CENTRE FOR CYBERSECURITY BELGIUM

DDOS : PRÉVENTION ET PROTECTION

DIRECTIVE TECHNIQUE 2024

Belnet

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

.be

Date : Février 2024
Version : 2.1 Français
Auteur : Le Centre pour la cybersécurité Belgique (CCB) avec la précieuse contribution de Belnet

Le Centre pour la cybersécurité Belgique (CCB) est l'autorité nationale en charge de la cybersécurité en Belgique. Institué par l'arrêté royal du 10 octobre 2014, le CCB relève de l'autorité du Premier ministre.

Sur la base de sa mission légale, le CCB tente d'informer et de conseiller les organisations à propos de la protection contre les attaques DDoS. Ce document se veut une directive technique, d'aide et de conseil à l'approche des élections belges de 2024, afin de prévenir les attaques DDoS et de s'en protéger.

RÉSUMÉ

Cette directive sur les mesures d'atténuation d'attaques DDoS a été rédigée dans le contexte des élections belges de 2024. Au niveau fédéral, différentes parties prenantes jouent un rôle de premier plan dans le processus électoral. Une protection efficace contre les attaques DDoS requiert une approche coordonnée entre ces différentes parties prenantes.

Ce document commence par expliquer ce qu'est une attaque DDoS, les différents types d'attaques DDoS, l'impact et les raisons d'une attaque DDoS. Le deuxième chapitre présente des mesures proactives pour se préparer à une attaque DDoS et propose des solutions d'atténuation. Le troisième chapitre explique comment réagir lorsque votre organisation est victime d'une attaque DDoS et décrit les mesures techniques d'atténuation. Le quatrième chapitre consiste en une checklist dont la première partie contient une checklist proactive. La deuxième partie met en évidence les étapes de la réponse à l'incident comme décrit au chapitre trois.

La directive a une vocation consultative et aide à se préparer et à être en mesure de répondre en cas d'attaque DDoS.

Ce document a été créé avec la participation précieuse de Belnet.

Contents

Glossaire

ASN	Autonomous system number
Botnet	Ensemble d'appareils connectés, souvent au sein d'un réseau IoT, qui devient infecté et contrôlé par des logiciels malveillants au profit de cybercriminels.
CCB	Centre pour la Cybersécurité Belgique
CDN	Content delivery network
CSIRT	Cyber security incident response team
C2 server	Command and Control server
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
Drupal	Logiciel de gestion de contenu
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ISP	Internet Service Provider
NSM	Network Security Monitoring
Modèle OSI	Le modèle OSI (« Open Systems Interconnection ») décrit les sept couches que les systèmes informatiques utilisent pour communiquer sur un réseau.
SIP	Session Initiation Protocol
SIEM	Security Information and Event Management system
SMTP	Simple Mail Transfer Protocol
SYN flood	Type d'attaque denial-of-service (DDoS) qui vise à rendre un serveur indisponible pour le trafic légitime, en consommant toutes ses ressources disponibles.
TCP	Transmission Control Protocol
TTL	Time to Life
UDP	User Datagram Protocol
WAF	Web Application Firewall

1. Introduction

1.1. GÉNÉRALITÉS

Une attaque de type « Denial of Service », ou DoS, est une cyberattaque qui vise à perturber l'accessibilité d'un service particulier. Une attaque DoS concerne un ordinateur et une connexion Internet. Lorsque l'attaque est distribuée, c'est-à-dire qu'elle utilise plusieurs ordinateurs et leurs connexions Internet, on parle de DDoS, « Distributed Denial of Service ». Il est important de souligner que, bien que distribués par nature, les ordinateurs participant à une attaque DDoS partagent un objectif commun et que l'attaque est coordonnée. Ces attaques peuvent avoir un impact majeur sur le fonctionnement des organisations et des entreprises.

Il existe différents types d'attaques DDoS, qui sont examinés en détail au point 1.4. Types d'attaques DDoS.

1.2. RAISONS DERRIÈRE LES ATTAQUES DDOS

Les auteurs d'attaques DDoS peuvent avoir diverses motivations : chantage, attaques idéologiques ou haineuses, concurrence, politique, protestation électronique, diversion, test, expérience, hacktivisme, prestige/challenge ou extorsion. Par exemple, des hacktivistes ont ciblé des sites Internet liés aux élections principalement avec des attaques DDoS, qui consistent à envoyer des quantités massives d'informations vers des serveurs pour saturer le trafic et ainsi bloquer l'accès de sites Internet. Ces attaques sont souvent portées par des idéaux politiques et visent à perturber le processus démocratique, à provoquer le chaos ou à protester contre des décisions politiques.

La principale menace hacktiviste qui pèse actuellement en matière d'attaque DDoS est le projet DDoSia, lancé début 2022. Ce projet DDoS est lié à un groupe d'hacktivistes nationalistes russes et lance de nombreuses attaques contre des pays et des services liés à l'OTAN et à l'Ukraine.

1.3. SOURCE DES ATTAQUES DDOS

La majorité des attaques DDoS a lieu via un « botnet ».

Ces botnet sont le plus souvent « loués » pour quelques heures afin de mener l'attaque, ce qui s'apparente à un « DDoS as a service ». Les propriétaires des botnets ne sont généralement pas aux commandent de l'attaque. Un botnet est constitué d'un grand nombre d'ordinateurs infectés par un logiciel malveillant. Le logiciel malveillant, ou malware, contient un agent qui exécute l'attaque proprement dite. Il convient de noter que la plupart des logiciels malveillants présentent différentes caractéristiques et que les capacités DDoS ne sont souvent que l'une d'entre elles. L'agent installé sur l'appareil infecté est commandé depuis un serveur C2 (« Command and Control server »). Ce C2 contrôle les différents agents et leur indique ce qu'ils doivent faire. Les propriétaires d'appareils infectés ne savent généralement pas que leur appareil est infecté et qu'il prend part à une attaque DDoS. Il est important de souligner que lancer une attaque DDoS est à la portée de presque tout le monde.

De nombreux outils et ressources (botnets) sont disponibles. Toute personne disposant de compétences limitées mais d'une détermination suffisante (ou d'argent – bien que les botnets soient souvent abordables) peut lancer une attaque DDoS.

1.4. TYPES D'ATTAQUES DDOS

En règle générale, les formes les plus courantes d'attaques DDoS peuvent être classées en trois catégories :

1. **Volumétrique :** cette méthode d'attaque DDoS basée sur le volume est conçue pour perturber le trafic normal ou les requêtes en saturant la couche « réseau » d'un service cible avec un flot de trafic frauduleux provenant de nombreuses sources. Il en résulte un service dégradé ou complètement indisponible, même pour les utilisateurs légitimes. Ce type de DDoS est souvent appelé « attaque de couche 3 ». Parmi les exemples, on retrouve les attaques par réflexion/amplification (UDP flood) et les ICMP flood (« Internet Control Message Protocol »).

2. **Protocole :** les attaques DDoS basées sur un protocole s'appuient sur les faiblesses des protocoles de communication Internet pour exploiter les vulnérabilités organisationnelles. Des protocoles tels que TCP (« Transmission Control Protocol ») et ICMP peuvent être utilisés pour lancer des attaques DDoS basées sur ces protocoles. Typiquement, une attaque DDoS au niveau du protocole lancera un grand nombre de connexions sans les démarrer complètement (exemple : SYN flood) et ce, pour épuiser le nombre de connexions que le serveur peut gérer. Le principal vecteur de ce type d'attaque étant la SYN Flood (TCP),

on parle souvent d'une attaque DDoS de couche 4.

3. **Attaque applicative :** l'attaque de la couche applicative est également connue sous le nom d'attaque DDoS de couche 7. Cette méthode cible la couche « application » d'un réseau, qui est la couche responsable du traitement de protocoles spécifiques, tels que HTTP, SMTP (« Simple Mail Transfer Protocol ») ou DNS. Les attaques de la couche « application » nécessitent généralement une meilleure connaissance de l'infrastructure de la victime et, lorsqu'elles sont exécutées correctement, requièrent un minimum de ressources de l'attaquant. Typiquement, les attaques DDoS de la couche applicative enverrons des données aléatoires sur un formulaire de recherche de site Internet afin de surcharger la base de données, ou demanderont au serveur DNS un grand nombre de sous-domaines aléatoires qui n'existent pas. Un exemple d'attaque de la couche applicative est l'attaque HTTP slow post, où un attaquant envoie délibérément des données annoncées très lentement, pour maintenir les connexions ouvertes et finir par épuiser les ressources du serveur.

2. Mesures proactives

Ce chapitre reprend un certain nombre de mesures proactives, à la fois techniques et non techniques, permettant de limiter l'impact d'une éventuelle attaque DDoS.

2.1. APPRENEZ À CONNAÎTRE VOTRE RÉSEAU

Il est important de connaître votre réseau, de savoir quels sont les services et réseaux publics dont vous disposez. N'oubliez pas vos services hors site (par exemple : le cloud). Si votre connexion Internet est interrompue, vous ne pourrez pas accéder à ces services.

Il est recommandé de disposer d'un inventaire complet, y compris les typologies de réseau et les adresses IP externes et internes. Cette documentation sera essentielle en cas d'attaque. Assurez-vous également de disposer d'un accès hors ligne à la documentation en cas de cyberattaque.

L'exécution régulière d'un scanner de réseau hors réseau pour inventorier vos dispositifs et services accessibles au public permet de cartographier ce que vous mettez à disposition sur Internet. Assurez-vous de disposer d'une liste des propriétaires de services et d'une liste des responsables (techniques et non techniques) de tous vos services exposés.

2.2. APPRENEZ À CONNAÎTRE VOS APPLICATIONS

Il est important de connaître vos applications et de préparer des mesures d'atténuation des attaques en conséquence. Les attaques DDoS ont tendance à exploiter des parties spécifiques des applications pour augmenter la surcharge de plusieurs systèmes. Être conscient de ces faiblesses peut vous aider à préparer des mesures d'atténuation ciblées.

Sur un site Internet, certaines pages peuvent représenter une lourde charge sur la base de données (par exemple : un formulaire de recherche) et être ciblées pour surcharger la base de données du site Internet. Ces pages sont aussi souvent celles qu'il est difficile de placer efficacement derrière un cache. Garder un inventaire de ces pages et préparer une procédure pour les désactiver si elles sont ciblées par une attaque DDoS peut aider à en limiter les risques. Une copie statique du site pourrait également être élaborée à titre de remplacement temporaire pendant l'attaque.

2.3. PROCÉDURE DE RÉPONSE AUX INCIDENTS

Élaborez un plan d'intervention en cas d'incident et tenez-le à jour. Face à une attaque DDoS, il est important de réagir aussi rapidement et efficacement que possible.

Une procédure de réponse aux incidents décrit ce qu'il convient de faire en cas de cyberattaque. Définissez un certain nombre de procédures opérationnelles standard en cas d'attaque DDoS :

- Identifiez les actifs de votre organisation
- Mettez en œuvre un plan de continuité des activités/de reprise après attaque
- Attribuez des priorités pour la reprise des activités
- Documentez le fonctionnement de vos systèmes et tenez cette documentation à jour
- Attribuez des responsabilités et des rôles aux personnes compétentes
- Préparez un canal de communication hors bande
- Rédigez une liste des personnes de contact
- Faites appel à des experts en matière de réponse aux cyber incidents
- Préparez une stratégie de communication - pour plus d'informations : https://atwork.safeonweb.be/fr/recent-news-tips-and-warning/la-communication-de-crise-en-cas-de-cyberattaque

Pour les attaques DDoS en particulier, il est crucial de prêter une attention particulière aux points suivants :

- Consultez au préalable votre fournisseur d'accès à Internet (FAI) : discutez de ce que votre FAI a mis en place pour prévenir les attaques DDoS et de ce qu'il peut faire en cas d'attaque DDoS. Il peut s'agir, par exemple, d'un géoblocage, d'un changement d'adresse IP publique, de packet scrubbing, etc.

- Préparez des Service Level Agreements (SLA) avec votre FAI en cas d'attaque DDoS et préparez des

SLA pour les attaques DDoS à tous les niveaux du réseau.

- Vérifiez et révisez les contrats existants avec votre FAI, votre fournisseur de services cloud et votre fournisseur d'hébergement en ce qui concerne la protection contre les attaques DDoS.

- Un suivi étroit de l'infrastructure clé est nécessaire pour repérer rapidement l'utilisation accrue ou l'épuisement des ressources et permettre une réaction rapide. Définissez des responsabilités et des rôles concernant ce suivi.

- Assurez-vous qu'il existe une base de référence claire pour le trafic réseau, afin de repérer plus facilement tout trafic anormal/perturbé.

- Étudiez la possibilité d'augmenter l'échelle de votre infrastructure en cas d'attaque. En particulier pour les services fonctionnant dans le cloud (exemple : Azure).

- Effectuez régulièrement des tests de résistance pour vous assurer que l'infrastructure et les mesures d'atténuation fonctionnent comme prévu.

- Préparez un canal de communication hors bande : une plateforme de communication sécurisée doit fonctionner sur un réseau distinct qui ne fait pas l'objet de ces attaques. Voici quelques exemples : téléphone (non sécurisé), Signal, Threema, etc. Établissez clairement à l'avance quel groupe de personnes communiquera par quel moyen.

- Dressez une liste de contacts hors ligne : il est important de disposer d'une liste de contacts hors ligne (imprimée) des personnes qui peuvent vous aider ou que vous devez informer. Il peut s'agir de personnes internes (direction, employés, service IT) ou externes (FAI, expert en sécurité, clients).

- Outre l'expertise technique, la disponibilité du personnel capable de prendre des décisions exécutives est également requise. Ces deux rôles doivent être repris dans un plan de continuité des activités ou un plan de reprise après attaque.

- Tenez à jour une liste des menaces pour les botnets connus et les adresses IP malveillantes, et bloquez-les définitivement ou soyez au moins en mesure de les désactiver rapidement si nécessaire.

- Répartissez les différents services sur votre espace IP afin de minimiser les effets secondaires potentiels et de faciliter l'atténuation. Ne regroupez pas différents services indépendants derrière une même IP.

- N'utilisez jamais la même adresse IP publique pour des services/applications et l'accès à Internet des personnes au sein de votre organisation.

3. Étapes de la réponse à un incident lors d'une attaque DDoS

Le troisième chapitre explique comment réagir lorsque votre organisation est victime d'une attaque DDoS. Les mesures d'atténuation décrites ci-dessous sont les mesures minimales qu'une organisation devra suivre en cas d'attaque DDoS. Sachez qu'il n'existe pas de solution unique.

Il est important de souligner à la victime d'une attaque DDoS que ce processus nécessite une expertise technique ainsi qu'un accès à ses ressources techniques.

3.1. DÉTERMINER ET CONFIRMER L'AMPLEUR DE L'ATTAQUE

Avant de tirer des conclusions hâtives et de penser qu'une attaque DDoS est en cours, il est nécessaire d'évaluer l'indisponibilité de la ressource (par exemple : est-elle indisponible pour un nombre limité de personnes ou pour tout le monde ?).

Rassemblez autant d'informations que possible sur l'attaque. Afin de déterminer l'impact du DDoS, il est important de dresser l'inventaire des systèmes affectés. Cela peut par exemple se faire sur la base de plaintes d'utilisateurs.

3.2. VISIBILITÉ DE L'ATTAQUE

Une fois l'impact de l'attaque documenté et compris, il est important de rechercher les causes de cette indisponibilité. Une bonne compréhension du fonctionnement de l'attaque est essentielle pour pouvoir mettre en œuvre des contre-mesures efficaces.

- S'il est disponible, un Security Information and Event Management system (SIEM) ou Network Security Monitoring (NSM) peut s'avérer extrêmement utile pour comprendre ce qui se passe.
- Si aucune solution de monitoring ou de logging n'est disponible, il convient d'examiner directement les logs des équipements ou des applications du réseau.
- Si vous disposez d'une base de référence claire pour le trafic réseau normal, utilisez ces connaissances pour déterminer les types d'attaques utilisés par les attaquants. Il peut s'agir, par exemple, d'une augmentation significative du nombre de requêtes adressées à un serveur ou de requêtes (accrues) pour des domaines inexistants (DNS).
- Discutez avec votre fournisseur d'accès à Internet (FAI) de ce que vous pouvez mettre en œuvre pour améliorer la situation et mettre en place une surveillance proactive.

3.3. DEMANDEZ DE L'AIDE À VOTRE FAI OU METTEZ EN PLACE UNE SOLUTION ANTI-DDOS TIERCE

- Contactez votre FAI ou votre fournisseur de solution anti-DDoS dès que possible et fournissez-leur un maximum d'informations sur l'attaque dont vous êtes la cible. Transmettez-leur au moins l'Ips ciblé, le type de DDoS (voir 1.4. Types d'attaques DDOS), les potentiels vecteurs de l'attaque, etc.
- Vous pouvez également communiquer sur l'impact et les effets de l'attaque, afin d'aider votre FAI à comprendre ce à quoi vous êtes confronté et ce qui peut être fait pour y remédier.
- Si vous êtes en mesure de leur fournir un inventaire du trafic légitime, ils pourront se faire une idée du volume de trafic qu'ils doivent bloquer.
- Demandez l'ouverture d'un canal de communication pour faciliter la communication pendant l'attaque. Les vecteurs d'attaque changent souvent au cours de l'attaque pour contourner les mesures d'atténuation mises en place. Cela vous permettra également de donner du feedback sur les mesures prises. Le FAI sera en mesure de réagir plus rapidement à des mesures trop agressives qui bloquent le trafic légitime ou d'autres, trop souples, qui autorisent trop de paquets provenant de l'attaque.
- Bien que le FAI ne soit probablement pas en mesure d'atténuer les attaques de la couche 7 s'il n'héberge pas ou ne gère pas vos applications, n'hésitez pas à l'impliquer car il pourrait être en mesure d'atténuer certains vecteurs utilisés en même temps.
- Gardez à l'esprit que votre même si FAI doit proposer une forme de protection contre les attaques DDoS

(en interne ou par l'intermédiaire d'un tiers) permettant d'atténuer une grande partie des attaques volumétriques des couches 3 et 4, cette atténuation ne sera jamais intégrale.

- En dernier recours, si une IP spécifique (et non un périphérique) est la cible et que la protection n'est pas suffisante, demandez à votre fournisseur d'installer temporairement un « blackhole » sur cette IP. Cela signifie bien sûr que la ressource ne sera pas disponible, ce qui rend l'attaque partiellement réussie, mais au moins les garanties sont atténuées et l'organisation reste opérationnelle dans une certaine mesure.

3.4. Étapes que la victime peut suivreLes étapes ci-dessous supposent que la connectivité externe est toujours disponible. Si la gateway ou le firewall externe sont complètement mis à mal à cause de l'attaque, contactez le FAI.

Si vous disposez d'un système de monitoring/logging, examinez-le. À défaut, vous pouvez effectuer un PCAP sur la partie externe du firewall pour l'analyser, ou collecter des logs directement au sein des applications/périphériques.

3.4.1. COMPRENDRE L'ATTAQUE

- Déterminez la cible de l'attaque.
- Quel type de ressources l'attaquant vise-t-il ?
- Déterminez le type d'attaque DDOS (sur quelle couche de l'OSI, couches 3-4 ou jusqu'à 7).
- Effectuez une analyse statistique de la source de l'attaque : y a-t-il une source ou des pays qui se distinguent ? Y a-t-il des ASN qui sortent du lot ? Les visualisations/tableaux de bord généralement disponibles dans un NSM sont très utiles à cet égard.

3.4.2. ATTÉNUATIONS GÉNÉRALES DE DDOS

Il est généralement judicieux de procéder à un filtrage rapide du trafic de l'attaque, permettant à votre réseau de quelque peu respirer. À ce moment-là, vous pouvez sans doute vous limiter à un blocage très restrictif. La santé de votre réseau et de vos applications, ainsi que la disponibilité pour vos clients principaux, sont vos préoccupations premières. Cela vous permet de gagner du temps pour creuser davantage et trouver des solutions d'atténuation plus élégantes et mieux adaptées au vecteur d'attaque utilisé.

- Blocage temporaire des adresses IP assaillantes : créez une blacklist (de préférence séparée) qui consigne les adresses IP auxquelles l'accès doit être (temporairement) refusé. Si l'adresse IP qui a envoyé une demande y figure, le système intercepte la connexion et refuse l'accès. Ce refus peut prendre différentes formes, comme l'affichage d'un message d'erreur, la redirection de l'utilisateur vers une autre page ou l'interruption de la connexion sans réponse.

- Géoblocage temporaire/géorepérage de plages IP spécifiques : blocage de l'accès à partir d'une région géographique entière.

- Blocage d'ASN : si le trafic malveillant provient d'ASN distincts, bloquez ces ASN ou les blocs de réseaux de ceux-ci.

- Load balancing et upscaling : les techniques de load balancing distribuent le trafic entrant vers plusieurs serveurs ou centres de données. En équilibrant la charge de trafic, on peut éviter qu'un seul serveur ou une seule ressource ne soit submergé(e) par une attaque DDoS. La possibilité d'augmenter temporairement la capacité d'un service pendant une attaque peut en limiter l'impact.

- Isoler : si le service attaqué se trouve sur un serveur qui fournit également d'autres services, déplacez le service attaqué sur une machine dédiée afin de réduire au minimum l'impact collatéral de l'attaque.

- Alléger (strip down) : alléger un service jusqu'à son strict minimum.

- Blackhole déclenché à distance : détourner tout le trafic à destination d'une IP cible spécifique vers une « interface nulle », en supprimant le trafic malveillant avant qu'il n'atteigne sa destination.

- Arrêter les services et/ou applications ciblés : bien que cette mesure ne bloque pas les attaques, elle peut empêcher le dysfonctionnement de l'application/du service. Sachez que cette mesure peut entraîner une perte substantielle de données et de services.

3.4.3. MESURES D'ATTÉNUATION SPÉCIFIQUES PAR VECTEUR D'ATTAQUE

En cas d'attaque DDOS : rechercher un protocole (couche 3/couche 4) ou une application (couche 7) sur la base des modèles spécifiques suivants :

Aperçu couches 3 et 4

Protocole	Vecteur d'attaque	Mesures d'atténuation
UDP	Reflective/Amplification	• Peut être bloqué si ce trafic n'est pas utilisé/attendu sur le système cible. • Sinon, il faut compter sur les technologies de detection / nettoyage volumétrique anti-DDoS (DDoS scrubbing).
TCP	SYN Flood	• Mise en place de SYN cookies. • Ajustement des paramètres de délai d'expiration (timeout). • Recyclage des connections TCP partiellement-ouvertes.

Aperçu couche 7

Application	Vecteur d'attaque	Mesures d'atténuation
DNS	NX Flood (Legitimate) request flood	• Protection du cache du serveur DNS contre la pollution par les réponses NX. • Abandon de certaines requêtes DNS sur la base d'une whitelist de (sous-)domaines. • Limitation du débit par IP source.
HTTP/HTTPS	Low/slow Targeted URL flood	• Ajustement plus agressif des paramètres de délai d'expiration (timeout). • Limitation plus agressive du débit pour les URL les plus ciblées. • Si l'ampleur de impact sur le serveur web est importante : envisager de bloquer toutes les requêtes vers les URL les plus ciblées (en les rendant donc indisponibles). • Si disponible : vérifier l'URL de référence.

3.4.4. AUTRES MESURES D'ATTÉNUATION À ENVISAGER

- Mettez en place un dispositif dédié anti-DDOS capable d'atténuer les attaques DDoS. Notez qu'il s'agit d'une solution coûteuse. Toutefois, si les attaques DDoS sont fréquentes dans votre environnement, ce coût peut se justifier.

- Pour les applications web : remplacez les contenus dynamiques générés par du contenu statique. La désactivation du contenu dynamique comme les formulaires de recherche, l'utilisation d'images à faible résolution et la compression et la minification des fichiers CSS et JavaScript peuvent réduire la charge de trafic.

- Améliorez la résilience en mettant en œuvre (de manière permanente) une solution de Content Delivery Network (CDN).

- Envisagez une segmentation plus poussée de votre réseau. Évitez le partage d'infrastructure dans la mesure du possible.

- Enregistrements DNS : fixation d'un Time To Live (TTL) plus long pour les enregistrements DNS. Une TTL d'un jour (24h) pourrait limiter l'impact sur d'autres services si les serveurs DNS tombent en panne. Il faut toutefois garder à l'esprit qu'une TTL plus longue a également des implications lors de l'application de modifications.

- Pour les applications web telles que les sites Internet : installez un Web Application Firewall (WAF) et un Advanced Global CDN. Le WAF surveille et bloque le trafic malveillant à destination de votre site Internet/serveur sur la base d'un ensemble de règles. Il détecte/bloque les adresses IP malveillantes connues, les utilisateurs suspects et toute autre activité inhabituelle, comme les tentatives répétées d'attaques par force brute sur votre site Internet. L'AGCDN ajoute une protection contre les attaques DDoS sur votre site Internet en empêchant toute augmentation des demandes d'atteindre votre serveur principal (d'origine), ce qui pourrait entraîner l'indisponibilité de votre site. De nombreux fournisseurs de CDN gèrent le WAF de leur côté, dans le cadre d'un service payant.

- Lorsque vous utilisez des ressources du cloud accessibles depuis l'internet public, pensez à activer les mécanismes de protection contre les attaques DDoS du fournisseur cloud.

3.5. COLLECTE DE PREUVES

Que vous signaliez l'incident dans la phase post-incident à votre FAI, au CSIRT national, aux autorités judiciaires ou à tout autre partenaire, vous devrez produire des preuves. Les preuves peuvent être des NetFlow, des logs au niveau du réseau ou de l'application. Dans l'idéal, présentez l'ensemble de ces éléments.

3.6. RECOVERY

L'attaque DDoS est terminée lorsque le trafic de votre réseau revient à la base de référence établie précédemment.

Notez que les attaques DDoS se déroulent parfois par vagues. Les attaquants peuvent lancer plusieurs vagues. Vous pouvez donc penser que l'attaque est finie, vous baissez votre garde et les hackers choisissent ce moment pour lancer une nouvelle attaque, plus puissante. Ils peuvent également changer de méthode entre les différentes vagues afin de déterminer quelle technique est la plus efficace. Une fois l'attaque DDoS terminée, les services désactivés peuvent être redémarrés.

Vérifiez ensuite que tout fonctionne normalement. Si c'est le cas, communiquez cette information aux utilisateurs.

3.7. ÉVALUATION

Une fois l'attaque gérée, toutes les parties prenantes concernées doivent se réunir pour en tirer les enseignements. Évaluez ce qui s'est bien passé et ce qui s'est moins bien passé. Effectuez régulièrement des tests de résistance pour vous assurer que l'infrastructure et les mesures d'atténuation fonctionnent comme prévu.

Évaluez les points d'amélioration et convertissez-les en points d'action concrets dans la phase de préparation ; adaptez ensuite la procédure d'incident pour l'avenir.

Il s'agit notamment des aspects suivants :

- Envisagez de changer les adresses IP des serveurs back end qui sont connues des hackers.

- Dimensionnez correctement la bande passante de votre connexion Internet ; les activités quotidiennes typiques ne devraient consommer qu'environ 50 % de votre bande passante totale.

- Révisez votre architecture en fonction des points faibles observés lors de l'attaque DDoS.

4. Checklist

La checklist ci-dessous est divisée en deux parties. La première partie consiste en une checklist proactive. La deuxième partie met en évidence les étapes de la réponse à l'incident comme décrit au chapitre 3.

4.1. CHECKLIST PROACTIVE

☐ Soyez informé des réseaux, hôtes et services que vous exposez, et mettez votre inventaire à jour régulièrement ; soyez conscient des éventuels goulets d'étranglement :

- Évaluez le risque et l'importance des actifs exposés de l'entreprise.
- Disposez d'une liste écrite et approuvée des propriétaires de services.
- Disposez de diagrammes actualisés du réseau et des services.
- Disposez de canaux de communication hors bande.
- Disposez de copies papier ou hors ligne des personnes de contact.

☐ Veillez à ce que votre FAI et votre CSIRT national connaissent votre organisation et vos points de contact, et vice versa.

☐ Soyez informé avec précision de ce que votre FAI peut faire et de ce qu'il ne peut pas faire lors d'une attaque DDoS.

☐ Préparez des SLA avec votre FAI en cas d'attaques DDoS.

☐ Révisez régulièrement vos règles de firewall.

☐ Veillez à ce que les systèmes d'exploitation, les programmes et les routeurs fassent l'objet de mises à jour de sécurité automatiques.

☐ Utilisez des services cloud dès que possible ; les sites Internet, les services de messagerie ou autres plateformes en ligne sont par exemple très vulnérables si vous les hébergez localement sur un serveur. Les services cloud sont moins susceptibles d'être touchés par des attaques DDoS en raison de leur grande disponibilité.

☐ Préparez un plan de communication de crise.

4.2. ÉTAPES DE LA RÉPONSE AUX INCIDENTS

☐ Disposez de capacités internes de réponse aux incidents.

☐ Utilisez un load balancer correctement configuré et recourez à l'upscaling.

☐ Implémentez un proxy inverse.

☐ Implémentez un WAF et un Advanced Global CDN.

☐ Révisez et consolidez les dispositifs de votre réseau et adoptez les bonnes pratiques.

☐ Préparez une version allégée de vos services à déployer en cas d'attaque.

☐ Pour les applications web : remplacez les contenus dynamiques générés par du contenu statique.

☐ Améliorez la résilience en mettant en œuvre une solution Content Delivery Network (CDN).

☐ Pensez à scinder l'infrastructure DNS interne et publique.

☐ Enregistrements DNS : installation d'une TTL (Time To Live) plus élevée pour les enregistrements DNS. Une TTL d'un jour (24h) pourrait limiter l'impact sur d'autres services si les serveurs DNS tombent en panne lors d'une future attaque.

☐ Pour les applications web (par exemple Drupal) : appliquez un Web Application Firewall (WAF) et un Advanced Global CDN.

☐ Pensez à activer/demander une protection DDoS à vos fournisseurs (cloud).

☐ Bloquez temporairement les IP malveillantes.

☐ Bloquez temporairement des plages d'adresses IP spécifiques (geoblocking/geofencing).

☐ Blocage ASN : si le trafic malveillant provient d'ASN distincts, bloquez cet ASN ou des blocs de réseau de ce dernier.

☐ Load balancing et upscaling : les techniques de load balancing répartissent le trafic entrant entre plusieurs serveurs ou centres de données. En équilibrant la charge de trafic, elles permettent d'éviter qu'un seul serveur ou une seule ressource ne soit submergé(e) par une attaque DDoS.

☐ Packet scrubbing : le trafic destiné à une plage d'adresses IP particulière est redirigé vers des centres de données, où le trafic de l'attaque peut être « nettoyé » (scrubbed). Seul le trafic sain est alors ensuite acheminé vers la destination cible.

☐ Stoppez les services et/ou les applications ciblés.

☐ Blackhole déclenché à distance.