Guide pour l'identification et l'atténuation des collisions de noms pour les professionnels des TI

1er août 2014
Version 1.1

Table des matières

1. Introduction

Après l'entrée d'un nouveau nom de domaine de premier niveau dans la racine du DNS mondial, les organisations pourront se rendre compte que les requêtes en résolution de certains des noms « internes » spécifiques à leur réseau renvoient différentes valeurs, donnant aux utilisateurs et programmes des résultats différents. Deux principaux problèmes se posent : les fuites de noms « internes » sur Internet, et les espaces de noms privés qui sont définis comme étant en conflit avec l'espace de noms du DNS mondial.

Ces différents résultats sont dûs au fait qu'une requête DNS envoyée à un gestionnaire de réseau et qui devait être résolue au niveau local, à l'aide d'un espace de nom interne, est dorénavant résolue à l'aide des nouvelles données de domaine de premier niveau dans le DNS mondial. Dans de telles circonstances, les requêtes qui n'étaient jamais censées quitter le réseau interne obtiennent désormais des résultats dans le DNS mondial, et ces résultats sont différents. Au minimum, les fuites de noms qui produisent des résultats différents peuvent s'avérer gênantes pour les utilisateurs (elles peuvent par exemple retarder l'accès aux pages Web). Elles peuvent également poser des problèmes de sécurité (tels que l'envoi d'e-mails au mauvais destinataire).

Le présent document présente les stratégies d'atténuation et de prévention pour les types les plus courants d'espaces de noms privés utilisés par les organisations. Il décrit ce à quoi les organisations peuvent se trouver confrontées en cas de fuites de noms internes dans le DNS mondial et recommande certaines pratiques en matière d'atténuation. La description et les recommandations ici prévues sont destinées aux professionnels des TI (gestionnaires de réseaux/systèmes et personnel du service informatique) qui disposent d'une compréhension générale du fonctionnement du DNS et de leurs systèmes de noms internes. Les lecteurs souhaitant en savoir plus sont priés de consulter les documents de l'annexe A. Ceux concernés par les questions de sécurité doivent tout particulièrement prendre connaissance des rapports du Comité consultatif sur la sécurité et la stabilité (SSAC) de l'ICANN.

L'ICANN, l'organisation assurant la gestion du contenu de la racine du DNS mondial, a élaboré le présent document en collaboration avec des experts en matière d'espaces de noms afin d'aider les organisations dont les espaces de noms privés peuvent entrer en conflit avec la racine du DNS mondial. L'ICANN a publié d'autres documents décrivant l'organisation du DNS mondial, la façon dont les nouveaux noms sont ajoutés à la racine du DNS, etc. L'annexe A du présent document donne des références bibliographiques eu égard à différents sujets. De plus, l'ICANN a récemment commencé à aider des organisations utilisant des espaces de noms privés afin de savoir à quel moment ces espaces de noms commenceront à entrer en collision ; ces aspects sont abordés aux sections 1.4 et 6.

Il convient de souligner que bien que le présent document traite des mesures d'atténuation en cas de collisions de noms, il n'aborde que les problèmes auxquels les organisations peuvent être confrontées lors de la résolution de noms. Il ne s'attaque pas à d'autres questions liées à l'exploitation même du DNS mondial. À titre d'exemple, les serveurs de noms racine du DNS mondial ont toujours reçu quantité de requêtes qui ne devaient en aucun cas être traitées par le DNS mondial (voir *SAC 045* à l'annexe A), mais les serveurs de noms racine ont en tout temps reçu suffisamment de ressources leur permettant de prendre en charge cet excès de requêtes. Les questions connexes liées aux serveurs de noms racine ne sont pas traitées dans le présent document. Il examine uniquement les conséquences des fuites par inadvertance des requêtes vers les serveurs de noms racine du DNS mondial.

L'ICANN a mis au point une page Web fournissant des supports d'information liés aux collisions de noms disponible à l'adresse suivante : http://www.icann.org/namecollision. Cette page contient

également un processus visant à apporter la preuve d'un préjudice grave suite aux collisions de noms provoquées par les nouveaux domaines génériques de premier niveau (gTLD).

1.1 Collisions de noms

Le DNS mondial est un espace de nom hiérarchique, et les noms du DNS sont composés d'une ou de plusieurs étiquettes formant un nom complet. Au sommet de la hiérarchie, on trouve la zone racine du DNS qui comprend un ensemble de noms tels que `com`, `ru`, `asia`, etc ; il s'agit des TLD (domaines de premier niveau) mondiaux, communément appelés « TLD ». Un exemple de nom de domaine complet (souvent appelé *nom de domaine pleinement qualifié* ou *FQDN*) est `www.ourcompany.com`.

Presque l'ensemble des espaces de noms privés sont également hiérarchiques. Il existe trois principaux types d'espaces de noms privés :

- **Espaces de noms ramifiés au DNS mondial** – Les espaces de noms ramifiés au DNS mondial sont raccordés via un nom résoluble dans le DNS mondial, mais toute la structure d'annuaire sous ce nom est gérée au niveau local avec des noms que les gestionnaires informatiques n'ont jamais souhaité rendre visibles dans le DNS mondial. Par exemple, prenez un espace de nom privé raccordé via le nom `winserve.ourcompany.com` : les noms dans cet espace de noms privé (`winserve`) sont gérés par le serveur de noms privé et ne sont pas visibles dans le DNS mondial.

- **Espaces de noms utilisant leurs propres racines avec des TLD privés** – La racine de l'espace de noms privé constitue une étiquette unique ne correspondant pas à un TLD mondial. Toute la structure d'annuaire, y compris celle du TLD privé, est gérée par des serveurs de noms privés qui ne sont pas visibles dans le DNS mondial. Par exemple, si l'espace de noms privé est raccordé dans `ourcompany`, alors les serveurs de noms privés sont également responsables de `www.ourcompany`, `region1.ourcompany`, `www.region1.ourcompany`, etc. Différents types d'espaces de noms utilisent leurs propres racines avec des TLD privés. On peut citer par exemple l'Active Directory de Microsoft (sous certaines configurations), le multicast DNS (RFC 6762) et les anciens services d'annuaire de LAN encore utilisés dans certaines zones d'Internet.

- **Espaces de noms qui sont créés via l'utilisation de listes de recherche** – Une liste de recherche est un résolveur de nom local (soit un espace de noms privé soit un résolveur récursif pour le DNS mondial). Une liste de recherche permet à un utilisateur de saisir des noms plus courts pour plus de commodité ; lors de la résolution, le serveur de noms ajoute les noms configurés à la droite du nom dans une requête. (Ces noms configurés sont également appelés *suffixes*.)

Les espaces de noms ramifiés au DNS mondial ne provoquent des collisions de noms que lorsqu'ils sont combinés avec des listes de recherche. Toute requête impliquant un FQDN provenant du DNS mondial n'entrera jamais, par définition, en collision avec un nom différent dans le DNS mondial. Une telle requête ne pourrait provoquer de collisions de noms que si elle était créée par inadvertance via l'utilisation de listes de recherche.

Le concept d'« espaces de noms privés » déconcerte de nombreuses personnes habituées à une utilisation typique d'Internet, c'est-à-dire des personnes qui sont uniquement sensibilisées au nommage du DNS mondial et qui pourraient être surprises d'apprendre que certaines requêtes en résolution de nom ne conduisent pas ou ne devraient pas conduire à l'envoi de requêtes au DNS mondial. Elles pourraient être encore plus surprises d'apprendre que certaines requêtes de noms sont délibérément censées débuter dans l'espace de noms privé, mais finissent dans le DNS global. Une raison

expliquant la survenue de collisions de noms est que les requêtes destinées au serveur de noms d'un espace de noms a débuté, à tort, dans le DNS mondial.

1.2 Collisions de noms dues à des TLD privés

Les collisions de noms surviennent suite à deux événements. Tout d'abord, une requête de nom de domaine complet qui est raccordé à un TLD privé s'échappe du réseau privé vers le DNS mondial. Deuxièmement, la demande localise dans le DNS mondial le même nom qui existe sur le réseau privé en vertu du TLD privé.

Une cause fréquente de telles collisions de noms est l'utilisation d'un nom dans un système tel que l'Active Directory de Microsoft qui n'est pas un TLD dans le DNS mondial au moment où le système est configuré, mais qui est ajouté ultérieurement au DNS mondial. Ce type de collision de noms est déjà survenu à maintes reprises par le passé et devrait se reproduire avec l'introduction de nouveaux TLD dans le DNS mondial (voir *Introduction au programme des nouveaux gTLD* à l'annexe A).

1.3 Collisions de noms dues à des listes de recherche

Le traitement des listes de recherche constitue une autre cause de collisions de noms. Si une requête n'est pas un FQDN, il s'agit d'un *nom court non qualifié*. Une liste de recherche contient un ou plusieurs suffixes. Ils sont ajoutés de façon itérative sur la droite d'une requête. Lorsqu'un résolveur n'est pas en mesure de résoudre un nom court non qualifié, il essaie de résoudre le nom en ajoutant des suffixes de la liste jusqu'à ce qu'un nom identique soit trouvé. Une liste de recherche est un outil utile ; toutefois, le traitement des listes de recherche prend en charge l'utilisation de noms courts non qualifiés qui ne sont pas des FQDN et crée ainsi par inadvertance des espaces de noms qui ne sont pas raccordés au DNS mondial. Dans ce cas, la collision de noms se produit lorsqu'une chaîne que l'utilisateur essaie d'utiliser en tant que nom court non qualifié est complétée par la liste de recherche et résolue en tant que FQDN.

Par exemple, prenons un résolveur de nom disposant d'une liste de recherche comprenant les suffixes `ourcompany.com` et `marketing.ourcompany.com`. Supposons qu'un utilisateur saisisse `www` dans un programme qu'utilise ce résolveur. Le résolveur peut tout d'abord rechercher `www`, et si aucun résultat n'est obtenu, il peut alors chercher `www.ourcompany.com` et `www.marketing.ourcompany.com`.

Veuillez remarquer l'utilisation du terme « peut » dans la description de cet exemple. Les règles relatives à la façon dont les listes doivent être appliquées lors d'une résolution de nom dépendent des systèmes d'exploitation ou des applications. Certains systèmes essaieront toujours de résoudre un nom soit dans l'espace de noms privé soit dans le DNS mondial avant d'appliquer la liste de recherche. Toutefois, d'autres systèmes utiliseront d'abord la liste de recherche si la chaîne recherchée ne comprend pas de caractère « `.` ». Encore d'autres utiliseront la liste de recherche si la chaîne recherchée finit par un caractère « `.` ». Certains systèmes d'exploitations et certaines applications (tels que les navigateurs) ont plusieurs fois modifié leurs règles relatives aux listes de recherche. Il est ainsi impossible de prévoir si des listes de recherche seront ou ne seront pas utilisées, ce qu'est ou n'est pas un nom court non qualifié, et donc si les noms courts non qualifiés sont susceptibles ou non de s'échapper vers le DNS mondial. Voir *Problèmes relatifs aux nouveaux gTLD : noms sans point et collisions de noms* à l'annexe A pour de plus amples informations concernant la diversité du traitement des listes de recherche.

Cette description des listes de recherche pourrait étonner certains lecteurs dans la mesure où elles sont si fréquentes qu'on ne s'imagine pas, à première vue, qu'elles puissent créer des « espaces de noms privés ». Chaque suffixe dans une liste de recherche définit un autre espace de noms qui peut

être consulté lors de la résolution de noms. Cela crée un espace de noms privé qui fonctionne de manière fiable uniquement lorsque le client envoie une requête aux résolveurs en question pour ledit espace de noms. En fonction de la mise en œuvre de la liste de recherche, certains résolveurs de noms peuvent même essayer le nom court non qualifié saisi par l'utilisateur ou configuré via un logiciel avant d'ajouter les noms dans la liste de recherche. Par exemple, taper `www.hr` sur un emplacement d'Internet peut produire un résultat à partir du résolveur de DNS, mais taper la même chose sur un autre emplacement peut produire un résultat différent. Lorsque cela se produit, l'un de ces espaces de noms est « privé » par rapport à l'autre.

Avoir recours aux listes de recherche au lieu de résoudre des FQDN via le DNS mondial entretient l'incertitude liée à la résolution de noms. Il est difficile de prévoir les collisions de noms dues à des listes de recherche car les listes de recherche sont monnaie courante. Elles font partie du logiciel du résolveur de noms dans bon nombre de systèmes d'exploitation, équipements réseau, serveurs, etc. Le logiciel du résolveur agit différemment d'un système à l'autre, d'une version à une autre du même système d'exploitation, et même selon la détermination par le système d'exploitation ou l'application de l'endroit sur le réseau d'où provient la demande. Le déploiement d'un service de résolution de noms résolvant les noms uniquement à l'aide du DNS mondial constitue la meilleure garantie contre l'incertitude et l'imprévisibilité des résultats.

1.4 Aide à la détection des collisions de noms dans les nouveaux gTLD

À partir du 18 août 2014, lorsqu'un gTLD sera délégué de la zone racine du DNS, le gTLD sera tenu d'assurer un service d'*interruption contrôlée* pendant 90 jours. Lors de la période d'interruption contrôlée, des réponses facilement identifiables sont envoyées des serveurs de noms faisant autorité pour les nouveaux gTLD pour toute une variété de requêtes DNS. Le but de ces réponses est d'avertir les organisations qui seront confrontées à des collisions de noms qu'elles devront prendre des mesures immédiates afin de prévenir tout dommage éventuel lié à la fuite de requêtes.

En outre, à compter de la même date, certains gTLD déjà situés dans la zone racine seront tenus d'assurer un service d'interruption contrôlée pendant 90 jours avant de déléguer certains noms de deuxième niveau au DNS mondial. Le but étant ici le même que précédemment : informer les organisations coupables de fuites de requêtes qu'elles doivent atténuer les éventuels dommages dès que possible.

Veuillez noter que ces règles ne s'appliquent qu'aux gTLD et non aux TLD de code pays (couramment appelés « ccTLD »). Lorsqu'un ccTLD est ajouté à la zone racine, son opérateur peut décider d'une interruption contrôlée, mais ce n'est pas une obligation.

2. Problèmes causés par les collisions de noms

Les collisions de noms liées à des fuites de requêtes depuis des réseaux privés vers le DNS mondial peuvent avoir des effets indésirables. Lorsqu'une requête obtient une réponse positive, mais si la réponse est donnée par le DNS mondial et non par l'espace de noms qui devait la donner, l'application à la base de la requête tentera de se connecter à un système ne faisant pas partie du réseau privé, et pourrait obtenir ce qu'elle souhaite. Une telle connexion pourrait constituer un désagrément (en retardant la résolution de nom). Elle pourrait également soulever un problème en termes de sécurité, c'est-à-dire qu'elle pourrait créer une vulnérabilité susceptible d'être exploitée à des fins malveillantes, selon les actions ultérieures entreprises par l'application.

2.1 Redirection vers des sites Web indésirables

Supposons qu'un utilisateur saisisse `https://finance.ourcompany` dans son navigateur sur un réseau privé, et que le réseau ait un espace de noms dont le TLD privé est `ourcompany`. Si la requête du navigateur pour le nom `finance.ourcompany` est résolue comme prévu, le navigateur obtient une adresse IP pour le serveur Web interne du service financier. Imaginons alors que le TLD `ourcompany` fasse également partie du DNS mondial et que ce TLD ait comme nom de domaine de deuxième niveau (SDL) `finance`. En cas de fuite de la requête, le nom sera résolu avec une adresse IP différente de celle utilisée lorsque la requête a été résolue dans l'espace de noms privé. Imaginons à présent que cette adresse IP différente puisse héberger un serveur Web. Le navigateur tenterait de se connecter à un serveur Web sur Internet, et non sur un réseau privé.

Tel que montré précédemment, le même problème peut survenir sur des réseaux ne disposant pas de TLD privés mais utilisant des listes de recherche. Prenons un navigateur normalement utilisé sur un réseau où des utilisateurs disposent d'une liste de recherche ayant comme nom `ourcompany.com`, et imaginons que l'utilisateur saisisse le nom `www.finance` afin d'accéder à l'hôte `www.finance.ourcompany.com`. Imaginons à présent que le navigateur soit utilisé par un employé à partir d'un dispositif mobile dans un café. Si cette requête s'échappe d'Internet, et qu'il y a un TLD appelé `finance`, la requête pourrait être résolue via une adresse IP différente, par exemple un hôte complètement différent dont le nom dans le DNS mondial est `www.finance`. Cette requête pourrait conduire le navigateur à tenter de se connecter à un serveur Web sur une partie d'Internet tout autre que si la requête était parvenue au résolveur sur le réseau privé.

Généralement, dans un tel scénario, l'utilisateur se rendrait compte qu'il s'agit du mauvais site Web et le quitterait immédiatement. Toutefois, un navigateur peut donner un grand nombre d'informations à un serveur Web si le navigateur « fait confiance » au serveur Web du fait qu'il ait le même nom de domaine que l'un des noms de domaine que le navigateur a visité au préalable. Le navigateur peut automatiquement saisir son identifiant ou d'autres données sensibles, exposant ainsi ces informations au risque de capture ou d'analyse hors de l'organisation. Dans d'autres circonstances (par exemple une attaque soigneusement formulée à l'encontre de l'organisation), le navigateur pourrait se connecter à un site hébergeant un code malicieux installant des programmes dangereux sur l'ordinateur.

Veuillez noter que l'utilisation de certificats TLS et numériques peut empêcher de prévenir un dommage dû à des collisions de noms ; en fait, cela peut même aggraver la situation en donnant aux utilisateurs un faux sentiment de sécurité. Bon nombre des autorités de certification (CA) émettant des certificats pour des noms dans le DNS mondial émettent également des certificats pour des noms courts non qualifiés dans des espaces d'adressage privés, de sorte qu'il est possible qu'un utilisateur

qui est redirigé par erreur sur un site voie encore un certificat valide. Voir *SAC 057* à l'annexe A pour de plus amples informations relatives aux certificats avec des noms provenant d'espaces de noms privés.

2.2 Envoi d'e-mails aux mauvais destinataires

Les éventuelles conséquences découlant des collisions de noms ne sont pas limitées aux navigateurs Web. Un e-mail destiné à un individu peut être envoyé à un destinataire différent si les noms de l'hôte dans les adresses du destinataire sont identiques ; par exemple, un e-mail envoyé à `chris@support.ourcompany` pourrait être transmis à un tout autre compte d'utilisateur si `ourcompany` devient un TLD dans le DNS mondial. Même si le message n'est pas transmis à un utilisateur donné, tentative peut être faite de l'envoyer, et une telle tentative peut exposer le contenu de l'e-mail au risque de capture ou d'analyse hors de l'organisation.

De nombreux dispositifs réseau tels que pare-feux, routeurs et même imprimantes peuvent être configurés afin d'envoyer des notifications ou des données enregistrées par e-mail. Si le nom du destinataire saisi à des fins de notifications par e-mail est par la suite soumis à une collision de noms dans le DNS mondial, la notification sera transmise à un destinataire tout autre. Des données d'événements ou enregistrées contenues dans le corps du message et pouvant révéler la configuration du réseau et le comportement de l'hôte peuvent être transmises à un autre destinataire. Les performances normales du réseau ou l'analyse du trafic par le personnel informatique peuvent être interrompues si le destinataire visé de telles données ne reçoit jamais les données enregistrées, ou les événements déclenchant les notifications peuvent ne pas faire l'objet d'une enquête ou de mesures d'atténuation.

2.3 Réductions de la sécurité

Les situations de collision de noms auxquelles il n'est pas remédié peuvent exposer les systèmes des réseaux privés à des comportements ou dommages indésirables. Les systèmes qui reposent sur la résolution de noms et qui assurent également des fonctions de sécurité peuvent fonctionner de manière fiable lorsqu'ils utilisent des FQDN et les résolvent à partir du DNS mondial.

Par exemple, eu égard aux pare-feux, les règles de sécurité sont souvent fondées sur la source ou la destination d'un flux de paquets. La source et la destination des paquets sont des adresses IPv4 ou IPv6, mais de nombreux pare-feux leur permettent d'être saisies également sous forme de noms de domaine. Si des noms courts non qualifiés sont utilisés et que la résolution de noms n'est pas menée tel que prévu, il est possible que les règles ne permettent pas de bloquer ou d'autoriser le trafic comme le gestionnaire l'avait prévu. De même, les journaux de pare-feu utilisent souvent des noms de domaine, et le recours à des noms courts non qualifiés effectuant une résolution de manière imprévisible peut interférer avec le suivi, l'analyse des événements ou la réponse qui y est apportée. Le personnel informatique qui examine les journaux peuvent, par exemple, ne pas bien appréhender la gravité d'un événement du fait qu'un nom court non qualifié dans le journal peut identifier différents hôtes en fonction du lieu de création du journal (c'est-à-dire, dans le journal, le même nom court non qualifié peut sembler être associé à au moins deux adresses IP différentes). Ce problème peut être compensé par le fait que la plupart des pare-feux peuvent agir comme leur propre résolveur de DNS ou permettre aux gestionnaires d'utiliser ou de configurer des listes de recherche.

2.4 Systèmes affectés par les collisions de noms

L'ensemble des systèmes liés à un réseau doivent faire l'objet d'un contrôle afin de déterminer s'ils utilisent des noms d'hôte raccordés à un TLD privé ou des noms d'hôte basés sur des listes de

recherche. Toutes ces utilisations devront être mises à jour afin d'utiliser un FQDN du DNS mondial. Voici une liste non exhaustive de systèmes ou applications devant faire l'objet d'un contrôle :

- **Navigateurs** – Les navigateurs Web permettent aux utilisateurs de préciser l'emplacement des proxys HTTP, ces derniers se trouvant très souvent sur le réseau privé. Vérifiez si un utilisateur ou un membre du personnel informatique possède une page d'accueil personnalisé, des signets ou des moteurs de recherche : ces éléments peuvent avoir des liens vers des serveurs sur le réseau privé. Certains navigateurs disposent également d'options de configuration permettant d'obtenir des informations de révocation sur les certificats SSL/TLS qui peuvent être associées à des noms d'hôte sur le réseau privé.

- **Serveurs Web** – Les serveurs Web proposent un contenu HTML comprenant des liens et des métadonnées ayant des noms d'hôte intégrés. Vérifiez si le contenu des serveurs Web sur un réseau privé donné comprend des noms courts non qualifiés. Vérifiez si les fichiers de configuration pour le serveur Web contiennent des noms courts non qualifiés d'autres hôtes sur le réseau privé.

- **Agents d'utilisateur de messagerie** – Les clients de messagerie tels que Outlook et Thunderbird ont tous des options de configuration permettant de déterminer où recevoir des e-mails à l'aide de protocoles POP ou IMAP, et où envoyer des e-mails sur le protocole SUBMIT ; ils peuvent tous utiliser des noms d'hôte sur le réseau privé. Vérifiez si ces applications sont configurées afin d'obtenir des informations de révocation sur les certificats SSL/TLS à partir de noms courts non qualifiés attribués à des hôtes.

- **Serveurs de messagerie** – Vérifiez si les serveurs de messagerie ont des configurations indiquant les noms courts non qualifiés d'autres hôtes locaux, telles que des passerelles e-mail de sauvegarde, des serveurs de stockage hors ligne, etc.

- **Certificats** – Vérifiez si les applications ayant recours à des certificats X.509, telles que des programmes de téléphonie et de messagerie instantanée, ont des données de configuration utilisant des noms courts non qualifiés afin d'identifier où recevoir des informations de révocation sur les certificats SSL/TLS.

- **Autres applications** – Des applications personnalisées peuvent avoir des paramètres de configuration dans lesquels peuvent être stockés des noms d'hôte. L'espace le plus adapté serait les fichiers de configuration, mais des noms d'hôte peuvent apparaître dans de nombreux types de données d'application, liens sur médias sociaux ou sites wiki, ou peuvent même être encodés dans un code source. Vérifiez si ces données de configuration comprennent des noms courts non qualifiés.

- **Dispositifs réseau** – Vérifiez les dispositifs d'infrastructure réseau (pare-feux, systèmes de gestion des événements et des informations de sécurité (SIEM), routeurs, transferts, dispositifs de suivi du réseau, systèmes de détection ou prévention d'intrusion, serveurs VPN, serveurs DNS, serveurs DHCP, serveurs de connexion) afin de déterminer s'ils sont configurés avec des noms courts non qualifiés d'autres dispositifs sur le réseau privé.

- **Administration client** – Vérifiez si les outils d'administration client centralisés tels que ceux configurant les postes de travail et les dispositifs réseau d'une organisation ont des noms courts non qualifiés dans les configurations (notamment les listes de recherche) qui sont contrôlées et réinitialisées par les systèmes.

- **Dispositifs mobiles** – Les biens de consommation tels que téléphones et tablettes peuvent avoir des options de configuration similaires à celles des applications indiquées ci-dessus, et

donc des choix de configuration pouvant contenir des noms courts non qualifiés à partir du réseau local.

L'ensemble de ces systèmes doivent faire l'objet d'un contrôle afin de détecter la présence de données de configuration stockant des noms courts non qualifiés afin de veiller à ce que ces noms puissent être modifiés en cas de changement de la racine de l'espace de nom privé ou lorsque l'on cesse d'utiliser des listes de recherche.

3. Quand atténuer les collisions de noms

Les noms sont parfois ajoutés à la zone racine du DNS mondial, par exemple en cas de changement du nom d'un pays, ou lorsque l'ICANN délègue de nouveaux TLD. Les deux types de domaines de premier niveau ont été ajoutés presque chaque année depuis plus de vingt ans. De nouveaux TLD ont été ajoutés en 2013 et 2014 et il ne fait aucun doute que d'autres seront ajoutés au cours des années à venir.

L'histoire montre que des collisions de noms se sont produites lors d'ajout de TLD au DNS. L'histoire montre également que des noms se sont échappés des espaces de noms privés pendant de nombreuses années, parfois très fréquemment ; voir *SAC 045* à l'annexe A pour de plus amples informations. Il a été prouvé que les espaces de noms et la résolution de noms destinés aux réseaux privés n'ont jamais été aussi séparés que les gestionnaires le pensaient, et que les requêtes de noms que les gestionnaires souhaitent résoudre par des serveurs de noms internes sont parfois envoyées aux résolveurs dans le DNS mondial.

Les gestionnaires de réseaux choisissent parfois des noms en se fondant sur l'hypothèse selon laquelle la liste de noms dans la racine du DNS mondial est immuable, alors que cette liste a en fait changé et changera au fil du temps. Par exemple, lorsque le TLD `cs` a été ajouté il y a presque 25 ans pour la Tchécoslovaquie, de nombreuses universités utilisaient des listes de recherche qui permettaient à un utilisateur de saisir un nom finissant en `cs` pour le service des sciences informatiques qui serait pleinement qualifié avec le nom de domaine de l'université, et ces décisions ont conduit à une incertitude en matière de résolution de noms lorsque le nouveau TLD était ajouté à la zone racine car les noms finissant en `cs` étaient à présent des FQDN dans le DNS mondial. Même lorsque des noms racine du DNS mondial ne se chevauchent pas avec ceux d'un espace de noms privé (soit un TLD privé soit une liste de recherche), les gestionnaires de réseaux oublient souvent de se tenir informés des noms qui sont dans la racine du DNS mondial.

Il est recommandé qu'un service informatique commence à prendre des mesures d'atténuation dès que possible. Décider d'améliorer le pare-feu peut réduire certaines collisions mais ne les éradiquera jamais toutes. De même, veiller à ce que les utilisateurs utilisent des serveurs de noms appropriés ou faire en sorte que les travailleurs à distance utilisent des réseaux VPN permet de réduire certaines collisions mais pourrait également compromettre la détection des collisions restantes.

Des collisions de noms peuvent survenir indépendamment des caractères du nom ; toutefois, l'utilisation de caractères non ASCII tels que `ä`, `中` et `ǐ` dans des TLD privés complique l'analyse des collisions. Les résolveurs peuvent envoyer des requêtes concernant ces collisions selon des manières difficiles à prévoir, et peuvent ne pas respecter les normes d'Internet ; ainsi, déterminer le moment où les collisions de noms se produiront est très complexe.

Bien que la racine du DNS mondial finira par être plus grande qu'elle ne l'a été par le passé, l'ajout de noms à la racine n'a rien d'extraordinaire. Pour chaque ajout de nouveau TLD, il existe une possibilité de collisions de noms avec des espaces de noms privés qui se sont échappés vers Internet, pour la plupart sans que personne ne s'en rende compte. Pendant des années, les organisations ont utilisé des noms et assumé les risques de collisions.

Veuillez noter que l'ajout de nouveaux noms à la racine du DNS ne constitue pas, et ne constituera pas, un problème pour les organisations utilisant déjà des FQDN du DNS mondial dans leur réseau. Ces organisations ne verront aucune différence par rapport à leur propre utilisation des noms du DNS, car il n'y a pas de collisions de noms. Les problèmes ne se posent que pour les organisations utilisant

des TLD privés, ou les organisations utilisant des listes de recherche permettant la saisie de noms courts non qualifiés lorsque le nom raccourci même peut être un nom valide dans le DNS mondial.

3.1 Détermination du potentiel de collisions

Afin que vous déterminiez si oui ou non il y aura des collisions de noms avec l'espace de noms privé de votre organisation, vous devez identifier et répertorier tous les espaces de noms privés ainsi que les listes de recherche du DNS que votre organisation utilise, puis établir une liste des noms de premier niveau dans ces sources. Pour la plupart des organisations, il n'existe en règle générale qu'un espace de noms avec un seul nom de premier niveau, mais certaines organisations, notamment celles qui se sont associées à d'autres organisations qui utilisaient également des espaces de noms privés (par exemple suite à une fusion ou acquisition), ont de multiples noms de premier niveau privés.

Vous devez par la suite déterminer le contenu actuel et prévu de la zone du DNS mondial. Les noms dans la zone racine actuelle pour le DNS mondial sont disponibles à l'adresse suivante : http://data.iana.org/TLD/tlds-alpha-by-domain.txt. Afin de déterminer si un nom issu d'un espace de noms privé est examiné à des fins d'attribution via le programme des nouveaux TLD en cours, suivez les étapes suivantes :

1. Rendez-vous à https://gtldresult.icann.org/application-result/applicationstatus.
2. Cliquez sur la flèche dans la colonne « Chaîne ».
3. Faites défiler les pages jusqu'à trouver le nom de votre espace de noms privé.

En cas de chevauchement entre la liste de TLD privés que vous venez d'établir et la liste de noms dans la zone du DNS, il est possible que se produisent des collisions de noms, et des mesures d'atténuation doivent alors rapidement être prises.

Veuillez noter qu'après la saisie de la série actuelle de nouveaux TLD dans la zone racine, d'autres peuvent être proposés ; et notamment, la liste de nouveaux TLD peut changer et des collisions de noms entre des espaces de noms privés et de futurs nouveaux TLD peuvent se produire. De même, des organisations dotées de TLD privés constitués de deux lettres (telles que `ab`) doivent savoir que les noms de domaine de premier niveau en deux lettres peuvent être utilisés uniquement comme codes pays, et qu'ils sont ajoutés à la zone racine via une procédure complètement différente.

3.2 gTLD du DNS mondial dont la délégation est reportée indéfiniment

L'ICANN a annoncé qu'elle reporterait indéfiniment la délégation de trois TLD : .corp, .home et .mail. Ces gTLD sont toujours largement utilisés dans des espaces de noms privés et créent donc un risque accrue de collisions par rapport aux autres TLD. Il ne s'agit pas d'un report à vie ; toute organisation utilisant l'un de ces noms en tant qu'espace de noms privé doit alors respecter les orientations prévues aux sections 4 et 5 eu égard à la migration depuis l'espace de noms privé. Toutefois, de telles organisations disposent de davantage de temps afin de réaliser la migration qu'une organisation qui a utilisé un nom différent pouvant apparaître dans la racine du DNS mondial dans un avenir proche.

4. Étapes visant à atténuer les problèmes associés à un TLD privé

L'utilisation de TLD privés n'a pas été recommandée comme meilleure pratique depuis plusieurs dizaines d'années. En fait, les instructions accompagnant l'Active Directory de Microsoft et les produits serveur déconseillent clairement depuis plusieurs années l'utilisation de TLD privés. La mesure d'atténuation la plus efficace pour des collisions de noms dues à des noms qui finissent en TLD privé s'échappant du DNS mondial est d'utiliser un TLD raccordé au DNS mondial au lieu d'un TLD privé.

Les étapes prévues dans cette section s'appliquent à tout réseau qui a choisi, pour des raisons qui lui appartiennent, d'utiliser un TLD privé en tant que racine et d'utiliser des listes de recherche afin de résoudre des noms courts non qualifiés au lieu de raccorder son espace de noms dans le DNS mondial et d'envoyer une requête au DNS mondial à des fins de résolution de FQDN. Cette section s'applique à toute organisation qui utilise un TLD privé, et pas seulement celles dont les requêtes de noms s'échappent vers Internet. Si votre organisation utilise ce que vous considérez être un TLD privé « sécurisé », à savoir un nom n'ayant pas encore fait l'objet de demande ou pas encore autorisé à être délégué dans la racine du DNS mondial, vous devriez quand même envisager sérieusement d'adopter un nom raccordé au DNS mondial. Si vous travaillez dans une grande organisation disposant de plus d'un TLD privé (telle qu'une société ayant fusionné avec une autre société et n'ayant pas fusionné ses deux espaces de noms), les étapes prévues dans cette section doivent être effectuées pour chaque TLD privé.

Il y a de grandes chances que l'organisation ait pris la décision d'utiliser un TLD privé en ayant en tête une convention de nommage précise. Les étapes ici prévues pourraient se trouver en conflit avec ce modèle original. Afin de limiter de manière fiable les problèmes associés aux collisions de noms dues aux TLD privés, les utilisateurs et systèmes doivent changer leur façon d'utiliser les noms de domaine, et les serveurs de noms locaux doivent être reconfigurés d'une façon que certains utilisateurs pourraient juger contraignante. Utilisez les explications des effets indésirables ou inattendus pouvant affecter votre organisation afin de sensibiliser et de faciliter l'acceptation au sein de la communauté d'utilisateurs.

Important : En même temps que vous effectuerez les étapes de cette section, vous devrez probablement atténuer les collisions de noms provoquées par des listes de recherche, aspect abordé dans la section 5. Bon nombre d'étapes prévues dans cette section sont identiques aux étapes de la présente section et peuvent être effectuées en même temps.

4.1. Suivi des requêtes destinées aux serveurs de noms faisant autorité

Afin de limiter les difficultés liées à un TLD privé, indiquez tous les ordinateurs, équipements réseau et tout autre système utilisant le TLD privé actuel dans toute requête. En cas de modification des noms utilisés, tous les dispositifs utilisant les anciens noms privés de manière automatisée devront être mis à jour.

Il existe trois principales façons de réaliser ce suivi et cette énumération de systèmes :

- Le serveur de noms faisant autorité (par exemple l'Active Directory) peut disposer d'une fonction d'enregistrement. Activez la fonction d'enregistrement afin de rassembler les informations relatives à l'ensemble des requêtes pour les noms privés.

- Bon nombre de pare-feux modernes peuvent également être configurés afin de détecter et d'enregistrer les requêtes pour les noms privés. Cela peut ne pas être aussi efficace que d'enregistrer directement depuis le système de nommage, selon la topologie de votre réseau. Par exemple, si une requête ne parvient pas à un pare-feu, le pare-feu ne peut voir la requête qui sera ainsi ignorée.

- Si aucune des deux options précédentes ne peut être utilisée, suivez et rassemblez le trafic transmis au et émis par le serveur de noms faisant autorité à l'aide d'un programme de capture de paquets tel que Wireshark. Toutefois, cette méthode implique que les données capturées soient traitées avec un programme afin de trouver les requêtes uniquement pour les noms privés.

Certains organisations choisiront (et devront choisir) plus d'une des options susmentionnées afin d'accroître leurs chances de trouver l'ensemble des requêtes. Veuillez noter que cette étape peut produire des résultats confus. Les dispositifs tels qu'ordinateurs et téléphones ont des applications dans lesquelles les utilisateurs saisissent des noms ; ces dispositifs apparaîtront dans l'enquête même s'il n'y a pas de versions stockées des anciens noms privés. Dans le cadre de cette étape, il est seulement nécessaire de connaître tous les endroits dans votre réseau où l'ancien nom privé est stocké et utilisé pour des applications.

4.2. Création d'un inventaire de chaque système à l'aide du TLD privé de manière automatisée

Vous devez disposer d'un résumé des données enregistrées obtenues lors de l'étape précédente. Ce résumé doit consister en une liste de tous les dispositifs et tous les noms faisant l'objet d'une requête et non de chaque cas de requête réalisée par le dispositif. Vous devez disposer de tous les noms faisant l'objet d'une enquête car certains dispositifs auront de multiples applications qui devront chacune être mises en place. Ainsi, le résumé doit comprendre tous les systèmes et toutes les applications sur chaque système qui utilisent le TLD privé. Ce résumé devient le manifeste pour les dispositifs devant être changés.

4.3. Détermination de l'endroit où vos noms du DNS mondial sont administrés

Il est probable que vous ayez déjà un nom du DNS mondial pour votre organisation et que le nom de domaine puisse être utilisé pour la racine de votre espace de noms privé. Vous devez déterminer la personne en charge de vos noms de DNS ainsi que les processus qui devront être utilisés afin de créer et de mettre à jour les noms dans le DNS. Cela peut être effectué au sein de votre service informatique ou via un prestataire de service (bien souvent la même société qui vous fournit une connexion Internet).

4.4. Changement de la racine de votre espace de noms privé afin d'utiliser un nom du DNS mondial

Une stratégie courante permettant d'utiliser un nom de DNS mondial en tant que racine de votre espace de noms privé consiste à disposer d'un nom publiquement accessible délégué à partir du DNS mondial mais après à utiliser votre serveur de noms faisant autorité afin d'administrer l'ensemble des noms se trouvant sous la houlette de ce dernier. Par exemple, si le nom de domaine mondial de votre société est `ourcompany.com`, vous pouvez choisir `ad1.ourcompany.com` en tant que nom de racine.

Si votre organisation a plus d'un nom de domaine au sein du DNS mondial, vous devez raccorder vos noms à un nom pouvant être facilement contrôlé par le personnel informatique de votre organisation. Dans certains cas, des noms supplémentaires sont contrôlés par d'autres entités, par exemple un service marketing. Si possible, il convient de raccorder votre nom sous un nom déjà contrôlé par le service informatique.

Les étapes permettant d'effectuer ce changement dépendent du logiciel de serveur de noms privé que vous possédez, de la version de ce logiciel, de la topologie des serveurs de noms sur votre réseau privé et de la configuration existante du serveur de noms. Ces informations ne relèvent pas du présent document mais doivent vous avoir été fournies dans les instructions de votre vendeur pour votre système actuel. De même, dans de nombreuses organisations, ce changement devra faire l'objet d'une autorisation par certains niveaux de direction, notamment si la gestion des noms du DNS mondial est différente de la gestion de l'espace de noms privé.

Dans le cadre de cette étape, si vous disposez de certificats pour tout hôte utilisant des noms dans l'espace de noms privé, vous devez créer des certificats pour ces hôtes à l'aide des nouveaux noms (qualifiés). Les étapes permettant d'obtenir ces certificats dépendent de votre CA et ne relèvent donc également pas du présent document.

4.5. Attribution de nouvelles adresses IP pour des hôtes, le cas échéant

Si vous possédez des certificats TLS basés sur le nom de votre ancien TLD privé, vous devrez obtenir de nouveaux certificats pour les nouveaux noms. Si votre serveur Web ne prend pas en charge l'extension indication du nom du serveur (SNI) du protocole TLS qui permet à plus d'un nom de domaine d'être servi en vertu de TLS sur la même adresse IP, vous devrez ajouter des adresses IP aux hôtes de sorte que l'hôte prenne en charge l'ancien nom privé sur l'adresse IP originale et le nouveau nom sur une nouvelle adresse IP. Sinon, vous pouvez mettre à jour votre logiciel de serveur Web en téléchargeant une version assurant une prise en charge correcte des extensions SNI.

4.6. Création d'un système de suivi des équivalences entre les noms privés anciens et nouveaux

Lors du changement de l'ensemble des noms privés afin d'utiliser la nouvelle racine, vous continuerez à servir des adresses et à enregistrer des requêtes pour vos anciens noms privés afin de détecter la présence de systèmes non compris dans votre inventaire et qui n'ont pas été mis à jour afin d'utiliser les noms raccordés au DNS. De ce fait, vous devez vous assurer que les noms privés anciens et nouveaux présentent les mêmes valeurs pour les adresses IP.

Un logiciel d'espace de noms privé vous permet de maintenir les deux arbres en parallèle, mais si vous possédez un logiciel plus ancien ou de multiples serveurs de noms faisant autorité, il est probable que vous ayez à assurer un suivi des équivalences à l'aide d'outils personnalisés. Ces outils personnalisés doivent fréquemment interroger l'ensemble des noms dans les espaces de noms anciens et nouveaux, et vous avertir en cas de discordance afin que vous puissiez déterminer quel système a changé sans qu'un changement parallèle n'ait été effectué dans l'autre système.

Si vous deviez ajouter des adresses IP lors de l'étape précédente de par vos certificats SSL/TLS, la discordance doit être autorisée par le logiciel de suivi des équivalences.

4.7. Formation des utilisateurs et des gestionnaires de systèmes à l'utilisation du nouveau nom

En plus de changer les systèmes dans lesquels les noms sont saisis dans les configurations, vous devez changer les manières de penser des utilisateurs afin qu'ils passent des anciens noms privés aux nouveaux. Cette formation doit être dispensée avant la mise en œuvre des étapes suivantes afin que les utilisateurs puissent s'habituer aux nouveaux noms, mais il doit clairement ressortir de la formation que le changement est imminent et que les utilisateurs doivent commencer à penser avec les nouveaux noms. C'est également le bon moment pour former les utilisateurs à l'utilisation des FQDN. Utilisez les explications des effets indésirables et inattendus qui peuvent affecter votre organisation afin de sensibiliser et de faciliter l'acceptation.

4.8. Changement de tous les systèmes affectés avec les nouveaux noms

Il s'agit de la véritable transition entre les anciens noms privés et les nouveaux pour tous les systèmes (PC, dispositifs réseau, imprimantes, etc.) sur le réseau. Les noms privés sont remplacés par les nouveaux noms du DNS système par système. Chaque ancien nom privé est détecté via le logiciel sur le système et remplacé par le nouveau nom du DNS. En même temps, vous devez dénigrer l'utilisation des noms courts non qualifiés dans les listes de recherche.

Le suivi commencé précédemment est tout particulièrement important lors de cette étape. Vous ne serez probablement pas en mesure de déterminer l'ensemble des applications de tous les systèmes ayant les anciens noms privés intégrés dans ces derniers. Au lieu de quoi, le système de suivi doit être consulté après chaque changement du système afin de voir si le système effectue encore des requêtes pour les anciens noms privés.

De nombreux systèmes exécutent des applications d'initialisation lors de leur première activation. Ces applications peuvent avoir des noms de systèmes intégrés, et trouver l'ensemble de ces noms peut s'avérer complexe. Après que tous les noms d'un système ont acquis leurs nouveaux noms du DNS, redémarrez le système et utilisez le logiciel de suivi afin de voir apparaître les occurrences des noms. Si le système cherche l'un quelconque des anciens noms privés, vous devez déterminer quel logiciel provoque cette requête et le changer afin d'utiliser les nouveaux noms. Ce processus peut nécessiter quelques redémarrages afin de configurer entièrement et correctement le système.

4.9. Début du suivi de l'utilisation d'anciens noms privés au niveau du serveur de noms

Vous devez configurer votre serveur de noms faisant autorité afin de débuter le suivi de toutes les requêtes pour des noms disposant de l'ancienne racine. Du fait que les utilisateurs ne devraient plus utiliser ces noms, le journal créé lors de cette étape de suivi peut ne pas être très conséquent ; s'il l'est, vous devrez répéter certaines des étapes susmentionnées pour des systèmes spécifiques sur votre réseau.

4.10. Mise en place d'un suivi à long terme à des périmètres donnés pour rechercher les anciens noms privés

Les étapes précédentes doivent normalement avoir trouvé la grande majorité des utilisations des anciens noms privés, mais il est possible que quelques systèmes (éventuellement clés) continuent à utiliser les anciens noms privés, bien que probablement très peu. Une façon de détecter ces requêtes de noms consiste à ajouter des règles à tous les pare-feux sur le bord de votre réseau afin de détecter toute fuite de requêtes. Une haute priorité doit être associée à ces règles et ces dernières doivent être configurées de façon à générer des notifications d'événements visant à alerter le personnel informatique dans de brefs délais. Vous pouvez sinon trouver ces événements dans les journaux de pare-feu, mais cette option réduit les chances de les trouver. Les alertes qui sont déclenchées lors de requêtes permettront au personnel de détecter ces désormais rares (espérons-le) événements. Certains pare-feux prennent uniquement en charge ce type de règle en ajoutant de nouvelles fonctions moyennant des frais supplémentaires ; si cela est vrai pour votre pare-feu, vous devez évaluer le bénéfice lié à la détection de requêtes égarées par rapport à l'engagement de frais supplémentaires.

4.11. Changement de tous les noms de l'ancienne racine pour les diriger vers une adresse non fonctionnelle

Après la formation des utilisateurs, la manière la plus efficace de s'assurer qu'ils cessent d'utiliser les anciens noms privés avant de les supprimer est de diriger tous les anciens noms privés vers un serveur que vous aurez configuré afin qu'il ne réponde pas aux requêtes de service en tout genre. Cela permet également de se débarrasser de tout système utilisant encore l'ancien espace de noms et n'ayant pas été détecté lors des étapes précédentes.

L'adresse vers laquelle sont dirigés les anciens noms privés doit être un serveur dont on est sûr qu'il n'exécute aucun service. Ce faisant, il n'y a aucune chance qu'un système utilisant un ancien nom privé obtienne des informations erronées et que les applications ne communiquent des erreurs qui devraient être facilement détectables ou comprises par les utilisateurs ; dans le cadre de la formation de sensibilisation, vous pouvez conseiller aux utilisateurs de communiquer toutes les erreurs de ce type au personnel informatique. Lors de la mise en œuvre de cette étape, le système de suivi contrôlant les équivalences entre les anciens et les nouveaux noms (décrit ci-dessus) doit être mis à jour conformément aux changements.

Les noms doivent être changés un par un, probablement en laissant au moins quelques heures entre chaque changement ou ensemble de changements. Il est probable que le service informatique reçoive des appels lors de cette étape ; le fait d'activer les changements aidera alors à réduire le nombre des appels dans la mesure où les noms encore utilisés commencent à arrêter de fonctionner.

4.12. Révocation des certificats s'ils ont été émis pour des hôtes en vertu des anciens noms privés

Si votre organisation détenait des certificats SSL/TLS émis pour tous serveurs sur votre réseau utilisant les anciens noms privés, ces certificats doivent être révoqués. Cette démarche est relativement simple à effectuer si votre organisation est également sa propre CA. Si vous aviez recours à une CA commerciale afin d'émettre des certificats pour l'espace de noms privé, vous devez définir le processus de cette CA visant à demander une révocation : différentes CA peuvent avoir différentes exigences pour de telles demandes.

4.13. Opérations à long terme avec le nouveau nom

Veuillez noter que l'ancien nom privé et les domaines y afférents sont toujours servis et continueront d'être servis tant que vous exécuterez le serveur de noms. Rien ne justifie leur suppression et dans bien des systèmes tels que l'Active Directory, il peut s'avérer difficile de supprimer le premier nom configuré dans le système.

Il y a en fait une bonne raison de laisser le nom : cela vous permet de voir s'il existe des traces résiduelles de l'ancien nom privé dans des systèmes de votre réseau. Tant que les adresses associées à l'ensemble des noms appartenant à ce TLD privé sont dirigées vers un hôte n'exécutant aucun service, vous pouvez utiliser les journaux du serveur de noms (et, pour bénéficier de plus d'avantages, un système enregistrant tout le trafic de ce serveur) afin de déterminer si vous avez été efficace lors de la suppression de l'ancien nom privé.

5. Étapes permettant d'atténuer les collisions de noms associées aux listes de recherche

Afin de limiter de manière fiable les problèmes associés aux collisions de noms dues aux listes de recherche, les utilisateurs et systèmes doivent changer leur façon d'utiliser les noms de domaine. Il peut être utile de préparer à l'avance les utilisateurs via des notifications de changement, des programmes de sensibilisation et des formations.

Veuillez noter que si vous êtes déjà engagés dans un processus de centralisation des services administratifs, ces actions sont probablement moins complexes que vous ne le pensez. De nombreux individus utilisant normalement des listes de recherche savent qu'ils peuvent également saisir des noms complets si besoin est (comme s'ils accédaient à un serveur alors qu'ils ne se trouvaient pas sur le réseau privé de l'organisation), et leur formation sera alors plus courte que celle des individus ayant uniquement connaissance des noms courts non qualifiés.

5.1. Suivi des requêtes destinées au serveur de noms

Afin de limiter les problèmes liés aux listes de recherche, vous devez avoir connaissance de tous les ordinateurs, équipements réseau et autres systèmes utilisant des listes de recherche dans toute requête. Tous les dispositifs utilisant des listes de recherche de manière automatisée devront être mis à jour.

Il existe trois principales façons de réaliser ce suivi et cette énumération de systèmes :

- Le serveur de nom récursif (tel qu'Active Directory) peut disposer d'une fonction d'enregistrement, et vous pouvez activer la fonction d'enregistrement afin d'obtenir des informations concernant l'ensemble des requêtes ayant des noms courts non qualifiés.

- Bon nombre de pare-feux modernes peuvent également être configurés afin de détecter et d'enregistrer les requêtes de tous les noms. Cela peut ne pas être aussi efficace que d'enregistrer directement depuis le système de nommage, selon la topologie de votre réseau. Par exemple, si une requête ne parvient pas à un pare-feu, le pare-feu ne peut voir la requête qui sera ainsi ignorée.

- Si aucune des deux options précédentes ne peut être utilisée, le serveur de noms peut être suivi à l'aide d'un programme de capture de paquets tel que Wireshark. Toutefois, cette méthode implique que les données capturées soient traitées avec un programme afin de trouver les requêtes uniquement pour les noms courts non qualifiés.

Veuillez noter que cette étape peut produire des résultats confus. Les dispositifs tels qu'ordinateurs et téléphones peuvent avoir des applications dans lesquelles les utilisateurs saisissent des noms ; ces dispositifs apparaîtront dans l'enquête même s'il n'y a pas de versions stockées des anciens noms courts non qualifiés. Dans le cadre de cette étape, il est seulement nécessaire de connaître tous les endroits dans votre réseau où un nom court non qualifié est stocké et utilisé pour des applications.

5.2. Création d'un inventaire de chaque système à l'aide de noms courts non qualifiés de manière automatisée

Vous devez disposer d'un résumé des journaux obtenus lors de l'étape précédente. Ce résumé doit consister en une liste de tous les dispositifs et tous les noms courts non qualifiés faisant l'objet d'une requête et non de chaque cas de requête envoyée par le dispositif. Vous devez disposer de tous les noms faisant l'objet d'une requête car certains dispositifs auront de multiples applications qui devront chacune être mises en place. Ce résumé devient le manifeste pour les dispositifs devant être changés.

5.3. Formation des utilisateurs et des gestionnaires de systèmes à l'utilisation des FQDN

En plus de changer les systèmes dans lesquels les noms courts non qualifiés sont saisis dans les configurations (soit une configuration de l'ensemble du système soit la configuration d'une application individuelle), vous devez changer les manières de penser des utilisateurs afin qu'ils passent des noms courts aux noms complets.
Utilisez les explications des effets indésirables et inattendus qui peuvent affecter votre organisation afin de sensibiliser et de faciliter l'acceptation.

5.4. Changement de tous les systèmes affectés à des fins d'utilisation de FQDN

Remplacez les noms courts non qualifiés par leur FQDN équivalent système par système. Chaque nom court non qualifié qui est détecté via le logiciel sur le système doit être remplacé par le nom du domaine complet.

Le suivi commencé précédemment est tout particulièrement important lors de cette étape. Vous ne serez probablement pas en mesure de déterminer l'ensemble des applications de tous les systèmes modifiés ayant des noms courts non qualifiés intégrés dans ces derniers. Au lieu de quoi, le système de suivi doit être consulté après chaque changement du système afin de voir si le système effectue encore des requêtes pour les noms courts non qualifiés.

De nombreux systèmes exécutent des applications d'initialisation lors de leur première activation. Ces applications peuvent avoir des noms de systèmes reposant sur des listes de recherche intégrées, et trouver l'ensemble de ces noms peut s'avérer complexe. Après que tous les noms d'un système ont été changé afin d'utiliser les FQDN, redémarrez le système et utilisez le logiciel de suivi afin de voir apparaître les occurrences des noms. Si le système cherche l'un quelconque des noms courts non qualifiés, vous devez déterminer quel logiciel provoque cette requête et le changer afin d'utiliser les FQDN. Ce processus peut nécessiter quelques redémarrages afin de configurer entièrement et correctement le système.

5.5. Désactivation des listes de recherche au niveau des résolveurs de nom partagés

Il s'agit du véritable abandon des noms courts non qualifiés pour tous les systèmes (PC, dispositifs réseau, imprimantes, etc.) sur le réseau. Des listes de recherche peuvent exister sur tout système effectuant des résolutions de noms et réalisant des configurations d'autres systèmes, tels que le serveur DHCP. Ces systèmes sont souvent des serveurs de noms autonomes, mais ils peuvent aussi être des pare-feux ou autres dispositifs réseau. Indépendamment du type de système, les listes de

recherche doivent être désactivées sur chaque d'entre eux afin d'empêcher les utilisateurs d'essayer d'utiliser des noms courts non qualifiés au sein d'un espace de noms donné.

5.6. Début du suivi de l'utilisation de noms courts non qualifiés au niveau du serveur de noms

Vous devez configurer votre serveur de noms afin de débuter le suivi de toutes les requêtes pour des noms devant utiliser des listes de recherche. Si vous prévenez les utilisateurs à l'avance et leur dispenser une formation, ils ne devraient plus utiliser ces noms, le journal créé lors de cette étape de suivi pouvant alors ne pas être très conséquent ; s'il l'est, vous pourriez devoir répéter certaines des étapes susmentionnées pour des systèmes spécifiques sur votre réseau.

5.7. Mise en place d'un suivi à long terme à des périmètres donnés pour rechercher les noms courts non qualifiés

Les étapes précédentes doivent normalement avoir trouvé la grande majorité des utilisations des noms courts non qualifiés, mais il est possible que quelques systèmes (éventuellement clés) continuent à utiliser des noms courts non qualifiés, bien que probablement très peu. La meilleure façon de détecter ces requêtes de noms consiste à ajouter des règles à tous les pare-feux sur le bord de votre réseau afin de détecter toute fuite de requêtes. Une haute priorité doit être associée à ces règles et ces dernières doivent être configurées de façon à générer des notifications d'événements visant à alerter le personnel informatique dans de brefs délais. Vous pouvez sinon trouver ces événements dans les journaux de pare-feu, mais cette option réduit les chances de les trouver. Les alertes qui sont déclenchées lors de requêtes permettront au personnel de détecter ces désormais rares (espérons-le) événements. Certains pare-feux prennent uniquement en charge ce type de règle en ajoutant de nouvelles fonctions moyennant des frais supplémentaires ; si cela est vrai pour votre pare-feu, vous devez évaluer le bénéfice lié à la détection de requêtes égarées par rapport à l'engagement de frais supplémentaires.

6. Détection de collisions de noms dans les nouveaux gTLD

À compter du 18 août 2014, l'ICANN impose que les gTLD nouvellement délégués dans la zone racine aident les organisations à détecter les fuites de requêtes vers le DNS mondial pour les noms relevant du nouveau TLD. Cette aide durera 90 jours, probablement les premiers jours de présence du nouveau gTLD dans la zone racine ; suite à quoi, le nouveau gTLD agira comme tout autre TLD dans la zone racine. L'aide est assurée via un service d'« interruption contrôlée » décrit dans la présente section.

De toute évidence, une organisation devant atténuer des collisions de noms entre son espace de noms privé et le DNS mondial doit procéder à cette atténuation avant que le nouveau TLD correspondant n'entre dans la zone racine : elle ne doit pas attendre cette période de 90 jours. (Cela est particulièrement vrai pour les organisations ayant choisi un TLD en deux lettres pour leur nom, car ces noms ne sont pas tenus d'effectuer une interruption contrôlée.) Les interruptions contrôlées correspondent à un dernier avertissement envoyé à une organisation lui enjoignant de prendre rapidement des mesures d'atténuation avant que le TLD ne commence à donner de « vraies » réponses aux requêtes.

La présente section indique la façon dont est mise en œuvre une interruption contrôlée sur un serveur de noms faisant autorité, et comment elle apparaît dans les réponses aux requêtes. Cette section donne également des conseils aux organisations disposant d'espaces de noms privés afin de déterminer si les changements opérationnels auxquels elles font face sont dus à l'interruption contrôlée et, si c'est le cas, elle précise quoi faire eu égard à ces changements.

6.1 Description des interruptions contrôlées

Le service d'interruption contrôlée imposé par l'ICANN pour les nouveaux gTLD ajoutés à la zone racine après le 18 août 2014 est conçu afin de provoquer une interruption des dispositifs présentant des fuites de requêtes de noms de domaine dans les espaces de noms privés vers le DNS mondial. À l'heure actuelle, en cas de fuite d'une requête DNS dans le DNS mondial, les serveurs de noms racine renvoient une réponse avec un code indiquant que le domaine n'existe pas. (Techniquement, il s'agit du champ RCODE de l'en-tête de la réponse réglé sur une valeur de 3, mnémoniquement définie comme une réponse « NXDOMAIN ».)

Lors de la période de service de domaine contrôlé, aucune erreur NXDOMAIN n'apparaît dans la réponse. Cette réponse ne contient aucune indication d'erreur mais elle contient des données qui seront vraisemblablement repérées par le système qui a envoyé la requête. Il est impossible de concevoir une réponse qui sera toujours repérée car il existe de nombreux types de logiciels effectuant des requêtes DNS ; toutefois, l'interruption contrôlée imposée par l'ICANN pourra être observée sur des systèmes enregistrant de manière adéquate les erreurs, et sur des réseaux sur lesquels le trafic du DNS peut être observé par les gestionnaires de réseaux.

Les gTLD fonctionnant conformément à l'interruption contrôlée répondront à une grande variété de requêtes DNS de manière prévisible. La section 6.2 explique comment observer les comportements des systèmes obtenant des réponses d'interruption contrôlée à ces requêtes DNS.

- La requête DNS la plus courante est de loin pour les enregistrements A, à savoir les adresses IPv4 associées à un nom de domaine. Ces requêtes reviendront toujours avec l'adresse IPv4 de 127.0.53.53. Cette adresse est une adresse de bouclage pour l'hôte qui a envoyé la requête, de sorte que si l'application utilise cette adresse afin d'amorcer toute sorte de contact, elle recevra le message qu'elle aura envoyé. Cette action est bien évidemment très susceptible

d'échouer dans la mesure où tous les programmes effectuant des consultations DNS essaient d'utiliser l'adresse dans la réponse afin de contacter un autre serveur.

- Une autre requête DNS courante est pour les enregistrements contenant du texte, désignés sous le terme d'« enregistrements TXT ». Dans le cadre du service d'interruption contrôlée, la réponse d'enregistrement TXT sera toujours la même chaîne « Votre configuration du DNS requiert une attention immédiate, voir https://icann.org/namecollision ». Un système qui affiche de tels enregistrements de texte donne des informations relatives aux collisions de noms.

- Pour les requêtes DNS destinées aux serveurs de messagerie (techniquement, pour un enregistrement Mail eXchanger ou MX), le service d'interruption contrôlée répondra avec le nom de domaine votre-dns-requiert-attention-immédiate.<TLD>, où « <TLD> » est le TLD dans la requête DNS. Le nom de domaine peut être visible dans les réponses d'erreur du client de messagerie ou serveur de messagerie. La consultation de l'adresse du nom de domaine votre-dns-requiert-attention-immédiate.<TLD> renverra 127.0.53.53.

- Le service d'interruption contrôlée répondra aux requêtes d'enregistrements de service (SRV) avec le nom de domaine votre-dns-requiert-attention-immédiate.<TLD>. Les requêtes d'enregistrements SRV ne sont pas aussi courantes que les requêtes d'adresses IPv4, d'enregistrements de texte et de noms de serveur de messagerie mais sont de plus en plus fréquentes pour les applications les plus récentes telles que les messageries instantanées et la transmission vocale.

Un gTLD ajouté à la zone racine avant le 18 août 2014 peut également disposer d'un service d'interruption contrôlée pour un sous-ensemble des éventuels domaines de deuxième niveau dans le TLD. Les enregistrements renvoyés dans le cadre de l'interruption contrôlée pour ces noms sont identiques aux enregistrements décrits ci-dessus. L'ICANN a imposé que certains SDL ne puissent avoir accès au TLD, et ces noms pourraient devenir actifs peu de temps après avoir mené une interruption contrôlée pour les SLD.

6.2 Observation d'interruptions contrôlées

Il est important de noter qu'il n'existe aucune garantie qu'une application recevant une réponse d'interruption contrôlée agisse bien différemment qu'elle ne le faisait avant l'interruption contrôlée. Toutefois, il est fort probable que l'application se comporte différemment et cette différence prendra vraisemblablement la forme d'un échec ; cet échec aura espérons-le un message d'erreur qui lui sera associé et l'utilisateur de l'application en fera part à un gestionnaire de système chargé de gérer cette situation. Si le message d'erreur contient les adresses IPv4 127.0.53.53, cela indique clairement que l'erreur est due au fait que le programme a utilisé un nom issu d'un espace de noms privé qui s'est échappé vers Internet.

Les erreurs dues au service d'interruption contrôlée se produisent lorsqu'un programme qui obtenait auparavant des réponses NXDOMAIN aux requêtes commence à obtenir de vraies réponses. Bien évidemment, ces erreurs se produiront plus tard lorsque le nouveau gTLD répondra avec de véritables données, et le service d'interruption contrôlée ne durera probablement que les 90 jours imposés par l'ICANN. Pendant cette période, les erreurs seront plus évidentes car les messages d'erreur contiennent l'adresse IPv4 127.0.53.53, le texte « Votre configuration du DNS requiert une attention immédiate, voir https://icann.org/namecollision », ou un nom de domaine contenant « votre-dns-requiert-attention-immédiate ».

Des interruptions contrôlées peuvent également être observées sur le réseau d'une organisation si le gestionnaire de réseau recherche activement des messages DNS contenant ces réponses. Une telle recherche peut être effectuée via un TAP réseau au niveau de points d'entrée adéquats, ou peut être

effectuée sur un pare-feu. Ce type d'observation ne repose pas sur la visualisation des messages d'erreur sur l'ordinateur affecté ; au lieu de cela, le gestionnaire de réseau peut déterminer l'ordinateur dont les requêtes de noms dans des espaces de noms privés s'échappent du réseau de l'organisation.

Indépendamment de la façon dont l'interruption contrôlée est découverte, l'ordinateur obtenant la réponse d'interruption contrôlée doit être reconfiguré de façon à n'effectuer des requêtes DNS qu'au serveur de noms de l'organisation, et non au DNS mondial. Aucune norme ne précise une telle configuration, la configuration faisant toutefois normalement partie du système d'exploitation. Si l'ordinateur voit son réseau configuré par un serveur sur le réseau de l'organisation, communément appelé « serveur DHCP », la configuration de ce serveur doit être modifiée afin que les requêtes DNS soient dirigées au serveur de noms de l'organisation, et non au DNS mondial.

Un ordinateur obtenant une réponse d'interruption contrôlée peut indiquer que d'autres ordinateurs sur le réseau de cette organisation ont également obtenu cette réponse. Un administrateur de système doit immédiatement vérifier la configuration du DNS pour l'ensemble des ordinateurs présents sur le même réseau, même si ces ordinateurs ne montrent pas de signes d'obtention de réponses d'interruption contrôlée. Gardez à l'esprit que l'interruption contrôlée ne dure que 90 jours et que l'on dispose donc d'un temps limité afin de trouver des ordinateurs dont la configuration du DNS est incorrecte.

Bien sûr, procéder à de tels changements ne constitue qu'une atténuation temporaire pour le problème sous-jacent des collisions de noms. Les sections 4 et 5 du présent document donnent des conseils eu égard à la façon de procéder à des atténuations permanentes.

7. Résumé

Les collisions de noms sont susceptibles de produire des résultats inattendus pour des organisations utilisant des espaces de noms privés. Le présent document indique certains des résultats potentiels ainsi que les meilleures pratiques permettant de modifier la façon dont sont utilisés les espaces de noms privés au sein des organisations. Ce document décrit également l'interruption contrôlée comme moyen d'identification des situations dans lesquelles les collisions de noms pourraient se manifester clairement.

Pour les espaces de noms qui utilisaient un TLD privé qui est en passe de devenir (ou est déjà devenu) un TLD au sein du DNS mondial, les meilleures mesures d'atténuation sont celles qui font passer l'espace de noms à un espace de noms raccordé au DNS mondial. Pour les espaces de noms qui utilisent le raccourcissement de noms avec des listes de recherche, l'atténuation ne peut être réalisée qu'en supprimant l'utilisation des listes de recherche. Les étapes menant à ces mesures d'atténuation comprennent également un suivi à long terme du réseau privé afin de veiller à ce que tous les noms susceptibles de provoquer des collisions ne soient plus utilisés. Les organisations disposeront de moyens leur permettant d'indiquer à quel moment elles seront confrontées à des collisions de noms lors de la délégation de nouveaux TLD dans la zone racine.

Des mesures d'atténuation complètes pour les problèmes de collisions de noms devront avoir recours à des FQDN chaque fois qu'un nom de domaine est utilisé. Sur un réseau qui utilise déjà le DNS mondial, cela implique de ne pas utiliser de listes de recherche. Sur un réseau qui utilise un espace de nom privé, cela implique que l'espace de noms privé doit être raccordé au DNS mondial et ne pas utiliser de listes de recherche.

Annexe A : Pour en savoir plus

Les documents suivants ont été élaborés par différentes organisations au sein de l'ICANN. D'autres organisations proposent des documents pouvant également être utiles. Plus important encore, le vendeur de votre logiciel et/ou matériel informatique de serveur de noms peut disposer d'informations précieuses dans la rubrique support technique de son site Web.

A.1. Introduction au programme des nouveaux gTLD

Cette page décrit l'histoire, la mise en œuvre et l'évolution du programme visant à ajouter des centaines de nouveaux gTLD au DNS mondial. http://newgtlds.icann.org/en/about/program

A.2. Collisions de noms dans le DNS

L'ICANN a chargé Interisle Consulting Group, LLC d'élaborer ce rapport détaillé relatif aux potentielles collisions de noms. Il donne un aperçu des collisions de noms, présente des données sur des TLD n'existant pas actuellement qui font l'objet de requêtes au niveau des serveurs racine, et donne de nombreuses informations générales eu égard aux problèmes pouvant être soulevés par les collisions de noms. http://www.icann.org/en/about/staff/security/ssr/new-gtld-collision-mitigation-05aug13-en.pdf

A.3. Plan de gestion de l'occurrence de collision de noms dans les nouveaux gTLD

Il s'agit du plan adopté par l'ICANN concernant la façon de gérer les occurrences de collisions de noms entre les nouveaux gTLD et les espaces de noms privés. Il comprend également de nombreuses références aux commentaires reçus par l'ICANN eu égard à de précédentes propositions relatives aux collisions de noms dans la zone racine. http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-annex-1-07oct13-en.pdf

A.4. Cadre de gestion de l'occurrence de collision de noms

Ce document fait partie du plan de gestion de l'occurrence de collision de noms dans les nouveaux gTLD. Il définit les conditions du service d'interruption contrôlée pour les gTLD délégués dans la zone racine du DNS à compter du 18 août 2014. http://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf

A.5. Problèmes relatifs aux nouveaux gTLD : noms sans point et collisions de noms

Les listes de recherche sur différents systèmes peuvent donner différents résultats en fonction de l'élément du nom court non qualifié faisant l'objet d'une requête. Cet article traite des listes de recherche pour les domaines sans point (TLD qui ont des enregistrements d'adresse à leur sommet), mais la description du traitement de listes de recherche est intéressante à bien d'autres égards. https://labs.ripe.net/Members/gih/dotless-names

A.6. SAC 045 : Requêtes invalides de domaines de premier niveau au niveau de la racine du système de noms de domaine

Ce rapport du SSAC de l'ICANN décrit les types de requêtes pour les TLD qui ont été détectées par les serveurs racine au moment de son élaboration.

A.7. SAC 057 : Avis du SSAC sur les certificats de noms internes

Ce rapport du SSAC de l'ICANN décrit les implications en termes de sécurité et de stabilité pour les certificats contenant des noms (internes) privés. Il identifie une pratique des CA qui peut être exploitée par les pirates et pourrait faire peser un risque important sur la confidentialité et l'intégrité des communications réalisées sur Internet. http://www.icann.org/en/groups/ssac/documents/sac-057-en.pdf