Document de référence sur l'atténuation des DDoS

Champ des DDoS : infrastructure du DNS des ccTLD

Atelier sur les TLD-OPS

Version 1.0, mercredi 25 avril 2018

Aperçu de l'atelier

L'objectif de l'atelier était d'explorer comment les membres des TLD-OPS peuvent collaborer pour élaborer un document de référence des DDoS. L'accent a été mis sur les DDoS ciblant l'infrastructure du DNS faisant autorité sur unicast et anycast, exploitée par le ccTLD et leurs partenaires fournisseurs DNS.

Motivation

Cet atelier faisait suite à l'atelier d'atténuation des DDoS qui s'est tenu à l'ICANN58 à Copenhague le 12 mars 2017. Puisque les attaques DDoS peuvent avoir un impact sérieux sur la cible (et potentiellement des dommages collatéraux pour d'autres), le comité permanent TLD-OPS estime qu'il est important de mobiliser l'expérience collective de la communauté TLD-OPS pour élaborer et documenter un cadre de travail pour mieux préparer les ccTLD à répondre à des attaques de DDoS.

L'atelier a facilité ce dialogue par un partage d'expériences, des débats et de la formulation d'idées.

Atelier d'atténuation des DDoS n° 2 — ICANN61, 2017-10-29, observations générales

Nous avions un petit groupe pour cet atelier : 22 personnes. Cela a permis une bonne dynamique & collaboration. Nous nous sommes réunis face à un tableau papier, avons examiné les résultats de l'atelier précédent, et développé chaque sujet pour se concentrer sur les éléments qui devront faire partie du guide, pour chaque étape du cycle de vie. Les résultats qui sont nés sur le tableau papier sont interprétés dans le présent document.

Les cycles de vie pour une atténuation « efficace » des DDoS sont :

- identifier
- Protéger
- Détecter
- Répondre
- Récupérer

La portée de ce document n'est pas d'élaborer un cadre de sécurité complexe pour atténuer les DDoS. L'objectif est de faire ressortir les éléments importants dans chaque cycle de vie pour qu'un ccTLD soit efficace à atténuer une attaque DDoS (si et lorsqu'il est mis en œuvre).

Il a été mentionné durant l'atelier que c'est toujours une bonne idée de mettre en œuvre les meilleures pratiques telles que la gestion de la sécurité des opérations du service IT et de l'informatique (ITIL) (cybersécurité).

IDENTIFIER :

L'objectif de l'IDENTIFICATION est de documenter et de comprendre l'infrastructure DNS de votre ccTLD avant qu'une attaque se produise -- à savoir qui appeler, sur qui compter, qui avertir (et la procédure d'escalade pour la résolution du problème). Vérifiez que vous avez une relation solide avec votre FAI, les fournisseurs, le gouvernement, la presse, les titulaires de noms de domaine et les utilisateurs d'Internet de votre ccTLD. C'est le travail qui doit être effectué en continu avant qu'une attaque se produise.

CONTACTS	
Votre équipe de gestion des ccTLD	Titre, nom, numéro de téléphone, numéro à domicile, e-mail personnel (Président du Conseil d'administration)
Numéro d'urgence de l'IANA	+1 (310) 306-6308 (à mettre à jour)
Vendeurs de diffusion anycast	E-mail et numéros de téléphone, numéros de contact des SOC/NOC
FAI de transit en amont	E-mail et numéros de téléphone, numéros de contact des SOC/NOC
FAI du pays	E-mail et numéros de téléphone des SOC/NOC
CERT	E-mail et numéros de téléphone des SOC/NOC Nom du contact, numéro de téléphone, adresse e-mail
Opérateurs principaux de résolveurs (Récursifs)	Adresses IP Opérateur, e-mail et numéros de téléphone
Liste de contacts TLD-OPS	Accès à la liste de contacts TLD-OPS
Médias	Nom du contact, numéro de téléphone, adresse e-mail
Organe de réglementation	Nom du contact, numéro de téléphone, adresse e-mail
Vendeurs de logiciels	Nom du contact, numéro de téléphone, adresse e-mail
Consultant en informatique légale	Nom du contact, numéro de téléphone, adresse e-mail
Titulaires de nom de domaine	Méthode pour joindre efficacement les titulaires
Autres contacts pertinents	

Étayer clairement l'infrastructure DNS de votre ccTLD :

Il est très important de bien documenter l'infrastructure DNS de votre ccTLD, avec le nom des serveurs opérationnels, leur emplacement physique, les connexions réseau, les fournisseurs de transit, les connexions IXP, les fournisseurs de diffusion Anycast PII, la capacité de chaque lien de transit et d'IXP.

C’est l’actif que vous devez protéger.

Serveur de nom de ccTLD, adresses IPv4 et IPv6.

```
Exemple...
;; SECTION AUTORITÉ :
dk.                     172800  IN      NS      a.nic.dk.
dk.                     172800  IN      NS      b.nic.dk.
…
;; SECTION SUPPLÉMENTAIRE :
a.nic.dk.               172800  IN      A       212.88.78.122
b.nic.dk.               172800  IN      A       193.163.102.222
b.nic.dk.               172800  IN      AAAA    2a01 : 630:0 : 80 :: 53
…
```

Topologie exacte du DNS, de réseau et de serveur :

Documenter le réseau, l’architecture du serveur et les logiciels pour l’infrastructure DNS de votre ccTLD, et mettre l’ensemble à jour régulièrement.

<insérer des diagrammes de réseau ici>

- Fournir des liens vers le réseau et les schémas de topologie

Adresses IP Maître Masquées

Maître masqué	
Adresse IP	Détails de la liste d’accès (au cas où vous auriez besoin d’ajouter un nouveau fournisseur)
Comment ajouter	Étapes rapides à suivre pour ajouter un nouveau serveur de nom…

Infrastructure signature DNSSEC

Ajouter ici des détails de votre infrastructure DNSSEC et les protections/stockage de clés.

Les serveurs de noms récursifs importants utilisant votre ccTLD (un exemple serait les serveurs de noms récursifs d’un grand fournisseur d’accès de votre pays desservant une importante population)

Récursif	
Nom du FAI	Adresses IP
Comment faire une liste blanche	Étapes rapides pour mettre en liste blanche certains récursifs ?

Gardez vos informations à jour :

Accès aux informations importantes	
Sécurité par un mot de passe	Emplacement (pour accéder aux routeurs et

	serveurs)
Stocks d'équipement	Emplacement (quelle est l'adresse IP, le nom)
Plan de communication	Emplacement (comment nous sensibilisons, communiquons)
Rôles et responsabilités	Emplacement (qui fait quoi et quand)
Plans BCP, RD	Emplacement

Processus de gestion des risques :

Identifier les risques, l'impact associé et la probabilité dans le cas où cela se produirait, et les cartographier sur l'analyse d'impact commercial pour le(s) service(s) de l'impact commercial de cette analyse pour le ccTLD résoudre le ou les service(s).de résolution du ccTLD. Créer un processus pour régulièrement revoir et mettre à jour ce document.

Processus de gestion du changement :

Il est essentiel que cette information reste à jour ; mettez en œuvre des processus pour conserver cette information à jour. Créez un processus trimestriel pour revoir et mettre à jour ce document.

PROTÉGER :

L'objectif de PROTECTION est d'élaborer et de mettre en œuvre les garanties appropriées pour assurer la livraison de vos services DNS autoritaires de ccTLD, et d'activer la capacité de contenir ou de limiter l'impact d'une attaque DDoS.

Dans le cas spécifique des attaques DDoS, le résultat de PROTECTION est d'élaborer et de mettre en œuvre les meilleures pratiques en matière de sécurité telles que les contrôles d'accès, les technologies de protection, la diversité et l'architecture DNS. Cette section se concentre sur l'identification des meilleures pratiques en matière de sécurité (processus) pour la technologie, les personnes et les partenaires.

Technologie :

Mettez en place des mesures de protection pour assurer la sécurité et la stabilité des opérations.

Listes d'accès :

- Liste de contrôle d'accès (ACL), le cas échéant, autorise uniquement le trafic à destination du port 53 (TCP/UDP)
- ACL pour la gestion hors bande

Anycast :

- Mettez en œuvre la topologie DNS anycast mondialement pour augmenter la résilience de livraison
- Déployez les nœuds anycast pour augmenter la résilience (nœuds de DNS sans transit mondial), de préférence en :
    - Étendant votre DNS Anycast mondial avec des nœuds anycast locaux qui desservent une communauté résolveur « importante » (FAI majeure dans pays, gouvernement, réseaux régionaux)
    - Ajoutant des nœuds anycast locaux aux IXP clés

Autres protections :

- Diversité des logiciels de serveur DNS (Bind, NSD, nœud, etc…)
- Filtrage de trou noir déclenché à distance (RTBH)
- Matériel d'atténuation des DDoS
- Mettez en œuvre RRL (un impératif)
- Protection de l'interface de gestion (port physique/câble distinct, transit, tunnel VPN,…)
- Suffisamment de ressources système (au niveau capacité)
- Suffisamment de connectivité du réseau et de diversification dans la sélection du fournisseur de service (FAI, IXP, etc.)

Personnes/processus :

Formez l'équipe informatique

- Formations de sensibilisation à la sécurité
- Exercice annuel <— partagez un script sur la simulation d'attaque TLD-OPS DDoS
- Durcissement de configuration (meilleure pratique…) et tests PEN
- Comment utiliser les outils externes de surveillance DNS (c.à-d. DNSMON, DNS-OARC, BGPMon ou autres ?)
- Aucun changement manuel, utilisez un processus de gestion de config et changement

Travaillez en collaboration avec l’ISP (fournisseurs de transit) à l’avance

- Découvrez comment ils peuvent aider à atténuer les effets de futurs événements DDOS
- Assurez-vous qu’ils comprennent l’importance de votre ccTLD

Partenaires :

Travaillez avec des partenaires où des services d’atténuation des DDoS peuvent être utilisés :

- Ajoutez des fournisseurs anycast permanents tiers
- Sécurisez des fournisseurs anycast d’urgence tiers
- Enquêtez sur les services de lavage de DDoS

DÉTECTER :

L'objectif de DÉTECTION est d'élaborer et de mettre en œuvre les activités appropriées pour identifier -- en temps opportun -- l'apparition d'une attaque DDoS, et de déterminer la portée et l'ampleur de l'attaque DDoS. Plus le mécanisme de détection est bon, plus les techniques d'atténuation pourront être efficaces.

Les résultats de la DÉTECTION sont des processus de surveillance et de détection DNS internes et externes.

Surveillance :

Surveillance interne

- SNMP surveille le trafic (routeur, serveurs, liens)
- Résilience des notifications (SMS, e-mail) des alarmes de seuil
- Comprendre le fonctionnement normal pour chaque nœud.
- Outils d'analyse DNS
- Capture PCAP (donne un aperçu exhaustif lorsque l'incident se produit, mais les volumes de trafic peuvent créer un DoS interne lors d'une attaque DDoS, voir remarque ci-dessous)

Surveillance externe

- RIPE atlas DNSMON externe (temps de réponse de requête DNS, perte de requête et tendances)
- Statistiques de lien de transit de FAI (consommation réelle de trafic sortant à votre nœud de DNS)
- Surveillance SLA de l'ICANN (Système de surveillance API de l'ICANN (MoSAPI) (toujours au début du déploiement pour les ccTLD)
- Netlabs 360 — https://ddosmon.net/

Outils évolutifs (fonctionnel sous mode DDoS)

- PCAP, certains outils peuvent se casser sous DDoS ou négatif d'affecter les opérations
    - Procédure pour désactiver temporairement la collecte de données dans des conditions défavorables
    - Commande d'envoi à distance des journaux de transaction en temps réel l'afin de s'assurer qu'aucune perte de données ne se produit

Identifier le type d'attaque :

Comprenez l'attaque

- Type d'attaque
- Liste des attaques classiques, profil, ainsi que les outils et les mesures d'atténuation
- Origine (d'où vient-elle ?)
- Quels nœuds (ce qui est touché)
- Quel est l'impact réel sur les utilisateurs de l'Internet ?

RÉPONDRE :

L'objectif de la RÉPONSE est d'élaborer et de mettre en œuvre les activités appropriées pour prendre des mesures contre l'attaque DDoS détectée. La fonction Répondre prend en charge la possibilité d'atténuer l'impact d'un événement DDoS potentiel.

L'ensemble des actions de RÉPONSE comprend sa planification, les communications, son analyse et les mesures d'atténuation.

Planification de réponse :

Ne paniquez pas ! La communauté sera plus susceptible de détecter l'apparition d'un DDoS sur votre ccTLD en même temps que vous et la communauté veut vous aider à atténuer les attaques.

- Communiquez
- Continuez l'analyse
- Résolvez le problème
- Concentrez-vous sur le cœur du problème
- Documentez {ce que vous modifiez, et les observations}

Plan de communication :

La communication est essentielle pour atténuer l'attaque.

Mécanismes de communication	
CERT locale	Contactez la CERT locale même si l'attaque n'est pas entièrement identifiée
TLD-OPS	Envoyez un e-mail à Tld-ops@dns-oarc.net Demandez de l'aide pour identifier davantage l'attaque
Pont de conférence	Demandez aux TLD-OPS/l'ICANN d'ouvrir un pont de conférence pour collaborer à propos des mesures d'atténuation
Sensibilisation	Demandez et/ou autorisez les membres des TLD-OPS de joindre une autre lettre de diffusion/groupes pour qu'ils coopèrent dans l'atténuation de l'attaque
Autres	

RÉCUPÉRER :

L’objectif de la RÉCUPÉRATION consiste à élaborer et mettre en œuvre les activités appropriées pour maintenir les plans de résilience et restaurer les capacités ou les services qui ont été altérés par l’attaque DDoS. La fonction de récupération prend en charge la reprise rapide des opérations normales afin de réduire l’impact d’une attaque DDoS.

L’ensemble des actions de RÉCUPÉRATION comprennent sa planification, son amélioration, les leçons apprises et les communications.

Récupération :

- Revenez sur les mesures temporaires
- Restaurez l’infrastructure DNS à son état original
- Documentez les changements permanents
- Compilez les notes

Leçons tirées :

- Tenez une réunion bilan avec les parties prenantes appropriées (internes)
- Documentez :
    - Ce qui a fonctionné
    - Ce qui n’a pas fonctionné
    - Identifier les améliorations

Améliorations :

- identifier
- Évaluez
- Partagez
- Mettez en œuvre les améliorations

Communications :

- Communiquez avec les partenaires, clients et employés, titulaires de nom de domaine