excédentaire et protégés par un dispositif de protection DoS/DDoS spécialement conçu à cet effet. Les exploitants d'infrastructures critiques doivent déployer du matériel et des logiciels capables de résister aux attaques DoS chaque fois que cela est possible.

Référence BP/Commentaires :

Note : Cette meilleure pratique pourrait avoir un impact sur les opérations du 9-1-1.

Par exemple, défense contre les attaques SYN Flood, CERT/CC ® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks - http://www.cert.org/advisories/CA-1996-21.html. Lié à NRIC BP 8753A.

Il convient de noter que les opérateurs de réseau, les fournisseurs d'hébergement, les cibles et les fournisseurs d'équipements doivent déterminer quels services sont essentiels à la mise en œuvre de cette meilleure pratique.

Phase : Préparation (capacité et ressources, opérateur de réseau, fournisseur d'hébergement, cible)

Guide de mise en œuvre : Efficacité (H/M/L) : M

Difficulté de mise en œuvre : (H/M/L) : H

Numéro BP : 9-9-8725

Mis à jour à :

Protection contre le DoS de la signalisation :

Les opérateurs de réseau doivent établir des seuils d'alarme pour divers indicateurs de trafic afin de s'assurer que les conditions de DoS/DDoS sont reconnues. Les exemples incluent la comparaison des niveaux de base du trafic normal aux points clés du réseau avec les niveaux de trafic actuels, et la comparaison des informations de base du flux net pour les niveaux de trafic et les protocoles avec les niveaux de trafic actuels.

Référence BP/Commentaires :

Note : Cette meilleure pratique pourrait avoir un impact sur les opérations du 9-1-1.

Les seuils d'alarme sont destinés à reconnaître les conditions de DoS qui peuvent constituer une menace pour l'infrastructure de l'opérateur.

Phase : Préparation (Suivi & Visibilité, Opérateur de réseau)

Orientation de la mise en œuvre : Efficacité (H/M/L) : H

Difficulté de mise en œuvre : (H/M/L) : M

Numéro BP : Nouveau BP3

Sinkhole Routing :

Les opérateurs de réseaux devraient déployer le Sinkhole Routing afin d'acheminer le trafic d'attaque vers d'autres parties du réseau pour analyse (sinkholing) et abandon (offramping).

Référence BP/Commentaires :

Phase : Préparation (déploiement d'outils d'atténuation, opérateur réseau, filtrage de l'hébergement)

Guide de mise en œuvre : Efficacité (H/M/L) : M

Difficulté de mise en œuvre : (H/M/L) : H

RFC 4778 peut être utilisé avec Anycast pour fournir une redondance.

Numéro BP : Nouveau BP4
Filtrage des trous noirs à la source :

Les opérateurs de réseau devraient déployer le SBBHF (Source Based Black Hole Filtering) ou des mécanismes dynamiques similaires qui déclenchent un filtrage à l'échelle du réseau sur la base des informations de l'en-tête du paquet source afin de protéger leurs réseaux des attaques DDoS. Notez que cela peut ne pas être aussi efficace si un grand nombre d'adresses IP sources sont utilisées dans l'attaque, par exemple une attaque de botnet, ou si le trafic d'attaque utilise des adresses IP usurpées pour l'obscurcissement.

Référence BP/Commentaires :

Greene, Barry Raveendran. "Phase 1 - Préparer les outils et les techniques, utiliser le routage IP comme outil de sécurité". ISP Security Bootcamp Singapore 2003. 31 juillet 2003 ftp://ftp-eng.cisco.com/cons/isp/security/ISP-Security-Bootcamp-Singapore-2003/H-Preparation-Tools-v3-0.pdf

Phase : Préparation (déploiement d'outils d'atténuation, opérateur réseau, filtrage de l'hébergement)

Guide de mise en œuvre : Efficacité (H/M/L) : M

Difficulté de mise en œuvre : (H/M/L) : M

Numéro BP : Nouveau BP5
Déployer la distribution automatique des filtres de trafic :

Les opérateurs de réseau devraient déployer des systèmes, tels que BGP Flowspec, qui distribuent automatiquement des filtres de trafic aux appareils concernés en cas d'attaque DOS/DDoS. Ces systèmes peuvent permettre de filtrer le trafic d'attaque vers une cible (scrubbed) tout en laissant passer le trafic légitime.

Référence BP/Commentaires :

RFC 5575, RFC 4360

Phase : Préparation (déploiement d'outils d'atténuation, opérateur réseau, filtrage de l'hébergement)

Orientation de la mise en œuvre : Efficacité (H/M/L) : H

Difficulté de mise en œuvre : (H/M/L) : H

Notez qu'actuellement, tous les fournisseurs de routeurs ne prennent pas en charge cette technologie.

Numéro BP : Nouveau BP9
Hiérarchisation du trafic pour garantir que le trafic critique, par exemple le plan de contrôle, ne soit pas affecté par une attaque DDOS basée sur un serveur :

Les opérateurs de réseau doivent donner la priorité au trafic du plan de contrôle et aux autres trafics critiques sur le trafic de transit afin de s'assurer que le trafic des attaques DDoS n'a pas d'impact sur le fonctionnement du protocole de routage.

Référence BP/Commentaires :

Phase : Préparation (capacité et ressources, opérateur de réseau)

Orientation de la mise en œuvre : Efficacité (H/M/L) : H

Difficulté de mise en œuvre : (H/M/L) : M

Numéro BP : Nouveau BP14
Empêcher les services DNS d'être utilisés dans les attaques par réflexion :

Les opérateurs de réseaux doivent appliquer des protections pour empêcher que leurs services DNS ne soient

utilisées dans le cadre d'une attaque par réflexion, si possible. Ces protections peuvent inclure, mais ne sont pas limitées à :

1. Limitez les serveurs DNS récursifs pour qu'ils ne répondent qu'aux requêtes provenant du plus petit ensemble pratique de sous-réseaux IP requis pour le service.
2. Mettre en œuvre des processus d'instrumentation et d'alarme pour détecter les domaines, les IP et les serveurs utilisés de manière abusive dans une attaque.
3. Configurez des contrôles pour permettre l'atténuation d'attaques spécifiques telles que des limites de taux de requête, la suppression de domaines spécifiques ou le filtrage de types de requêtes qui peuvent être appliqués lorsqu'une attaque est détectée.
4. Disposer d'une capacité de détection et de réponse aux anomalies du trafic.
5. Déployer des systèmes de validation du protocole DNS, le cas échéant, afin d'éliminer le trafic DNS illégitime ou malveillant.

Référence BP/Commentaires :

Cette BP remplace la BP 9-8-8118

Il convient de noter qu'étant donné que le nombre de serveurs DNS sous le contrôle de l'opérateur de réseau est faible par rapport au nombre total de serveurs DNS déployés, l'impact de la mise en œuvre de cette meilleure pratique uniquement par les opérateurs de réseau sur le problème global des serveurs DNS ouverts utilisés dans les attaques par réflexion est faible.

Phase : Préparation (protéger, opérateur de réseau, capacité et ressources, opérateur de réseau)

Guide de mise en œuvre : Efficacité (H/M/L) : L

Difficulté de mise en œuvre : (H/M/L) : M

Identification

Numéro BP : 9-8-8916

Mis à jour à :

La détection des robots et la notification correspondante doivent être effectuées en temps utile :

Les opérateurs de réseau et les fournisseurs d'hébergement doivent veiller à ce que la détection des bots et la notification correspondante aux clients hébergeurs se fassent en temps utile, car ces problèmes de sécurité sont sensibles au facteur temps. Si une analyse complexe est nécessaire et que plusieurs confirmations sont requises pour confirmer la présence d'un bot, il est possible que le malware cause des dommages, soit à l'hôte infecté, soit au système ciblé à distance (au-delà des dommages causés par l'infection initiale) avant de pouvoir être arrêté. Ainsi, un opérateur de réseau ou un fournisseur d'hébergement doit trouver un équilibre entre le désir de confirmer définitivement une infection par un logiciel malveillant, ce qui peut prendre un certain temps, et la capacité de prédire la forte probabilité d'une infection par un logiciel malveillant dans un laps de temps très court. Ce défi "définitif vs. probable" est difficile à relever et, dans le doute, les opérateurs de réseau et les fournisseurs d'hébergement devraient pécher par excès de prudence en communiquant une infection probable par un logiciel malveillant tout en prenant des mesures raisonnables pour éviter les notifications faussement positives.

Référence BP/Commentaires :

La mise en œuvre de la notification par l'opérateur de réseau doit équilibrer la certitude d'une infection détectée et l'incertitude d'une détection transitoire de trafic malveillant afin de minimiser la possibilité de notifications faussement positives qui pourraient devenir une gêne pour les clients et devenir ingérables par l'opérateur de réseau.

Pour plus d'informations, voir le Code de conduite anti-bots (ABC) des États-Unis pour les services Internet.
fournisseurs d'accès Internet (FAI) :
http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

Phase : Identification (Surveillance et Visibilité, Opérateur de réseau, Fournisseur d'hébergement)
Guide de mise en œuvre : Efficacité (H/M/L) : L (notification uniquement)
Difficulté de mise en œuvre : (H/M/L) : M

Notez que les meilleures pratiques de ce groupe s'adressent principalement aux ISP qui fournissent des services aux utilisateurs finaux sur des réseaux résidentiels à large bande, mais qu'elles peuvent également s'appliquer à d'autres utilisateurs et réseaux.

Numéro BP : Nouveau BP6
Utiliser l'analyse des données Netflow pour analyser les attaques DDoS :

Dans la mesure du possible, les opérateurs de réseau et les fournisseurs d'hébergement doivent permettre, collecter et analyser les données Netflow afin de faciliter l'identification et la classification des attaques DDoS. Les données doivent être disponibles après l'attaque pour permettre une analyse plus approfondie. Les données Netflow doivent être conservées conformément à la politique de conservation des données de l'opérateur de réseau.

Référence BP/Commentaires :

Les données Netflow peuvent être utiles pour identifier les attaques de type spoofing.
Phase : Identification (surveillance et visibilité, opérateur de réseau, fournisseurs d'hébergement)
Orientation de la mise en œuvre : Efficacité (H/M/L) : H
Difficulté de mise en œuvre : (H/M/L) : M

Numéro BP : 9-8-8913
Maintenir les méthodes de détection d'une infection par un bot/malware :

Les exploitants de réseaux doivent disposer de méthodes permettant de détecter l'infection probable des équipements des clients par des logiciels malveillants. Les méthodes de détection peuvent varier considérablement en raison d'une série de facteurs. Les méthodes, outils et processus de détection peuvent comprendre, sans s'y limiter, les éléments suivants : retour d'information externe, observation des conditions et du trafic du réseau, comme l'analyse de la bande passante et/ou des schémas de trafic, les signatures, les techniques comportementales et la surveillance judiciaire des clients à un niveau plus détaillé.

Référence BP/Commentaires :

Vous trouverez de plus amples informations à l'adresse suivante
http://teamcymru.org
http://shadowserver.org
http://abuse.ch
http://cbl.abuseat.org
Code de conduite anti-robot américain (ABC) pour les fournisseurs de services Internet (ISP) :
http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

Notez que les meilleures pratiques de ce groupe s'adressent principalement aux ISP qui fournissent des services aux utilisateurs finaux sur des réseaux résidentiels à large bande, mais qu'elles peuvent également s'appliquer à d'autres utilisateurs et réseaux.
Phase : Identification (surveillance et visibilité, opérateur de réseau)
Guide de mise en œuvre : Efficacité (H/M/L) : M

Difficulté de mise en œuvre : (H/M/L) : H

Numéro BP : 9-8-8914
Utilisez une approche de détection des robots à plusieurs niveaux :

Les opérateurs de réseau doivent utiliser une approche par paliers pour la détection des botnets, en appliquant d'abord les caractéristiques comportementales du trafic utilisateur (en ratissant large), puis en appliquant des techniques plus granulaires (par exemple, la détection de signatures) au trafic signalé comme un problème potentiel.

Référence BP/Commentaires :

Cette technique devrait permettre de minimiser l'exposition des informations relatives aux clients lors de la détection des bots en ne collectant pas d'informations détaillées avant qu'il soit raisonnable de penser que le client est infecté.

L'examen du trafic des utilisateurs à l'aide d'une approche large peut inclure un retour d'information externe ainsi que d'autres approches internes.

Cette approche est utile pour limiter le recours à des outils plus sophistiqués tels que l'inspection approfondie des paquets et les signatures. Une fois que le trafic de robots malveillants est suspecté (un large filet), une analyse plus détaillée du trafic peut être effectuée.

Pour plus d'informations, voir le Code de conduite anti-bots (ABC) des États-Unis pour les services Internet.
fournisseurs d'accès Internet (FAI) :
http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf
Phase : Identification (surveillance et visibilité, opérateur de réseau)
Guide de mise en œuvre : Efficacité (H/M/L) : M
Difficulté de mise en œuvre : (H/M/L) : H

Notez que les meilleures pratiques de ce groupe s'adressent principalement aux ISP qui fournissent des services aux utilisateurs finaux sur des réseaux résidentiels à large bande, mais qu'elles peuvent également s'appliquer à d'autres utilisateurs et réseaux.

Classification

Numéro BP : Nouveau BP 18
Classifier les attaques DoS/DDoS :

Les opérateurs de réseau, les fournisseurs d'hébergement et les cibles DDoS doivent, dans la mesure du possible, disposer de processus et/ou de capacités permettant d'analyser et de classer une attaque DoS/DDoS. La classification des attaques peut aider à déterminer les meilleures mesures d'atténuation de l'attaque et à identifier les améliorations nécessaires pour assurer une protection future.

Référence BP/Commentaires :

Exemple de classification :
Attaque volumétrique ?
- Envoi direct de paquets
- Réflexion/Amplification

Attaque de la couche d'application ?
Attaque par épuisement de l'état ou des ressources ?
Attaque de l'avion de contrôle ?
Attaque spécifique Ipv6 ?

Date ?

Phase : Classification (type d'attaque, opérateur réseau, fournisseur d'hébergement, cible), post-mortem et récupération (opérateur réseau, fournisseur d'hébergement, cible).

Guide de mise en œuvre : Efficacité (H/M/L) : M

Difficulté de mise en œuvre : (H/M/L) : H

Traceback

Numéro BP : 9-8-0507 :
Remontée de l'attaque :

Les opérateurs de réseau doivent disposer de processus et/ou de capacités permettant d'analyser et de déterminer la source du trafic malveillant, puis de remonter et de supprimer les paquets à la source ou plus près de celle-ci. Les références fournissent plusieurs techniques différentes possibles. (Le trafic malveillant est le trafic tel que les attaques par déni de service distribué (DDoS), les attaques de type smurf et fraggle, conçues et transmises dans le but de consommer les ressources d'un réseau de destination afin de bloquer le service ou de consommer les ressources jusqu'à un état de dépassement qui pourrait provoquer des pannes de système).

Référence BP/Commentaires :

"Practical Network Support for IP Trace back" par Stefan Savage et.al., Dept. of Computer Science and Engineering, Univ of Washington, Tech Report UW-CSE-2000-02-01 avec une version publiée dans les Proceedings of the 2000 ACM SIBCOMM pp256-306 Stockholm, Sweden, August 2000.

Phase : Traceback (opérateurs de réseau)

Orientation de la mise en œuvre : Efficacité (H/M/L) : H

Difficulté de mise en œuvre : (H/M/L) : H

Réaction

Numéro BP : 9-9-8065

Les opérateurs de réseau et les fournisseurs d'hébergement doivent établir une procédure de communication des informations aux membres des forces de l'ordre et désigner un point de contact (POC) pour les activités de coordination.

Référence BP/Commentaires :

Aucun.

Phase : Réaction (opérateur de réseau, fournisseurs d'hébergement)

Guide de mise en œuvre : Efficacité (H/M/L) : L

Difficulté de mise en œuvre : (H/M/L) : L

Post-mortem et récupération

Numéro BP : 9-9-8762
Récupérer après une attaque DoS :
Mis à jour à :
Les opérateurs de réseau et les fournisseurs d'hébergement doivent, dans la mesure du possible, coopérer avec d'autres opérateurs de réseau et fournisseurs d'hébergement.
pendant et après des cyberincidents importants, afin de partager des informations sur les mesures à prendre.
pour caractériser l'attaque, sur les techniques permettant d'identifier, de filtrer et d'isoler l'origine de l'attaque.
de l'attaque, et sur les mesures prises pour réacheminer le trafic légitime et pour dissuader ou se défendre contre des attaques DoS similaires.
Référence BP/Commentaires :
IETF RFC2350, CMU/SEI-98-HB-001. Remarque : Cette meilleure pratique pourrait avoir un impact sur le 9-1-1.
opérations.
Mis à jour pour ajouter :
Cette meilleure pratique vise à la récupération de l'infrastructure de l'opérateur après une attaque DoS. Phase : Réaction (Opérateur réseau, fournisseurs d'hébergement) ; Post Mortem (Opérateur réseau, fournisseurs d'hébergement).
Guide de mise en œuvre : Efficacité (H/M/L) : M
Difficulté de mise en œuvre : (H/M/L) : M

Numéro BP : 9-8-8515
Mis à jour à :
Récupération en cas de mauvaise utilisation ou de consommation indue des ressources du système :
En cas de détection d'une mauvaise utilisation ou d'une utilisation non autorisée d'un système sous leur contrôle (par exemple, la détection d'une participation à une attaque DDoS), les opérateurs de réseau, les fournisseurs d'hébergement ou les cibles doivent, dans la mesure du possible, effectuer une analyse médico-légale du système, réaliser une analyse post-mortem, appliquer des contrôles pour empêcher de futures attaques et/ou faire respecter les quotas de ressources du système.
Référence BP/Commentaires :
IETF RFC2350, CMU/SEI-98-HB-001.
Phase : Post-mortem (opérateur réseau, hébergeur, cible)
Guide de mise en œuvre : Efficacité (H/M/L) : M
Difficulté de mise en œuvre : (H/M/L) : H

Fournisseurs d'hébergement

Préparation

Numéro BP : Nouveau BP10
Mettre régulièrement à jour la technologie avec les mises à jour de sécurité ou les nouvelles versions fournies par
Vendeurs :

Les fournisseurs d'hébergement doivent prendre des mesures raisonnables pour fournir des logiciels et des plug-ins à jour à leurs clients (dans les cas où les fournisseurs d'hébergement proposent des logiciels). Les logiciels fournis aux clients doivent faire l'objet d'un support actif de la part du fournisseur pour les correctifs de sécurité. Des outils, processus ou instructions de mise à jour doivent être fournis aux clients pour les aider à maintenir leurs logiciels à jour avec les correctifs de sécurité. Dans la mesure du possible, choisissez des logiciels qui fournissent des mises à jour de sécurité automatiques et fournissez aux clients des instructions sur la manière d'activer les mises à jour.

Référence BP/Commentaires :

TBD
Phase : Préparation (protection, fournisseur d'hébergement)

Guide de mise en œuvre : Efficacité (H/M/L) : H
Difficulté de mise en œuvre : (H/M/L) : H

Numéro BP : 9-8-8753 (répété depuis la section des opérateurs de réseau)
Mis à jour à :
Gestion des vulnérabilités :

Les opérateurs de réseau, les fournisseurs d'hébergement et les vendeurs de matériel/logiciels doivent s'assurer qu'ils peuvent gérer les vulnérabilités de sécurité dans les produits qu'ils gèrent ou maintiennent pour les clients. Cette gestion peut être passive, comme la simple tenue d'une liste des clients auxquels ils ont distribué le produit, ou active, comme l'analyse et le signalement des vulnérabilités. En outre, les produits, services, matériels et logiciels doivent être testés pour détecter les vulnérabilités avant les déploiements importants.

Référence BP/Commentaires :

Institut Sans, "Vulnerability Management : Tools, Challenges and Best Practices". 2003. Pg. 12 - 13.
Préparation (Protect) BP
Phase : Préparation (protéger, opérateur de réseau, fournisseurs d'hébergement)
Orientation de la mise en œuvre : Efficacité (H/M/L) : H
Difficulté de mise en œuvre : (H/M/L) : H

Numéro de BP : 9-8-8753A - Nouveau BP (anciennement BP 9-8-8563) (repris de la section des opérateurs de réseau)
Mis à jour à :
Gestion des vulnérabilités - Notification :

Lorsqu'une vulnérabilité ou un exploit DoS ou DDoS est découvert, les opérateurs de réseau, les fournisseurs d'hébergement et les vendeurs de matériel/logiciels doivent informer les propriétaires/opérateurs des systèmes concernés du problème afin de s'assurer que les logiciels, les configurations ou les équipements sont mis à jour pour

remédier à la vulnérabilité. Si la correction à court terme n'est pas possible, les propriétaires/exploitants doivent envisager des mesures d'atténuation du système ou du réseau afin de minimiser la probabilité d'exploitation d'une attaque DDoS.

Référence BP/Commentaires :

Institut Sans, "Vulnerability Management : Tools, Challenges and Best Practices". 2003. Pg. 12 - 13.

Préparation (Protect) BP

Phase : Préparation (protéger, opérateur de réseau, fournisseurs d'hébergement)

Orientation de la mise en œuvre : Efficacité (H/M/L) : H

Difficulté de mise en œuvre : (H/M/L) : H

Numéro BP : 9-8-8917 (répété depuis la section des opérateurs de réseau)

Notification aux utilisateurs finaux :

Les opérateurs de réseaux et les fournisseurs d'hébergement devraient développer et maintenir des méthodes de notification critiques pour communiquer à leurs clients que leur ordinateur, leurs serveurs et/ou leur réseau a probablement été infecté par un logiciel malveillant. Ces méthodes devraient inclure une gamme d'options afin de s'adapter à un groupe diversifié de clients et de technologies de réseau. Une fois qu'un opérateur de réseau a détecté un problème de sécurité probable chez l'utilisateur final, des mesures doivent être prises pour informer l'internaute qu'il peut avoir un problème de sécurité. Un opérateur de réseau ou un fournisseur d'hébergement doit décider de la ou des méthodes les plus appropriées pour fournir une notification à ses clients ou utilisateurs d'Internet, et doit utiliser des méthodes supplémentaires si la méthode choisie n'est pas efficace. L'éventail des options de notification peut varier en fonction de la gravité et/ou de la criticité du problème.

Des exemples de différentes méthodes de notification peuvent inclure, sans s'y limiter, l'email, l'appel téléphonique, le courrier postal, la messagerie instantanée (IM), le service de messagerie courte (SMS) et la notification par navigateur web.

Référence BP/Commentaires :

Une décision de l'opérateur de réseau et du fournisseur d'hébergement sur la méthode ou le moyen le plus approprié. des méthodes pour fournir une notification à un ou plusieurs de leurs clients ou utilisateurs d'Internet dépend d'une série de facteurs, depuis les capacités techniques de l'opérateur de réseau, aux attributs techniques du réseau de l'opérateur de réseau, aux considérations de coût, les ressources disponibles du serveur, les ressources organisationnelles disponibles, le nombre de probables d'hôtes infectés détectés à un moment donné, ainsi que la gravité des menaces éventuelles, parmi les suivantes de nombreux autres facteurs. L'utilisation de plusieurs méthodes de notification simultanées est raisonnable. Pour un opérateur de réseau mais peut être difficile pour un faux fournisseur d'anti-virus. Notez que le l'utilisation de notifications aveugles, c'est-à-dire de notifications sans suivi, s'est avérée être moins efficace que les méthodes qui vérifient ou exigent une action de l'utilisateur. La meilleure pratique 9-8-8921 prévoit des informations sur la manière de traiter l'infection par le logiciel malveillant.

https://otalliance.org/best-pratiques/meilleures pratiques de l'industrie

Vous trouverez de plus amples informations à l'adresse suivante

https://otalliance.org/system/files/files/resource/documents/ota_botnet_notification_whitepaper2012.pdf

Phase : Préparation (communication, opérateur de réseau, fournisseur d'hébergement)

Guide de mise en œuvre : Efficacité (H/M/L) : L

Difficulté de mise en œuvre : (H/M/L) : M

Notez que les meilleures pratiques de ce groupe s'adressent principalement aux ISP qui fournissent des services aux utilisateurs finaux sur des réseaux résidentiels à large bande, mais qu'elles peuvent également s'appliquer à d'autres utilisateurs et réseaux.

Numéro BP : 9-8-8901

Mis à jour à :

Fournisseurs d'hébergement Soutien aux ressources éducatives pour l'hygiène informatique / la sécurité informatique :

Les fournisseurs d'hébergement doivent fournir, mettre à disposition, identifier ou soutenir des ressources tutorielles, éducatives et d'auto-assistance tierces pour leurs clients afin de les sensibiliser à l'importance de la sécurité informatique et de les aider à la pratiquer. Les clients des fournisseurs d'hébergement doivent savoir comment protéger les appareils et les réseaux des utilisateurs finaux contre les accès non autorisés par le biais de diverses méthodes, y compris, mais sans s'y limiter :

1) Utilisez un logiciel de sécurité légitime qui protège contre les virus et les logiciels espions ;
2) Assurez-vous que tout téléchargement ou achat de logiciel provient d'une source légitime ;
3) Utilisez des pare-feu ;
4) Maintenir à jour les correctifs de sécurité du système d'exploitation, des bases de données, des applications et des plug-ins d'application ;
5) Sensibiliser les clients à l'importance de la gestion et de l'analyse des vulnérabilités.
6) Supprimez et cessez d'utiliser les logiciels qui ne sont pas mis à jour avec des correctifs de sécurité ;
7) Analysez régulièrement les serveurs pour détecter les logiciels malveillants, les logiciels espions et autres logiciels potentiellement indésirables ;
8) Maintenez toutes les applications, les plug-ins d'application et les logiciels du système d'exploitation à jour et utilisez leurs fonctions de sécurité ;
9) Utilisez des mots de passe forts et/ou une authentification à 2 facteurs ; et
10) Ne partagez jamais vos mots de passe.
11) Fournir les coordonnées des personnes à contacter pour signaler les problèmes.

Référence BP/Commentaires :

Vous trouverez de plus amples informations à l'adresse suivante

National Cyber Security Alliance - http://www.staysafeonline.org/
OnGuard Online - http://www.onguardonline.gov/default.aspx
Département de la sécurité intérieure -

StopBadware - http://www.stopbadware.org/home/badware_prevent
Comcast.net Security - http://security.comcast.net/ Verizon Safety & Security
-

http://www.verizon.net/central/vzc.portal?_nfpb=X&_pageLabel=vzc_help_safety Site
Qwest Incredible Internet Security : http://www.incredibleinternet.com/ Microsoft-
http://www.microsoft.com/security/pypc.aspx Phase : Préparation (éducation, fournisseurs d'hébergement)

Guide de mise en œuvre : Efficacité (H/M/L) : L

Difficulté de mise en œuvre : (H/M/L) : L

Notez que les meilleures pratiques de ce groupe s'adressent principalement aux ISP qui fournissent des services aux utilisateurs finaux sur des réseaux résidentiels à large bande, mais qu'elles peuvent également s'appliquer à d'autres utilisateurs et réseaux.

Numéro BP : 9-9-8068 (répété depuis la section des opérateurs de réseau)

Les fournisseurs de services, les opérateurs de réseaux, les fournisseurs d'hébergement, les services de sécurité publique et les fournisseurs d'équipements doivent élaborer et mettre en pratique un plan de communication dans le cadre d'un plan d'intervention plus large en cas d'incident, en identifiant les acteurs clés et en incluant autant d'éléments suivants que nécessaire : noms des personnes à contacter, numéros de téléphone professionnels, numéros de téléphone à domicile, numéros de téléavertisseur, numéros de fax, numéros de téléphone portable, adresses à domicile, adresses Internet, numéros de pont permanents, etc. Les plans de notification doivent être élaborés avant qu'un événement/incident ne se produise, si nécessaire. Le plan doit également prévoir des canaux de communication alternatifs (p. ex. téléavertisseurs alpha, Internet, téléphones satellites, VOIP, lignes privées, téléphones intelligents) en mettant en balance la valeur de toute méthode alternative et les risques de sécurité et de perte d'information introduits.

Référence BP/Commentaires :

Une autre voie de communication à large bande pour la coordination et la gestion.
Phase : Préparation (communication, opérateur de réseau, fournisseur d'hébergement)

Orientation de la mise en œuvre : Efficacité (H/M/L) : H

Difficulté de mise en œuvre : (H/M/L) : L

Numéro BP : 8-9-8074 (répété depuis la section des opérateurs de réseau)
Mise à jour de
Attaque par déni de service (DoS) - Cible : (Repris de la section Opérateur de réseau)

Dans la mesure du possible, les opérateurs de réseaux, les fournisseurs d'hébergement, les réseaux cibles et les équipements des fournisseurs d'équipements doivent être capables de survivre à des augmentations significatives du nombre de paquets et de l'utilisation de la bande passante. Dans la mesure du possible, les fournisseurs d'équipements et de logiciels doivent développer des fonctions efficaces de survie aux attaques DoS/DDoS pour leurs gammes de produits. L'infrastructure soutenant les services critiques doit être conçue pour faire face à des augmentations significatives du volume de trafic et doit inclure des dispositifs de réseau capables de filtrer et/ou de limiter le trafic. Les ingénieurs réseau doivent comprendre les capacités de ces dispositifs et savoir comment les utiliser de manière optimale. Dans la mesure du possible, les systèmes essentiels à la mission doivent être déployés dans une configuration en grappe permettant l'équilibrage de la charge du trafic excédentaire et protégés par un dispositif de protection DoS/DDoS spécialement conçu à cet effet. Les exploitants d'infrastructures critiques doivent déployer du matériel et des logiciels capables de résister aux attaques DoS chaque fois que cela est possible.

Référence BP/Commentaires :

Note : Cette meilleure pratique pourrait avoir un impact sur les opérations du 9-1-1.

Par exemple, défense contre les attaques SYN Flood, CERT/CC ® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks - http://www.cert.org/advisories/CA-1996-21.html. Lié à NRIC BP 8753A.

Il convient de noter que les opérateurs de réseau, les fournisseurs d'hébergement, les cibles et les fournisseurs d'équipements doivent déterminer quels services sont essentiels à la mise en œuvre de cette meilleure pratique.

Phase : Préparation (capacité et ressources, opérateur de réseau, fournisseur d'hébergement, cible)

Guide de mise en œuvre : Efficacité (H/M/L) : M

Difficulté de mise en œuvre : (H/M/L) : H

Numéro de BP : Nouveau BP8 (repris de la section "opérateur de réseau")

Déployer des technologies anti-spoofing :

Les opérateurs de réseaux et les fournisseurs d'hébergement devraient, dans la mesure du possible, déployer des technologies anti-spoofing pour empêcher le trafic usurpé de provenir de leurs réseaux.

Référence BP/Commentaires :

Relatif à la BP 9-7-0408

Notez que le déploiement peut ne pas être réalisable sur certains réseaux multi-hommes en raison de la nécessité d'un routage asymétrique.

Phase : Préparation (protéger, opérateur de réseau, fournisseurs d'hébergement)

Guide de mise en œuvre : Efficacité (H/M/L):H

Difficulté de mise en œuvre : (H/M/L) :

Réseaux de maisons individuelles : L

Réseaux multi-hommes : H

Numéro BP : Nouveau BP1

Protection des réseaux basée sur les applications :

Les fournisseurs d'hébergement et les sources d'attaques doivent envisager d'utiliser des systèmes de détection d'intrusion basés sur l'application et/ou l'hôte, des pare-feu ou d'autres dispositifs de sécurité, configurés pour refuser le trafic par défaut, afin de se protéger contre le trafic réseau entrant ou sortant malveillant ou non autorisé dans leurs centres d'hébergement ou sur les serveurs.

Référence BP/Commentaires :

GB973 Guide - 4 /DSD 2011 #8 (Modifié)

GB973 Guide - 5 /DSD 2011 #9 (Modifié)

Par exemple : Utiliser la fonction de contrôle de frontière, par exemple les contrôleurs de frontière de session ou des dispositifs similaires, pour empêcher le déni / la dégradation de la communication VOIP en bloquant les tempêtes d'enregistrement provenant des fermes de serveurs (points d'extrémité non autorisés) et en bloquant les tentatives de fuzzing de protocole.

Notez qu'il est important de s'assurer que la protection applicative déployée n'est pas elle-même vulnérable à une attaque DoS/DDoS. Si sa conception ou sa configuration le rend vulnérable à une attaque, le dispositif peut rendre l'application plus sensible à une attaque DDoS. Phase : Préparation (prévention, fournisseur d'hébergement)

Guide de mise en œuvre : Efficacité (H/M/L) : M

Difficulté de mise en œuvre : (H/M/L) : M

Identification

Numéro BP : Nouveau BP11

Surveillance de l'environnement d'hébergement pour le trafic malveillant ou DDoS :

Les fournisseurs d'hébergement, dans la mesure du possible, doivent surveiller leurs environnements pour détecter tout trafic réseau malveillant ou DDoS afin d'identifier les sources et les méthodes d'attaque.

Référence BP/Commentaires :

TBD

Phase : Identification (fournisseur d'hébergement)

Guide de mise en œuvre : Efficacité (H/M/L) : H

Difficulté de mise en œuvre : (H/M/L) : M

Numéro BP : 9-8-8916 (répété depuis la section des opérateurs de réseau)
Mis à jour à :
La détection des robots et la notification correspondante doivent être effectuées en temps utile :

Les opérateurs de réseau et les fournisseurs d'hébergement doivent veiller à ce que la détection des bots et la notification correspondante aux clients hébergeurs se fassent en temps utile, car ces problèmes de sécurité sont sensibles au facteur temps. Si une analyse complexe est nécessaire et que plusieurs confirmations sont requises pour confirmer la présence d'un bot, il est possible que le malware cause des dommages, soit à l'hôte infecté, soit au système ciblé à distance (au-delà des dommages causés par l'infection initiale) avant de pouvoir être arrêté. Ainsi, un opérateur de réseau ou un fournisseur d'hébergement doit trouver un équilibre entre le désir de confirmer définitivement une infection par un logiciel malveillant, ce qui peut prendre un certain temps, et la capacité de prédire la forte probabilité d'une infection par un logiciel malveillant dans un laps de temps très court. Ce défi "définitif vs. probable" est difficile à relever et, dans le doute, les opérateurs de réseau et les fournisseurs d'hébergement devraient pécher par excès de prudence en communiquant une infection probable par un logiciel malveillant tout en prenant des mesures raisonnables pour éviter les notifications faussement positives.

Référence BP/Commentaires :

La mise en œuvre de la notification par l'opérateur de réseau doit équilibrer la certitude d'une infection détectée et l'incertitude d'une détection transitoire de trafic malveillant afin de minimiser la possibilité de notifications faussement positives qui pourraient devenir une gêne pour les clients et devenir ingérables par l'opérateur de réseau.
Pour plus d'informations, voir le Code de conduite anti-bots (ABC) des États-Unis pour les services Internet.
fournisseurs d'accès Internet (FAI) :
http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

Phase : Identification (Surveillance et Visibilité, Opérateur de réseau, Fournisseur d'hébergement)
Guide de mise en œuvre : Efficacité (H/M/L) : L (notification uniquement)
Difficulté de mise en œuvre : (H/M/L) : M

Notez que les meilleures pratiques de ce groupe s'adressent principalement aux ISP qui fournissent des services aux utilisateurs finaux sur des réseaux résidentiels à large bande, mais qu'elles peuvent également s'appliquer à d'autres utilisateurs et réseaux.

Numéro de BP : Nouveau BP6 (repris de la section "opérateur de réseau")
Utiliser l'analyse des données Netflow pour analyser les attaques DDoS :

Dans la mesure du possible, les opérateurs de réseau et les fournisseurs d'hébergement doivent permettre, collecter et analyser les données Netflow afin de faciliter l'identification et la classification des attaques DDoS. Les données doivent être disponibles après l'attaque pour permettre une analyse plus approfondie. Les données Netflow doivent être conservées conformément à la politique de conservation des données de l'opérateur de réseau.

Référence BP/Commentaires :

Les données Netflow peuvent être utiles pour identifier les attaques de type spoofing.
Phase : Identification (surveillance et visibilité, opérateur de réseau, fournisseurs d'hébergement)
Orientation de la mise en œuvre : Efficacité (H/M/L) : H
Difficulté de mise en œuvre : (H/M/L) : M

Classification

Numéro de BP : Nouveau BP18 (repris de la section "opérateur de réseau")
Classifier les attaques DoS/DDoS :

Les opérateurs de réseau, les fournisseurs d'hébergement et les cibles DDoS doivent, dans la mesure du possible, disposer de processus et/ou de capacités permettant d'analyser et de classer une attaque DoS/DDoS. La classification des attaques peut aider à déterminer les meilleures mesures d'atténuation de l'attaque et à identifier les améliorations nécessaires pour assurer une protection future.

Référence BP/Commentaires :

Exemple de classification :
Attaque volumétrique ?
Envoi direct de paquets
Réflexion/Amplification
Attaque de la couche d'application ?
Attaque par épuisement de l'état ou des ressources ?
Attaque de l'avion de contrôle ?
Attaque spécifique Ipv6 ?
Date ?

Phase : Classification (type d'attaque, opérateur réseau, fournisseur d'hébergement, cible), post-mortem et récupération (opérateur réseau, fournisseur d'hébergement, cible).
Guide de mise en œuvre : Efficacité (H/M/L) : M
Difficulté de mise en œuvre : (H/M/L) : H

Traceback

Réaction

Numéro BP : Nouveau BP12
Notifier les clients de l'hébergement en cas de trafic malveillant ou de DDoS

Les fournisseurs d'hébergement, dans la mesure du possible, doivent informer les clients concernés si un trafic réseau malveillant ou DDoS est détecté en provenance de leurs serveurs et, le cas échéant, aider les clients à y remédier.

Référence BP/Commentaires :

TBD

Phase : Réaction (fournisseur d'hébergement)
Guide de mise en œuvre : Efficacité (H/M/L) : M
Difficulté de mise en œuvre : (H/M/L) : H

Numéro BP : 9-9-8065 (répété depuis la section des opérateurs de réseau)

Les opérateurs de réseau et les fournisseurs d'hébergement doivent établir une procédure de communication des informations aux membres des forces de l'ordre et désigner un point de contact (POC) pour les activités de coordination.

Référence BP/Commentaires :
Aucun.
Phase : Réaction (opérateur de réseau, fournisseurs d'hébergement)
Guide de mise en œuvre : Efficacité (H/M/L) : L
Difficulté de mise en œuvre : (H/M/L) : L

Post-mortem et récupération

Numéro BP : 9-9-8762 (répété depuis la section des opérateurs de réseau)
Récupérer après une attaque DoS :
Mis à jour à :
Les opérateurs de réseau et les fournisseurs d'hébergement doivent, dans la mesure du possible, coopérer avec d'autres opérateurs de réseau et fournisseurs d'hébergement.
pendant et après des cyberincidents importants, afin de partager des informations sur les mesures à prendre.
pour caractériser l'attaque, sur les techniques permettant d'identifier, de filtrer et d'isoler l'origine de l'attaque.
de l'attaque, et sur les mesures prises pour réacheminer le trafic légitime et pour dissuader ou se défendre contre des attaques DoS similaires.
Référence BP/Commentaires :
IETF RFC2350, CMU/SEI-98-HB-001. Remarque : Cette meilleure pratique pourrait avoir un impact sur le 9-1-1.
opérations.
Mis à jour pour ajouter :
Cette meilleure pratique vise à la récupération de l'infrastructure de l'opérateur après une attaque DoS. Phase : Réaction (Opérateur réseau, fournisseurs d'hébergement) ; Post Mortem (Opérateur réseau, fournisseurs d'hébergement).
Guide de mise en œuvre : Efficacité (H/M/L) : M
Difficulté de mise en œuvre : (H/M/L) : M

Numéro BP : 9-8-8515 (répété depuis la section des opérateurs de réseau)
Mis à jour à :
Récupération en cas de mauvaise utilisation ou de consommation indue des ressources du système :
En cas de détection d'une mauvaise utilisation ou d'une utilisation non autorisée d'un système sous leur contrôle (par exemple, la détection d'une participation à une attaque DDoS), les opérateurs de réseau, les fournisseurs d'hébergement ou les cibles doivent, dans la mesure du possible, effectuer une analyse médico-légale du système, réaliser une analyse post-mortem, appliquer des contrôles pour empêcher de futures attaques et/ou faire respecter les quotas de ressources du système.
Référence BP/Commentaires :
IETF RFC2350, CMU/SEI-98-HB-001.
Phase : Post-mortem (opérateur réseau, hébergeur, cible)
Guide de mise en œuvre : Efficacité (H/M/L) : M
Difficulté de mise en œuvre : (H/M/L) : H

Cibles

Préparation

Numéro BP : 8-9-8074 (répété depuis la section des opérateurs de réseau)
Mise à jour de
Attaque par déni de service (DoS) - Cible :

Dans la mesure du possible, les opérateurs de réseaux, les fournisseurs d'hébergement, les réseaux cibles et les équipements des fournisseurs d'équipements doivent être en mesure de survivre à des augmentations significatives du nombre de paquets et de l'utilisation de la bande passante. Dans la mesure du possible, les fournisseurs d'équipements et de logiciels doivent développer des fonctions efficaces de survie aux attaques DoS/DDoS pour leurs gammes de produits. L'infrastructure soutenant les services critiques doit être conçue pour faire face à des augmentations significatives du volume de trafic et doit inclure des dispositifs de réseau capables de filtrer et/ou de limiter le trafic. Les ingénieurs réseau doivent comprendre les capacités de ces dispositifs et savoir comment les utiliser de manière optimale. Dans la mesure du possible, les systèmes essentiels à la mission doivent être déployés dans une configuration en grappe permettant l'équilibrage de la charge du trafic excédentaire et protégés par un dispositif de protection DoS/DDoS spécialement conçu à cet effet. Les exploitants d'infrastructures critiques doivent déployer du matériel et des logiciels capables de résister aux attaques DoS chaque fois que cela est possible.

Référence BP/Commentaires :

Note : Cette meilleure pratique pourrait avoir un impact sur les opérations du 9-1-1.

Par exemple, défense contre les attaques SYN Flood, CERT/CC ® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks - http://www.cert.org/advisories/CA-1996-21.html. Lié à NRIC BP 8753A.

Il convient de noter que les opérateurs de réseau, les fournisseurs d'hébergement, les cibles et les fournisseurs d'équipements doivent déterminer quels services sont essentiels à la mise en œuvre de cette meilleure pratique.

Phase : Préparation (capacité et ressources, opérateur de réseau, fournisseur d'hébergement, cible)

Guide de mise en œuvre : Efficacité (H/M/L) : M

Difficulté de mise en œuvre : (H/M/L) : H

Numéro BP : Nouveau BP7
Les services web doivent limiter les charges utiles susceptibles d'entraîner un encombrement de la bande passante en sortie des serveurs web :

Les fournisseurs d'applications Web doivent limiter les objets de grande taille, tels que les téléchargements de documents volumineux, afin d'éviter que les demandes répétées ne consomment une quantité importante de bande passante sortante du serveur (c'est-à-dire la bande passante du site du serveur au site du client), ce qui peut provoquer une situation de déni de service pour les utilisateurs légitimes. Envisagez également de limiter le nombre de requêtes http get/post autorisées par adresse IP dans une plage horaire spécifique.

Référence BP/Commentaires :

TBD

Phase : Préparation (minimiser la surface d'attaque, la cible)

Guide de mise en œuvre : Efficacité (H/M/L) : M

Difficulté de mise en œuvre : (H/M/L) : H

Numéro BP : Nouveau BP13

Surveillance de la cible pour le trafic malveillant ou DDoS :

Les cibles doivent surveiller les journaux de sécurité et de serveur pour déterminer si un trafic anormal ou des événements de sécurité se sont produits. Cela permet de déterminer si la cible fait l'objet d'une attaque ou si une attaque a récemment eu lieu ; cela peut également indiquer un signe précurseur d'une attaque.

Référence BP/Commentaires :

Il convient de noter que les cibles des attaques peuvent être des utilisateurs finaux ainsi que des opérateurs de réseau et des fournisseurs d'hébergement.

Phase : Préparation (Suivi & Visibilité, Cible)

Orientation de la mise en œuvre : Efficacité (H/M/L) : H

Difficulté de mise en œuvre : (H/M/L) : M

Numéro BP : Nouveau BP15

Utiliser les réseaux de diffusion de contenu pour assurer la robustesse des applications :

Les cibles d'attaques doivent utiliser des réseaux de diffusion de contenu (CDN) pour assurer une certaine robustesse et réduire la vulnérabilité aux attaques DoS/DDoS. Les CDN peuvent être utilisés pour distribuer la capacité des applications sur le réseau, ce qui le rend plus robuste contre les attaques DoS/DDoS.

Référence BP/Commentaires :

TBD

Phase : Préparation (Déploiement des outils d'atténuation, cible)

Orientation de la mise en œuvre : Efficacité (H/M/L) : H

Difficulté de mise en œuvre : (H/M/L) : L

Numéro BP : Nouveau BP17

Déployer l'épuration des données cibles sur site :

Les cibles DDoS peuvent employer, dans la mesure du possible, des centres d'épuration des données de trafic pour filtrer le trafic d'attaque DDoS. Pour ce faire, le trafic DDoS suspecté d'être une attaque peut être "détourné" vers un centre d'épuration sur site où le trafic d'attaque peut être filtré et le trafic légitime peut être "réacheminé" vers la cible.

Référence BP/Commentaires :

Il est important de dimensionner la capacité du réseau sur place et des centres d'épuration pour qu'ils puissent accueillir le trafic d'attaque, afin de minimiser les dommages collatéraux potentiels causés par de fortes hausses de trafic.

Phase : Préparation (déploiement d'outils d'atténuation, filtrage de l'hébergement)

Orientation de la mise en œuvre : Efficacité (H/M/L) : H

Difficulté de mise en œuvre : (H/M/L) : H

Identification

Classification

Numéro de BP : Nouveau BP18 (repris de la section "opérateur de réseau")
Classifier les attaques DoS/DDoS :

Les opérateurs de réseau, les fournisseurs d'hébergement et les cibles DDoS doivent, dans la mesure du possible, disposer de processus et/ou de capacités permettant d'analyser et de classer une attaque DoS/DDoS. La classification des attaques peut aider à déterminer les meilleures mesures d'atténuation de l'attaque et à identifier les améliorations nécessaires pour assurer une protection future.

Référence BP/Commentaires :

Exemple de classification :
Attaque volumétrique ?
Envoi direct de paquets
Réflexion/Amplification
Attaque de la couche d'application ?
Attaque par épuisement de l'état ou des ressources ?
Attaque de l'avion de contrôle ?
Attaque spécifique Ipv6 ?
Date ?

Phase : Classification (type d'attaque, opérateur réseau, fournisseur d'hébergement, cible), post-mortem et récupération (opérateur réseau, fournisseur d'hébergement, cible).

Guide de mise en œuvre : Efficacité (H/M/L) : M
Difficulté de mise en œuvre : (H/M/L) : H

Traceback

Réaction

Post-mortem et récupération

Numéro BP : 9-8-8561
Récupération d'une attaque par déni de service - Cible :

Si un élément de réseau, un système ou un serveur sous le contrôle de la cible a subi une attaque DoS ou une attaque d'un autre type, il est possible que le système soit endommagé.
Une attaque DDoS, la cible doit considérer :

1) Ajout d'une plus grande capacité locale (bande passante ou serveurs) au service attaqué ;
2) Déployer des dispositifs d'atténuation spécifiques aux DoS/DDoS sur site et/ou utiliser les capacités anti-DoS du matériel local ;
3) Acheter des protections DDoS basées sur le réseau pour leur opérateur de réseau, leur fournisseur d'hébergement ou un fournisseur tiers d'atténuation des DDoS ;
4) Pour les systèmes appropriés tels que les sites web, préparez un plan pour minimiser les services fournis par le site en cas d'attaque future qui diminue les effets de l'attaque tout en continuant à fournir des services essentiels ou importants à leurs clients ;
5) Coordonner avec les fournisseurs de logiciels et de matériel pour obtenir des conseils sur la configuration optimale des appareils ;
6) Architecturer leur système pour capturer le trafic d'attaque, les adresses IP des attaquants et les horodatages correspondants ;
7) Partager le code, les tactiques, les techniques et les sources d'attaques hostiles ou d'attaques.

aux organisations susceptibles d'être confrontées à des types d'attaques similaires et aux organisations centrales de coordination telles que l'US-CERT et le NCS/NCC pour examen, analyse et distribution à un public plus large ; et

8) Travaillez avec l'opérateur de réseau, le fournisseur d'hébergement, l'ISAC ou le CERT pour identifier les ordinateurs qui attaquent et nettoyer les machines du côté distant afin de minimiser l'impact de l'attaque. la possibilité d'attaques futures.

Référence BP/Commentaires :

Phase : Post Mortem (Cible)

Guide de mise en œuvre : Efficacité (H/M/L) : M

Difficulté de mise en œuvre : (H/M/L) : H

Numéro BP : 9-8-8515 (répété depuis la section des opérateurs de réseau)

Mis à jour à :

Récupération en cas de mauvaise utilisation ou de consommation indue des ressources du système :

En cas de détection d'une mauvaise utilisation ou d'une utilisation non autorisée d'un système sous leur contrôle (par exemple, la détection d'une participation à une attaque DDoS), les opérateurs de réseau, les fournisseurs d'hébergement ou les cibles doivent, dans la mesure du possible, effectuer une analyse médico-légale du système, réaliser une analyse post-mortem, appliquer des contrôles pour empêcher de futures attaques et/ou faire respecter les quotas de ressources du système.

Référence BP/Commentaires :

IETF RFC2350, CMU/SEI-98-HB-001.

Phase : Post-mortem (opérateur réseau, hébergeur, cible)

Guide de mise en œuvre : Efficacité (H/M/L) : M

Difficulté de mise en œuvre : (H/M/L) : H