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

5 Décembre 2013 Version 1.0

Table des matières

1. Introduction

Suite à l'entrée d'un nouveau nom de domaine de premier niveau dans la racine du DNS mondial, les organisations peuvent voir que les requêtes pour résoudre certains des noms « internes » spécifiques à leur réseau renvoient des valeurs différentes, les utilisateurs et les programmes recevant des résultats différents. Il existe d'autres problèmes fondamentaux : les noms « internes » qui s'échappent dans l'Internet mondial, et les espaces de noms privés définis comme étant en conflit avec l'espace de noms du DNS mondial.

La cause de ces différents résultats est qu'une requête DNS à un administrateur de réseau censée être résolue au niveau local, en utilisant un espace de noms interne, est maintenant résolue avec les données des nouveaux domaine de premier niveau dans le DNS mondial. Dans ces circonstances, les requêtes qui n'étaient pas censées quitter le réseau interne obtiennent maintenant des résultats dans le DNS global, et ces résultats sont différents. Au minimum, les noms divulgués qui produisent des résultats différents peuvent être ennuyeux pour les utilisateurs (ils pourraient par exemple retarder l'accès aux pages web). Ils peuvent également poser des problèmes de sécurité (tels que les courriers électroniques envoyés aux mauvais destinataires).

Ce document inclut les stratégies d'atténuation et de prévention pour les types les plus courants d'espaces de noms privés étant utilisés par les organisations. Ce document décrit ce que les organisations pourraient rencontrer lorsque les noms internes qui s'échappent dans le DNS global et spécifie les pratiques d'atténuation recommandées. La description et les conseils proposés ici sont adressés aux professionnels de l'informatique (administrateurs de réseaux, administrateurs de systèmes et personnel du service informatique) qui comprennent en général le fonctionnement du DNS et de leurs propres systèmes de noms internes. Les lecteurs voulant approfondir la question peuvent consulter les documents de l'annexe A. Les lecteurs préoccupés par la sécurité peuvent consulter les rapports du comité consultatif sur la sécurité et la stabilité de l'ICANN (SSAC).

L'ICANN, l'organisation qui administre les contenus de la racine DNS mondial, a préparé ce document en consultation avec les experts en matière d'espaces de noms pour aider les organisations dont les espaces privés peuvent se trouver en conflit avec la racine du DNS mondial. L'ICANN a publié d'autres documents décrivant l'organisation du DNS mondial et la manière dont les nouveaux noms sont ajoutés à la racine du DNS, etc. Pour plus d'informations, voir l'annexe A du présent document qui répertorie de nombreuses questions.

Il faut remarquer que bien que ce document aborde les mesures d'atténuation pour les collisions de noms, il traite seulement les problèmes que les organisations peuvent rencontrer lors de la résolution de noms. Il n'aborde pas les autres questions liées au fonctionnement du DNS global lui-même. Par exemple, les serveurs de noms racine du DNS mondial ont toujours reçu d'innombrables requêtes qui n'ont jamais être traitées par le DNS mondial (voir *SAC 045* à l'annexe A), mais les serveurs de noms racine ont aussi toujours été assez bien organisés pour être en mesure de répondre à ce grand nombre de requêtes. Des questions connexes concernant les serveurs de noms racine ne sont pas abordées dans ce document. Il porte seulement sur les conséquences des requêtes échappées par inadvertance dans les serveurs de noms racine du DNS public.

L'ICANN a développé un site Web qui fournit des documents d'information concernant les collisions de noms que vous trouverez à l'adresse http://www.icann.org/en/help/name-collision. Cette page inclut également un processus pour informer les préjudices manifestement graves produits suite aux collisions de noms causées par les nouveaux domaines de premier niveau génériques (gTLD).

1.1 Collisions de noms

Le DNS global est un espace de noms hiérarchique, et les noms dans le DNS sont composés d'une ou plusieurs étiquettes qui créent un nom complet. Au sommet de la hiérarchie se trouve la zone racine du DNS qui contient un ensemble de noms tels que `com`, `ru`, `Asie` et ainsi de suite ; ce sont les TLD mondiaux (domaines de premier niveau), normalement dénommés tout simplement « les TLD ». Un exemple d'un nom de domaine complet (souvent appelé un *nom de domaine entièrement qualifié* ou *FQDN*) pourrait être `www.ourcompany.com`.

Presque tous les espaces de noms privés sont aussi hiérarchiques. Il existe trois grands types d'espaces de noms privés :

- **Espaces de noms qui s'écartent du DNS mondial** – les espaces de noms privés qui s'écartent du DNS mondial sont enracinés sous un nom qui est résoluble dans le DNS mondial, mais dont la structure du répertoire est gérée localement avec les noms que les administrateurs des services informatiques n'ont jamais vus dans le DNS mondial. Par exemple, imaginez un espace de noms privé dans la racine sous `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 qui utilisent leurs propres racines avec des TLD privés** – la racine de l'espace de noms privé est un label unique qui n'est pas un TLD mondial. La structure de répertoire entière, 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 dans la racine `notreentreprise`, les serveurs privés sont donc également responsables de `www.ourcompany`, `region1.ourcompany`, `www.region1.ourcompany`et ainsi de suite. Il existe beaucoup de différents types d'espaces de noms qui utilisent leurs propres racines avec des TLD privés. Par exemple, *Active Directory* de Microsoft (dans certaines configurations), multicast DNS (RFC 6762) et des services de répertoire LAN plus anciens qui sont encore utilisés dans certains coins de l'Internet.

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

Les espaces de noms qui s'écartent du DNS global ne provoquent des collisions de noms que lorsqu'ils sont combinés à des listes de recherche. Par définition, toute requête comportant un nom de domaine entièrement qualifié (FQDN) venant du DNS mondial n'aura jamais de collision de nom avec un nom différent dans le DNS mondial. Une telle requête pourrait seulement provoquer des collisions de noms lorsque ceux-ci sont crées par inadvertance à travers l'utilisation de listes de recherche.

Le concept d'« espaces de noms privés » confond beaucoup d'utilisateurs qui sont tout à fait habitués à l'utilisation typique de l'Internet, c'est-à-dire les gens qui ne sont familiarisés qu'avec le nommage du DNS mondial et qui peuvent être surpris d'apprendre que certaines requêtes de résolution de noms ne sont pas ou ne devraient pas entraîner une requête dans le DNS mondial. Ils peuvent être encore plus surpris d'apprendre que certaines requêtes de noms commencent intentionnellement dans l'espace de noms privé, mais qu'elles finissent dans le DNS mondial. Les requêtes destinées à un serveur de noms d'un espace de noms privé, démarrées de manière incorrecte dans le DNS mondial, sont peut-être une des raisons pour lesquelles des collisions de noms peuvent se produire.

1.2 Collisions de noms dues aux TLD privés

Les collisions de noms se produisent à la suite de deux événements. En premier lieu, une requête pour un nom de domaine entièrement complet qui s'enracine dans un TLD privé s'échappe du réseau privé vers le DNS mondial. Deuxièmement, la requête repère dans le DNS mondial exactement le même nom qui existe dans le réseau privé sous le TLD privé.

Une cause fréquente de ce type de collisions de noms est l'utilisation d'un nom dans un système comme *Active Directory* de Microsoft qui n'est pas un TLD dans le DNS mondial lors de la configuration du système, mais qui est ajouté plus tard au DNS mondial. Ce genre de collision de noms est déjà arrivé plusieurs fois auparavant et il est censé se poursuivre avec l'introduction de nouveaux TLD dans le DNS mondial (voir l'*Introduction au programme des nouveaux gTLD* dans l'annexe A).

1.3 Collisions de noms dues aux listes de recherche

Une autre cause de la collision de noms est le traitement des listes de recherche. 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. Ceux-ci sont ajoutés en mode itératif sur le côté droit d'une requête. Lorsqu'un résolveur est incapable de résoudre un nom court non qualifié, il ajoute des suffixes de la liste car il tente de résoudre le nom jusqu'à ce qu'un nom correspondant soit trouvé. Une liste de recherche est une fonctionnalité utile ; toutefois, le traitement d'une liste de recherche s'adapte à l'utilisation de noms courts non qualifiés qui ne sont pas des FQDN et en conséquence crée, par inadvertance, des espaces de noms qui ne sont pas dans la racine du DNS mondial. Dans ce cas, la collision de noms se produit lorsqu'une chaîne que l'utilisateur a l'intention d'utiliser comme un nom court non qualifié est au contraire complétée par la liste de recherche et résolue comme un FQDN.

Par exemple, supposons qu'un résolveur de noms a une liste de recherche qui comprend les suffixes `ourcompany.com` et `marketing.ourcompany.com`. Supposons encore qu'un utilisateur saisit `www` dans un programme qui utilise ce résolveur. Le résolveur pourrait alors tout d'abord chercher des `www` et s'il n'y a pas de résultats, il pourrait chercher `www.ourcompany.com` et `www.marketing.ourcompany.com`.

Notez l'utilisation du mot « pourrait » dans la description de cet exemple. Les règles pour appliquer les listes de recherche lorsque vous effectuez la résolution de noms varient selon les systèmes d'exploitation ou les applications. Certains systèmes essaieront toujours de résoudre un nom dans l'espace de noms privé ou le DNS mondial avant d'appliquer la liste de recherche. Toutefois, d'autres systèmes utiliseront la liste de recherche en premier lieu si la chaîne recherchée ne contient pas un caractère « . ». D'autres encore utiliseront la liste de recherche si la chaîne recherchée finit par un caractère « . ». Certains systèmes d'exploitation et les applications (telles que les navigateurs web) ont changé les règles de leur liste de recherche à plusieurs reprises. Il est donc impossible de prédire quand est-ce que les listes de recherche seront utilisées ou non, ce qui est ou n'est pas un nom court non qualifié, et en conséquence si des noms courts non qualifiés sont susceptibles ou pas de fuir du DNS mondial. Voir *préoccupations sur les nouveaux gTLD : Noms sans point et collisions de noms* dans l'annexe A pour plus de détails en matière de diversité de traitement de la liste de recherche.

Cette description des listes de recherche peut surprendre certains lecteurs parce qu'elles sont très fréquentes dans les lieux qui à première vue, ne semblent pas créer des « espaces privés ». Chaque suffixe dans une liste de recherche définit un autre espace de noms qui peut être consulté au cours de la résolution de noms. Cela crée un espace de noms privé qui ne fonctionne de manière fiable que lorsque le client interroge les résolveurs particuliers pour cet espace de noms. Selon la mise en œuvre de la liste de recherche, certains résolveurs de noms pourraient même essayer le nom court non qualifié saisi par l'utilisateur ou configuré dans le logiciel avant d'ajouter les noms dans la liste de

recherche. Par exemple, si l'on tape `www.hr` dans un même endroit sur l'Internet cela pourrait produire un résultat du résolveur DNS, mais si on le tape dans un emplacement différent le résultat pourrait être différent. Lorsque cela se produit, l'un de ces espaces de noms est « privé » par rapport à l'autre.

Si l'on utilise les listes de recherche au lieu de résoudre les FQDN par le biais du DNS mondial, cela contribue à l'incertitude par rapport à la résolution du nom. Les collisions de noms produites par les listes de recherche sont difficiles à prévoir parce que les listes de recherche sont très couramment utilisées. Dans de nombreux systèmes d'exploitation, équipements de réseau, serveurs, etc., elles appartiennent à des logiciels de résolution de noms. Le logiciel du résolveur fonctionne de manière différente suivant le système, entre les différentes versions du même système d'exploitation et même comme une fonction du système d'exploitation ou de l'application ce qui dépend d'où vient la requête. Le déploiement d'un service de résolution de noms qui résout les noms en utilisant uniquement le DNS mondial est la meilleure assurance contre ces incertitudes et les résultats imprévisibles.

2. Problèmes provoqués par les collisions de noms

Les collisions de noms basées sur des requêtes qui s'enfuient dans le DNS mondial des réseaux privés peuvent avoir plusieurs conséquences inattendues. Lorsqu'une requête obtient une réponse positive, mais avec une réponse du DNS mondial au lieu de l'espace de noms privé espéré, l'application qui fait la requête essaiera de se connecter à un système qui ne fait pas partie du réseau privé et peut éventuellement réussir. Ce type de connexion pourrait être gênant (à cause du retard lors de la résolution du nom). Il pourrait également s'avérer être un problème de sécurité, c'est-à-dire, il peut entraîner une vulnérabilité qui pourrait être exploitée à des fins malveillantes, en fonction de ce que l'application fait après la connexion.

2.1 Diriger vers des sites Web inattendus

Supposons qu'un utilisateur saisit `https://finance.ourcompany` dans son navigateur Web ou sur un réseau privé, et que le réseau a un espace de noms dont le TLD privé est `notreentreprise`. Si la requête du navigateur pour le nom `finance.ourcompany` est résolue comme prévu, le navigateur reçoit une adresse IP pour le serveur web interne du département des finances. Imaginez, cependant, que le TLD `notreentreprise` fait également partie du DNS mondial, et que ce TLD a un nom de domaine de deuxième niveau (SLD) `Finances`. Si la requête s'enfuit, la résolution de l'adresse IP sera différente à celle qui aurait été résolue dans l'espace de noms privé. Imaginez maintenant que cette adresse IP différente pourrait héberger un serveur Web. Le navigateur tentera de se connecter à un serveur Web sur l'Internet public, et pas sur le réseau privé.

Comme indiqué précédemment, le même problème peut se produire même dans les réseaux qui n'ont pas de TLD privés, mais qui utilisent les listes de recherche. Pensez à un navigateur qui est normalement utilisé sur un réseau où les utilisateurs ont une liste de recherche contenant le nom `ourcompany.com`, et que l'utilisateur saisit le nom `www.finance` afin d'obtenir l'hôte `www.finance.ourcompany.com`. Imaginez maintenant que le navigateur est utilisé par un employé dans un dispositif mobile dans une cafétéria. Si cette requête fuit dans l'Internet et s'il y a un TLD dénommé `finance`, la requête pourrait résoudre une adresse IP différente, par exemple, un hôte complètement différent dans le DNS mondial dont le nom est `www.finance`. À partir de cette requête le navigateur essaiera de se connecter à un serveur Web dans une partie complètement différente de l'Internet public, ce qui est tout à fait différent du site auquel il serait connecté si la requête avait eu recours au résolveur sur le réseau privé.

Une réponse commune de l'utilisateur face à ce scénario est que l'utilisateur reconnaîtrait que le site Web n'était pas le bon et il le quitterait immédiatement. Cependant, un navigateur peut révéler un grand nombre d'informations à un serveur Web si le navigateur « croit » le serveur Web, car il a le même nom de domaine que celui que le navigateur a visité plus tôt. Le navigateur peut saisir automatiquement la connexion ou d'autres données sensibles, en mettant en risque les informations et qu'elles soient capturées ou analysées en dehors de l'organisation. Dans d'autres circonstances (par exemple, une attaque soigneusement formulée contre l'organisation), le navigateur peut se connecter à un site d'hébergement de code malveillant qui installe des programmes dangereux sur l'ordinateur.

Notez que l'utilisation de TLS et des certificats numériques pourrait ne pas aider à prévenir les dommages dus à des collisions de noms ; en fait, cela pourrait être pire car il donnerait aux utilisateurs un faux sentiment de sécurité. Un grand nombre d'autorités de certification (CA) qui émettent les certificats pour les noms dans le DNS mondial, émettent également des certificats pour les noms courts

non qualifiés dans des espaces d'adresses privés, de sorte qu'il est possible que l'utilisateur qui est mal dirigé vers un site pourrait toujours voir un certificat valide. Voir *SAC 057* à l'annexe A pour plus de détails sur les certificats de noms des espaces de noms privés.

2.2 Diriger le courrier électronique aux mauvais destinataires

Les conséquences possibles découlant de collisions de noms ne sont pas limitées aux navigateurs Web. Le courrier électronique censé être envoyé à un destinataire peut être envoyé à un destinataire différent si les noms d'hôte des adresses du destinataire sont les mêmes, par exemple, le courriel dirigé à `chris@support.ourcompany` pourrait être remis à un compte d'utilisateur complètement différente si `NotreEntreprise` devient un TLD dans le DNS mondial. Même si le message n'est pas livré à un utilisateur de messagerie particulier, il pourrait y avoir une tentative d'envoi qui pourrait exposer le contenu du courrier et que celui-ci soit capturé ou analysé en dehors de l'organisation.

De nombreux dispositifs de réseau tels que les pare-feu, les routeurs et même des imprimantes peuvent être configurés pour envoyer des notifications ou des données de connexion par courrier électronique. Si le nom du destinataire qui a été saisi pour les notifications par courriel fait par la suite l'objet de collision de noms dans le DNS mondial, la notification pourrait être remise à un destinataire non voulu. Un événement ou les données de connexion dans le corps du message peuvent révéler la configuration du réseau et les données de l'hôte peuvent fuir vers un destinataire non voulu. Les performances de routine du réseau ou l'analyse du trafic par le personnel TI peuvent être interrompus si le destinataire de ces données ne reçoit jamais les données de connexion, ou si les événements qui déclenchent les notifications ne peuvent être étudiés ou atténués.

2.3 Réductions de sécurité

Les occurrences de collision de noms qui sont moins atténuées peuvent exposer les systèmes dans des réseaux privés à un comportement inattendu ou nuisible. Les systèmes qui s'appuient sur la résolution de noms pour un fonctionnement correct et qui remplissent également des fonctions de sécurité *peuvent* fonctionner de manière fiable lorsqu'ils utilisent des FQDN résolus à partir du DNS mondial.

Par exemple, dans les pare-feu, les règles de sécurité sont souvent basées 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 permettent de les faire entrer également en tant que noms de domaine. Si les noms courts non qualifiés sont utilisés et la résolution du nom n'est pas effectuée comme prévu, les règles peuvent ne pas bloquer ou autoriser le trafic tel que prévu par l'administrateur. De même, les événements enregistrés par le pare-feu utilisent souvent des noms de domaine, et en utilisant des noms courts non qualifiés dont la résolution est imprévisible ils peuvent interférer avec la surveillance, l'analyse, ou la réponse des événements. Le personnel TI qui examine les événements pourrait, par exemple, mal comprendre la gravité d'un événement, car un nom court non qualifié dans la liste peut identifier différents hôtes en fonction de l'endroit où le journal a été créé (cela signifie que dans la connexion, le même nom court non qualifié pourrait être associée à deux ou plusieurs adresses IP différentes). Ce problème peut être aggravé par le fait que la plupart des pare-feux peuvent agir comme leurs propres résolveurs DNS ou permettre aux administrateurs d'utiliser ou de configurer des listes de recherche.

2.4 Systèmes affectés par les collisions de noms

Tous les systèmes connectés au réseau doivent être vérifiés pour l'utilisation de noms d'hôtes qui soient dans la racine d'un TLD privé ou des noms d'hôtes basés sur des listes de recherche. Tous ces cas « d'utilisation » devront être mis à jour pour utiliser un FQDN du DNS mondial. La liste non exhaustive des systèmes ou applications de vérification comprend :

- **Navigateurs** - Les navigateurs Web permettent aux utilisateurs de spécifier l'emplacement des HTTP d'enregistrement fiduciaire, et ceux-ci se trouvent très souvent sur le réseau privé. Vérifier si le personnel TI ou un utilisateur ont fait des pages d'accueil personnalisées, des signets ou des moteurs de recherche : ceux-ci peuvent avoir des liens vers des serveurs sur le réseau privé. Certains navigateurs ont aussi des options de configuration permettant de savoir où obtenir des informations de révocation des certificats SSL / TLS qui pourraient se référer à des noms d'hôte sur le réseau privé.

- **Serveurs Web** - Les serveurs Web proposent du contenu HTML qui contient des liens et des métadonnées qui ont intégré les noms d'hôte. Vérifiez si les serveurs d'un réseau privé d'Internet ont un contenu avec des noms courts non qualifiés. Vérifiez si les fichiers de configuration pour le serveur Web ont des noms courts non qualifiés des autres hôtes du réseau privé.

- **Agents de l'utilisateur de courrier électronique** - Des clients tels qu'Outlook et Thunderbird ont des options de configuration pour recevoir des courriers en utilisant les protocoles POP ou IMAP, et pour envoyer des courriers électroniques via le protocole SOUMETTRE ; des noms d'hôte sur le réseau privé pourraient être utilisés. Vérifiez si ces applications sont configurées pour obtenir des informations de révocation des certificats SSL / TLS des hôtes ayant des noms courts non qualifiés.

- **Serveurs de messagerie** - Vérifiez si les serveurs de messagerie ont des configurations qui répertorient les noms courts non qualifiés d'autres hôtes locaux, tels que la sauvegarde des passerelles de messagerie, les serveurs de stockage hors ligne, etc.

- **Certificats** - Vérifiez si les applications qui utilisent des certificats X.509, tels que la téléphonie et les programmes de messagerie instantanée ont des données de configuration qui utilisent des noms courts non qualifiés pour identifier où obtenir des informations de révocation des certificats SSL / TLS.

- **Autres applications** - Les applications personnalisées peuvent avoir de nombreux paramètres de configuration où les noms d'hôte peuvent être stockés. L'espace le plus évident serait dans les fichiers de configuration, mais les noms d'hôte pourraient apparaître dans de nombreux types de données d'application, les liens sur les médias sociaux ou des sites wiki, ou même être codés en dur dans le code source. Vérifiez ces données de configuration pour les noms courts non qualifiés.

- **Dispositifs de réseau** - Vérifiez les dispositifs d'infrastructure de réseau - pare-feux, systèmes de gestion de l'information et des événements de sécurité (SIEM), routeurs, commutateurs, dispositifs de surveillance de réseau, détection d'intrusion ou systèmes de prévention, serveurs VPN, serveurs DNS, serveurs DHCP, serveurs de connexion - afin de déterminer si ceux-ci sont configurés avec des noms courts non qualifiés d'autres périphériques ou dispositifs sur le réseau privé.

- **Administration des clients** - Vérifiez si les outils d'administration centralisés du client tels que ceux qui configurent les postes de travail de l'organisation et des dispositifs de réseau ont des

noms courts non qualifiés dans leurs configurations (en particulier les listes de recherche) qui sont contrôlés et redémarrés par les systèmes.

- **Appareils mobiles** - Les appareils grand public tels que les téléphones et les tablettes peuvent avoir des options de configuration similaire à certaines des applications mentionnées ci-dessus, et ils ont peut-être des choix de configuration qui pourraient contenir des noms courts non qualifiés du réseau local.

Tous ces systèmes devraient être vérifiés pour les données de configuration qui stockent les noms courts non qualifiés pour s'assurer que ces noms puissent être changés lorsque la racine de l'espace de noms privé se modifie ou lorsque les listes de recherche ne sont plus utilisées.

3. Quand atténuer les collisions de noms

Les noms sont parfois ajoutés à la zone racine du DNS mondial, par exemple, lorsque le nom d'un pays change, 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 deux décennies. De nouveaux noms ont été ajoutés cette année (2013), et il est prévu que d'autres seront ajoutés en 2014 et au-delà.

L'histoire montre que certaines collisions de noms ont eu lieu lorsque les TLD sont ajoutés au DNS. L'histoire montre également que les noms d'espaces de noms privés ont été divulgués depuis de nombreuses années, et dans certains cas, très fréquemment. Pour en savoir plus, voir *SAC 045* à l'annexe A. L'histoire montre que les espaces de noms et la résolution de noms prévue pour les réseaux privés ne sont jamais séparés aussi complètement que les administrateurs ne le pensent, et que les requêtes de noms que les administrateurs ont l'intention de résoudre par les serveurs de noms internes sont parfois envoyées aux résolveurs dans le DNS mondial.

Les administrateurs de réseau choisissent parfois des noms fondés sur l'hypothèse que la liste des noms dans la racine du DNS mondial est immuable, mais en fait, cette liste subit et subira des changements au fil du temps. Par exemple, lorsque le TLD `cs` a été ajouté il y a près de 25 ans pour la Tchécoslovaquie, de nombreuses universités utilisaient des listes de recherche qui ont permis à un utilisateur d'entrer un nom se terminant par `cs` pour le département informatique qui serait entièrement qualifié avec le nom de domaine de l'université, et ces décisions ont conduit à la résolution incertaine du nom lorsque le nouveau TLD a été ajouté à la zone racine parce que les noms se terminant en `cs` étaient maintenant des FQDN dans le DNS mondial. Même lorsque les noms actuels de la racine DNS mondiale ne sont souvent pas chevauchés avec les noms dans un espace privé (soit un TLD privé ou une liste de recherche), les administrateurs de réseau oublient souvent de se mettre à jour sur les noms qui se trouvent dans la racine du DNS mondial.

Il est recommandé que le département TI commence les efforts d'atténuation dès que possible. Au cas où la position de « nous ferons tout simplement mieux avec notre pare-feu » serait adoptée, cela pourrait réduire certains types de collision, mais il serait impossible de les éliminer complètement. De même, si l'on disait : « nos utilisateurs seront en toute sécurité s'ils utilisent nos serveurs de noms » ou « nous ferons que les travailleurs à distance utilisent des VPN » il serait possible de réduire certains types de collisions, mais dans ce cas, les collisions restantes seraient plus difficiles à diagnostiquer.

Les collisions de noms peuvent se produire indépendamment des caractères utilisés dans le nom, mais l'utilisation de caractères non-ASCII, comme `ä` et `中` et `ѝ` dans des TLD privés complique l'analyse des collisions. Les résolveurs peuvent envoyer des requêtes sous des modalités difficiles à prévoir et peuvent ne pas atteindre les normes requises par l'Internet, de sorte que le fait de déterminer quand est-ce que collisions de noms auront lieu résulte bien plus difficile.

Bien que la racine du DNS mondial soit plus grande qu'elle ne l'a été au cours des dernières années, l'ajout de noms à la racine n'est vraiment pas inhabituel. Pour chaque nouveau TLD étant ajouté, il est possible que des collisions de noms avec des espaces de noms privés qui ont fui vers l'Internet, la plupart du temps inaperçues, se produisent. Les organisations ont utilisé des noms et ont assumé le risque de collisions pendant des années.

Notez que l'ajout de nouveaux noms à la racine du DNS n'est pas, et ne sera jamais un problème pour les organisations qui utilisent déjà les FQDN du DNS mondial dans leur réseau. Ces organisations ne verront aucune différence pour leur propre utilisation de noms DNS, car il n'y a pas de collisions de noms. Les problèmes apparaissent seulement pour les organisations qui utilisent les TLD privées ou

celles qui utilisent des listes de recherche permettant l'entrée des noms courts non qualifiés où le nom raccourci lui-même pourrait être un nom valide dans le DNS mondial.

3.1 Déterminer les risques de collisions

Pour déterminer s'il y aura ou pas des collisions de noms avec l'espace privé de votre organisation, vous devez identifier et cataloguer tous les espaces de noms privés et les listes de recherche du DNS utilisés par votre organisation, et par la suite compiler une liste des noms de premier niveau dans ces sources. Pour la plupart des organisations, il existe généralement un seul espace de noms avec un seul nom de premier niveau, mais certaines organisations, notamment celles combinées avec d'autres organisations qui utilisent également des espaces de noms privés (par exemple, suite à une fusion de l'entreprise ou de son acquisition), il existe des noms de premier niveau privés multiples.

Ensuite, vous devez déterminer à la fois les contenus actuels et attendus de la zone du DNS mondial. Vous trouverez les noms de la zone racine actuelle du DNS mondial à l'adresse http://data.iana.org/TLD/tlds-alpha-by-domain.txt. Pour déterminer si un nom d'un espace de noms privé est considéré pour son attribution par le programme des nouveaux gTLD qui est actif en 2013 :

1. rendez-vous sur https://gtldresult.icann.org/application-result/applicationstatus
2. Cliquez sur la flèche dans la colonne « String » (*chaîne)*
3. Faites défiler les pages jusqu'à ce que vous trouviez la plage qui contient le nom de votre espace privé.

S'il existe un chevauchement entre la liste des TLD privés que vous venez de faire et la liste des noms dans la zone DNS, il y aura probablement des collisions de noms, et en conséquence l'atténuation s'avère nécessaire maintenant.

Notez qu'une fois que la série actuelle des nouveaux TLD sera entrée dans la zone racine, autre chose peut être proposée ; en particulier, la liste des nouveaux TLD peut changer et les collisions de noms entre les espaces de noms privés et les futurs nouveaux TLD peuvent se produire. En outre, les organisations avec des TLD privés à deux caractères (comme `ab`) doivent être conscientes que les noms de domaine de premier niveau à deux caractères sont réservés pour les codes géographiques, et ceux-ci sont ajoutés à la zone racine à travers une procédure tout à fait différente.

4. Mesures pour atténuer les problèmes associés à un TLD privé

L'utilisation des TLD privés n'a pas été une pratique recommandée depuis des décennies. En fait, les instructions de l'*Active Directory* de Microsoft et des produits pour les serveurs ont explicitement découragé l'utilisation des TLD privés pendant de nombreuses années. Les mesures d'atténuation les plus efficaces pour les collisions de noms produites par des noms qui finissent dans un TLD privé qui s'enfuit au DNS mondial sont de ne plus utiliser un TLD privé mais d'en utiliser un qui soit dans la racine du DNS mondial

Les étapes de cette section s'appliquent à tout réseau ayant choisi, pour ses propres raisons, d'utiliser un TLD privé comme sa racine et d'utiliser des listes de recherche pour résoudre les noms courts non qualifiés au lieu d'avoir un espace de noms dans la racine du DNS mondial et demander au DNS mondial de résoudre les FQDN. Le présent article s'applique à toute organisation qui utilise un TLD privé et non seulement à celles qui ont divulgué des requêtes de noms dans l'Internet mondial. Si votre organisation utilise ce que vous percevez comme un TLD privé « sûr », c'est à dire un nom qui n'est pas encore appliqué pour ou approuvé pour être délégué dans la racine du DNS mondial, vous devez toujours envisager sérieusement le passage à un nom qui se trouve dans la racine du DNS mondial. Si vous travaillez dans une grande entreprise avec plus d'un TLD privé (comme une société fusionnée avec une autre entreprise mais n'ayant pas fusionné ses deux espaces de noms), les étapes de cette section doivent être effectuées pour chaque TLD privé.

Il existe la possibilité que lorsque l'organisation a choisi d'utiliser un TLD privé, sa décision ait été prise sur la base d'une convention de nommage particulière à l'esprit. Dans ce cas, les étapes peuvent être en conflit avec ce modèle d'origine. Dans le but d'atténuer de manière fiable les problèmes liés à des collisions de noms dues aux TLD privés, les utilisateurs et les systèmes doivent changer la façon dont ils utilisent les noms de domaine, les serveurs de noms locaux devant être reconfigurés d'une manière que certains utilisateurs peuvent trouver inopportune. Utilisez les explications des conséquences inattendues ou indésirables qui peuvent affecter votre organisation afin de sensibiliser et de favoriser l'acceptation au sein de votre communauté d'utilisateurs.

Remarque importante : En même temps que vous suivez les étapes de cet article, vous aurez probablement besoin d'atténuer les collisions de noms causées par des listes de recherche, point qui est traité dans l'article 5. Un grand nombre des étapes de cet article sont les mêmes, et elles peuvent être réalisées en même temps.

4.1. Surveiller les requêtes venant des serveurs faisant autorité

Afin d'atténuer les problèmes avec un TLD privé, lister tous les ordinateurs, le matériel de réseau, et tout autre système utilisant le TLD privé actuel dans toutes les requêtes. Si vous changez les noms utilisés, tous les appareils qui utilisent les anciens noms privés de manière automatisée devront être mis à jour.

Il existe trois méthodes courantes pour effectuer cette surveillance et l'inventaire des systèmes :

- le serveur de noms faisant autorité (comme *Active Directory)* peut avoir une fonction de journalisation. Activez la fonction de journalisation pour recueillir les détails de toutes les requêtes pour les noms privés.

- de nombreux pare-feu modernes peuvent également être configurés pour détecter et identifier les requêtes de noms privés. Cela peut ne pas être aussi efficace que la connexion du système de nommage lui-même, en fonction de la topologie de votre réseau. Par exemple, si une requête ne passe pas par un pare-feu, le pare-feu ne peut pas voir la requête, et en conséquence elle sera perdue.

- si aucune des méthodes précédentes ne peut être utilisée, surveiller et collecter le trafic livré et émis par le serveur de noms faisant autorité en utilisant un programme de capture de paquets tel que Wireshark. Cependant, cette méthode exige que les données capturées soient traitées avec un programme dans le but de trouver les requêtes pour les noms privés.

Certaines organisations choisiront (et devraient le faire) de suivre une ou plusieurs des méthodes précédentes pour augmenter les chances de trouver toutes les requêtes. Notez que cette démarche peut produire des résultats déroutants. Les dispositifs tels que les ordinateurs et les téléphones ont des applications dans lesquelles les utilisateurs tapent des noms; ces dispositifs apparaîtront dans l'enquête, même si toutes les versions stockées des anciens noms privés pourraient ne pas apparaître. Pour cette étape, il est seulement nécessaire de connaître tous les endroits dans votre réseau où l'ancien nom privé est stocké et utilisé pour les applications.

4.2. Créer un inventaire de chaque système en utilisant le TLD privé de façon automatisée

Vous avez besoin d'un résumé des données enregistrées obtenues à partir de l'étape précédente. Ce résumé devrait être une liste de tous les appareils et tous les noms ayant fait l'objet d'une requête plutôt que chaque instance du dispositif faisant une requête. La raison pour laquelle vous avez besoin de tous les noms ayant fait l'objet d'une requête est que certains dispositifs auront de multiples applications qui devront être corrigées. En conséquence, le résumé doit inclure à la fois tous les systèmes et toutes les applications sur chaque système utilisant le TLD privé. Ce résumé met en évidence les appareils qui ont besoin d'être changés.

4.3. Déterminer où vos noms mondiaux DNS 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 privé. Vous devez déterminer qui est en charge de vos noms DNS et quels sont les processus utilisés pour créer et mettre à jour les noms dans le DNS. Cela peut se faire au sein de votre département TI, ou bien par un fournisseur de services (bien souvent la même société que celle à travers laquelle vous obtenez votre connexion Internet).

4.4. Changer la racine de votre espace privé pour utiliser un nom du DNS mondial

Une stratégie usuelle pour l'utilisation d'un nom DNS global comme la racine de votre espace de noms privé est d'avoir un nom accessible au public délégué par le DNS mondial, mais ensuite il vous faut utiliser votre serveur de noms faisant autorité pour administrer tous les noms en dessous. Par exemple, si votre entreprise a le nom de domaine mondial `ourcompany.com`, vous pouvez choisir `ad1.ourcompany.com` comme le nom de la racine.

Si votre organisation a plus d'un nom de domaine dans le DNS mondial, vous devez inclure vos noms dans une racine qui puisse être plus facilement contrôlée par le personnel TI de votre organisation.

Dans certains cas, les noms supplémentaires sont contrôlés par d'autres entités, comme par exemple un département de marketing. Dans la mesure du possible, il est préférable que votre nom soit dans la racine sous un nom déjà contrôlé par l'organisation TI.

Les étapes pour faire ce changement dépendent de votre logiciel de serveur de noms privé, de la version spécifique de ce logiciel, de la topologie des serveurs de noms de votre réseau privé, et de la configuration existante du serveur de noms. Ces détails sont au-delà de la portée de ce document, mais devraient être considérés dans les instructions du fournisseur de votre système actuel. En outre, dans de nombreuses organisations, ce changement nécessite l'autorisation de certains niveaux de gestion, 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 avez des certificats pour tous les hôtes qui utilisent des noms dans l'espace privé, vous devrez créer des certificats pour les hôtes utilisant les nouveaux noms (entièrement qualifiés). Les étapes pour obtenir ces certificats dépendent de votre autorité de certification et sont également au-delà de la portée de ce document.

4.5. Attribuer de nouvelles adresses IP pour les hôtes, si nécessaire

Si vous avez des certificats TLS basés sur votre ancien nom de TLD privé, vous devrez obtenir de nouveaux certificats pour les nouveaux noms. Si votre serveur web ne supporte pas l'extension au TLS de l'indication du nom du serveur (*Server Name Indication* - SNI) qui permet plus d'un nom de domaine pour être servi sous un TLS sur la même adresse IP, vous devrez ajouter des adresses IP aux hôtes de sorte à ce que l'hôte supporte l'ancien nom privé sur l'adresse IP d'origine et le nouveau nom sur une nouvelle adresse IP. Alternativement, vous pouvez mettre à jour le logiciel de votre serveur Web dans une version capable de gérer les extensions SNI correctement.

4.6. Créer un système de suivi de l'équivalence entre les nouveaux noms privés et les anciens

Lorsque vous changez tous les noms privés pour utiliser la nouvelle racine, vous continuerez à servir des adresses et à identifier les requêtes de vos anciens noms privés afin de vérifier que les systèmes qui ne se trouvent pas dans votre inventaire et qui n'ont pas été mis à jour utilisent les noms qui se trouvent dans la racine du DNS. Pour cette raison, vous devez vous assurer que les valeurs pour les adresses IP des nouveaux et des anciens noms privés soient les mêmes.

Certains logiciels d'espace de noms privés vous permettent de garder les deux arbres en parallèle, mais si vous avez des logiciels plus anciens ou plusieurs serveurs de noms faisant autorité, il est probable que vous ayez à faire le suivi de l'équivalence en utilisant des outils personnalisés. Ces outils personnalisés doivent interroger souvent tous les noms dans les espaces de noms actuels et anciens, et vous alerter s’il y a un décalage de sorte que vous puissiez déterminer quel est le système modifié sans un changement parallèle dans l'autre système.

Si vous aviez besoin d'ajouter des adresses IP à l'étape précédente du fait d'avoir des certificats SSL / TLS, le décalage doit être autorisé par le logiciel de monitorage de l'équivalence.

4.7. Former les utilisateurs et les administrateurs des systèmes pour utiliser le nouveau nom

Outre la modification des systèmes où les noms sont inscrits dans les configurations, vous devez changer la logique des utilisateurs afin qu'ils changent les vieux noms privés pour de nouveaux noms. Cette formation doit être effectuée avant la mise en œuvre des étapes suivantes afin que les utilisateurs puissent s'habituer aux nouveaux noms, mais la formation devrait établir clairement que le changement approche et qu'ils doivent commencer à penser en termes des nouveaux noms dès que possible. C'est aussi un bon moment pour former les utilisateurs sur l'utilisation des FQDN. Utilisez les explications des conséquences inattendues ou indésirables qui peuvent affecter votre organisation afin de favoriser la sensibilisation et l'acceptation.

4.8. Changez chaque système affecté pour les nouveaux noms

Voici le moment où la migration des anciens noms privés vers les nouveaux noms devient réelle pour tous les systèmes sur le réseau (ordinateurs, périphériques de réseau, imprimantes, etc.). Les noms privés sont remplacés par les nouveaux noms DNS système par système. Chaque instance de l'ancien nom privé se trouve dans tous les logiciels sur le système qui est remplacé par le nouveau nom DNS. En même temps, vous devriez déconseiller l'utilisation de noms courts non qualifiés dans les listes de recherche.

La surveillance qui a été démarrée ci-dessus est particulièrement importante pendant cette étape. Vous êtes peu susceptible d'être en mesure de déterminer toutes les applications dans tous les systèmes ayant les anciens noms privés incorporés. Au lieu de cela, le système de surveillance doit être consulté après la modification de chaque système afin de voir si ce système fait encore des requêtes pour les anciens noms privés.

De nombreux systèmes déclenchent certaines applications d'initialisation quand ils sont allumés. Ces applications peuvent avoir des noms de système incorporés qui peuvent être difficiles à trouver. Après avoir changé tous les anciens noms par les nouveaux noms DNS dans un système, redémarrer le système et utiliser le logiciel de surveillance pour surveiller les recherches de noms. Si le système est à la recherche de l'un des anciens noms privés, vous devez déterminer quel est le logiciel qui est à l'origine de cette demande et le modifier pour qu'il utilise les nouveaux noms. Ce processus peut prendre quelques redémarrages afin que le système soit bien configuré.

4.9. Commencer à surveiller l'utilisation des anciens noms privés au serveur de noms

Vous devez configurer votre serveur de noms faisant autorité pour commencer à surveiller toutes les requêtes de noms ayant la vieille racine. Comme vos utilisateurs ne devraient plus utiliser ces noms, l'enregistrement créé par cette étape de contrôle peut ne pas être très grand ; s'il l'était vous aurez à répéter certaines des étapes ci-dessus pour les systèmes particuliers de votre réseau.

4.10. Mettre en place une surveillance à long terme sur le périmètre pour surveiller les anciens noms privés

Les étapes précédentes auraient du trouver la grande majorité des utilisations des anciens noms privés, mais quelques systèmes (éventuellement clés) peuvent encore utiliser les anciens noms privés,

bien que cela se produise rarement. Une façon de détecter ces requêtes de noms est d'ajouter des règles à tous les pare-feux au bord de votre réseau pour rechercher toutes les requêtes qui s'enfuient. Ces règles devraient avoir une haute priorité qui leur est associée et devraient être configurées pour générer des notifications d'événements afin que le personnel TI soit alerté rapidement. Par contre, vous pouvez trouver ces événements enregistrés dans le pare-feu, mais cela augmenterait les probabilités de les perdre. Les alertes qui sont déclenchées lorsque les requêtes arrivent permettront au personnel de détecter ces événements qui, nous espérons, deviendront de plus en plus rares. Certains pare-feux ne supportent ce type de règle qu'en ajoutant des fonctionnalités supplémentaires à un coût supplémentaire ; si cela est vrai pour votre pare-feu, vous devez évaluer si l'avantage de trouver des demandes perdues vaut le coût supplémentaire ou pas.

4.11. Changer tous les noms de la vieille racine pour indiquer une adresse ne fonctionnant pas

Après avoir formé les utilisateurs, le moyen le plus efficace pour être sûr que les anciens noms privés ne soient plus utilisés avant de les supprimer est d'avoir tous les anciens noms privés dans un serveur que vous aurez configuré pour ne pas répondre à toute sorte de requêtes de service. Cela aide aussi à débusquer tous les systèmes qui utilisent encore l'ancien espace de noms mais qui n'ont pas été détectés dans les étapes précédentes.

L'adresse identifiée devrait être un serveur qui, à coup sûr, n'exécute aucun service. Ce faisant, il n'y a aucune chance que les systèmes qui utilisent un ancien nom privé reçoivent des informations erronées et que les applications rapportent des erreurs qui devraient être facilement détectables ou comprises par les utilisateurs ; dans le cadre de la formation de sensibilisation, vous pouvez recommander aux utilisateurs d'informer toutes les erreurs de ce genre au personnel TI. Une fois cette étape mise en œuvre, le système de surveillance qui vérifie l'équivalence entre les anciens et les nouveaux noms (décrite ci-dessus) doit être tenu à jour avec les changements.

Les noms doivent être changés un à la fois, probablement avec au moins quelques heures entre chaque modification ou lot de modifications. Pendant cette étape il se peut qu'il soit nécessaire d'appeler le département TI. La mise en place des changements aidera donc à équilibrer la charge des appels alors que les noms encore utilisés commenceront à ne plus fonctionner.

4.12. Si les certificats ont été délivrés pour des hôtes sous les anciens noms privés, il faudra les révoquer

Si votre organisation a des certificats SSL / TLS émis pour tous les serveurs de votre réseau en utilisant les anciens noms privés, ces certificats doivent être révoqués. C'est assez facile à faire si votre organisation agit comme sa propre autorité de certification. Si vous avez utilisé une autorité de certification commerciale pour délivrer des certificats pour l'espace de noms privé, vous devez déterminer le processus de l'autorité de certification pour demander la révocation ; différentes autorités de certification peuvent avoir des exigences différentes pour ce type de requêtes.

4.13. Opérations à long terme avec le nouveau nom

Notez que l'ancien nom privé et les domaines sont encore servis, et ils continueront d'être servis aussi longtemps que le serveur de noms sera utilisé. Il n'y a aucune raison de les supprimer, et dans de nombreux systèmes tels qu'*Active Directory*, il peut s'avérer difficile de supprimer le premier nom qui a été configuré dans le système.

Voici une bonne raison de laisser le nom là: cela vous permet de voir s'il y a des traces résiduelles de l'ancien nom privé dans les systèmes de votre réseau. Tant que toutes les adresses associées à tous les noms sous ce point de TLD privé à un hôte sans services seront en cours d'exécution, vous pouvez utiliser les journaux du serveur de noms (et, pour avantage supplémentaire, un système connectant tout le trafic à ce serveur) pour déterminer si vous avez été minutieux en supprimant l'ancien nom privé.

5. Mesures pour atténuer les collisions de noms associées aux listes de recherche

Afin d'atténuer de manière fiable les problèmes liés à des collisions de noms dues aux listes de recherche, les utilisateurs et les systèmes doivent changer la façon dont ils utilisent les noms de domaine. Il serait peut être utile de préparer les utilisateurs à l'avance par le biais de notifications de modification, des programmes de sensibilisation et de formation.

Notez que si vous faites déjà une administration centralisée, ces actions sont sans doute moins difficiles de ce que vous pourriez imaginer. Beaucoup de gens qui utilisent normalement des listes de recherche savent qu'ils peuvent aussi taper le nom complet si cela était nécessaire (par exemple s'ils ont accès à un serveur autre que le réseau privé de l'organisation), et qu'ils auront besoin de moins de formation que ceux qui ne comprennent que les noms courts non qualifiés.

5.1. Surveiller les requêtes venant dans le serveur de noms

Afin d'atténuer les problèmes causés par des listes de recherche, vous devez connaître tous les ordinateurs, le matériel de réseau, et tout autre système qui utilise des listes de recherche dans les requêtes. Tous les dispositifs qui utilisent des listes de recherche de façon automatisée devront être mis à jour.

Il existe trois méthodes courantes pour effectuer cette surveillance et l'inventaire des systèmes :

- le serveur de noms récursif (comme *Active Directory*) peut avoir une fonction de journalisation, et vous pouvez activer la fonctionnalité de journalisation pour obtenir des détails sur toutes les requêtes ayant des noms courts non qualifiés.

- de nombreux pare-feu modernes peuvent également être configurés pour détecter et identifier les requêtes de tous les noms. Cela peut ne pas être aussi efficace que la connexion du système de nommage lui-même, en fonction de la topologie de votre réseau. Par exemple, si une requête ne passe pas par un pare-feu, le pare-feu ne peut pas voir la requête, et en conséquence elle sera perdue.

- si aucune des possibilités précédentes ne peut être utilisée, le serveur de noms peut être contrôlé à l'aide d'un programme de capture de paquets tel que Wireshark. Toutefois, cette méthode exige que les données capturées soient traitées avec un programme dans le but de trouver les requêtes tout juste pour les noms courts non qualifiés.

Notez que cette démarche peut produire des résultats déroutants. Les dispositifs tels que les ordinateurs et les téléphones peuvent avoir des applications dans lesquelles les utilisateurs tapent des noms; ces dispositifs apparaîtront dans l'enquête, même si toutes les versions stockées des noms courts non qualifiés pourraient ne pas apparaître. Pour 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 les applications.

5.2. Créer un inventaire de chaque système en utilisant les noms courts non qualifiés de façon automatisée

Vous avez besoin d'un résumé des registres de l'étape précédente. Ce résumé devrait être une liste de tous les dispositifs et de tous les noms courts non qualifiés ayant fait l'objet d'une requête plutôt que de chaque instance du dispositif ayant fait une requête. La raison pour laquelle vous avez besoin de tous les noms ayant fait l'objet d'une requête est que certains dispositifs auront de multiples applications qui devront être corrigées. Ce résumé met en évidence les appareils qui ont besoin d'être changés.

5.3. Former les utilisateurs et les administrateurs de système pour utiliser les noms de domaine complets entièrement qualifiés (FQDN)

Outre la modification des systèmes où les noms courts non qualifiés sont entrés dans n'importe quelle configuration (soit une configuration de système ou la configuration d'une application individuelle), vous devez changer les manières dont les utilisateurs pensent à les faire changer, ne plus utiliser des noms courts mais des noms complets. Utilisez les explications sur les conséquences inattendues ou indésirables qui peuvent affecter votre organisation afin de favoriser la sensibilisation et l'acceptation.

5.4. Changer chaque système affecté pour l'utilisation des FQDN

Remplacez les noms courts non qualifiés avec leur équivalent de nom de domaine complet entièrement qualifié système par système. Chaque instance du nom court non qualifié qui se trouve dans tous les logiciels sur le système doit être remplacée par le nouveau nom de domaine complet.

La surveillance qui a été démarrée ci-dessus est particulièrement importante pendant cette étape. Vous êtes peu susceptible d'être en mesure de déterminer toutes les applications dans tous les systèmes en cours de changement ayant les noms courts non qualifiés incorporés. Au lieu de cela, le système de surveillance doit être consulté après la modification de chaque système afin de voir si ce système fait encore des requêtes pour les noms courts non qualifiés.

De nombreux systèmes déclenchent certaines applications d'initialisation quand ils sont allumés. Ces applications doivent avoir des noms de systèmes incorporés qui dépendent de listes de recherche incorporées, et tout cela peut être difficile à trouver. Après avoir changé tous les noms du système pour utiliser les FQDN, redémarrer le système et utiliser le logiciel de surveillance pour surveiller les recherches de noms. Si le système est à la recherche d'un nom court non qualifié, vous devez déterminer quel est le logiciel qui est à l'origine de cette demande et le modifier pour qu'il utilise les FQDN. Ce processus peut prendre quelques redémarrages afin que le système soit bien configuré.

5.5. Désactiver les listes de recherche dans les résolveurs de noms partagés

Voici le moment où l'abandon des noms courts non qualifiés devient réel pour tous les systèmes sur le réseau (ordinateurs, périphériques de réseau, imprimantes, etc.). Les listes de recherche peuvent exister dans tout système faisant la résolution de nom ou qui sert la configuration à d'autres systèmes, comme un serveur DHCP. Bien souvent, ces systèmes sont des serveurs de noms autonomes, mais ils peuvent aussi être des pare-feu ou d'autres périphériques de réseau. Quel que soit le type de système,

les listes de recherche doivent être désactivées sur chacun d'eux afin d'empêcher que les utilisateurs se servent des noms courts non qualifiés dans un espace de noms donné.

5.6. Commencer la surveillance pour l'utilisation des noms courts non qualifiés dans les serveurs de noms

Vous devriez configurer votre serveur de noms pour commencer à surveiller toutes les requêtes de noms ayant besoin d'utiliser des listes de recherche. Si vous donnez un préavis et de la formation, vos utilisateurs ne devraient plus utiliser ces noms, de sorte que le journal créé par cette étape de contrôle peut ne pas être très grand ; s'il l'était vous aurez à répéter certaines des étapes ci-dessus pour les systèmes particuliers de votre réseau.

5.7. Mettre en place une surveillance à long terme sur le périmètre pour surveiller les noms courts non qualifiés

Les étapes précédentes auraient trouvé la grande majorité des utilisations des anciens noms privés, mais quelques systèmes (éventuellement clés) peuvent encore utiliser les non courts non qualifiés, bien que cela se produise rarement. La meilleure manière de détecter ces requêtes de noms est d'ajouter des règles à tous les pare-feux au bord de votre réseau pour rechercher toutes les requêtes qui s'enfuient. Ces règles devraient avoir une haute priorité qui leur est associée et devraient être configurées pour générer des notifications d'événements afin que le personnel TI soit alerté rapidement. Par contre, vous pouvez trouver ces événements enregistrés dans le pare-feu, mais cela augmenterait les chances de les perdre. Les alertes qui sont déclenchées lorsque les requêtes arrivent permettront au personnel de détecter ces événements que, nous espérons, deviendront de plus en plus rares. Certains pare-feux ne supportent ce type de règle qu'en ajoutant des fonctionnalités supplémentaires à un coût supplémentaire ; si cela est vrai pour votre pare-feu, vous devez évaluer si l'avantage de trouver des demandes perdues vaut le coût supplémentaire ou pas.

6. Récapitulatif

Les collisions de noms ont le potentiel de produire des résultats inattendus pour les organisations qui utilisent les espaces de noms privés. Ce document répertorie certains de ces résultats potentiels et indique les meilleures pratiques pour changer la façon dont les espaces de noms privés sont utilisés au sein des organisations.

Pour les espaces de noms qui ont utilisé un TLD privé qui devient (ou est déjà) un TLD dans le DNS mondial, l'atténuation se produit plutôt dans la forme de la migration de l'espace de nom vers un espace de noms dans la racine du DNS mondial. Pour les espaces de noms qui utilisent des noms raccourcis avec des listes de recherche, l'atténuation ne peut venir que par l'élimination de l'utilisation des listes de recherche. Les étapes à suivre pour la réalisation de ces mesures d'atténuation comprennent également la surveillance à long terme dans le réseau privé pour être sûr que toutes les instances de noms qui pourraient causer des collisions ne soient plus utilisés.

Pour atténuer complètement les problèmes de collisions de noms il faut utiliser les noms complets pleinement qualifiés dans tous les endroits où un nom de domaine est utilisé. Dans un réseau qui utilise déjà le DNS mondial, cela signifie ne pas utiliser des listes de recherche. Dans un réseau qui utilise un espace privé, cela signifie que l'espace de noms privé devrait se trouver dans la racine du DNS mondial, et ne devrait pas utiliser des listes de recherche.

Annexe A : Pour en savoir plus

Les documents suivants ont été produits par diverses organisations au sein de l'ICANN. D'autres organisations fournissent des documents qui pourraient également s'avérer utiles. Plus important encore, le fournisseur de votre logiciel et / ou matériel de serveur de noms peut vous offrir des informations précieuses sur son site Web de support technique.

A.1. Introduction au programme des nouveaux gTLD

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

A.2. Collision de noms dans le DNS

ICANN a chargé le cabinet Interisle Consulting Group, LLC, pour créer ce rapport en profondeur concernant les collisions de noms potentielles. Le rapport donne un aperçu des collisions de noms, présente des données sur les TLD actuellement inexistants qui sont actuellement interrogés sur les serveurs racine, et donne beaucoup de contexte sur les problèmes que les collisions de noms pourraient présenter. 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.

C'est le plan adopté par l'ICANN sur la façon de gérer les occurrences de collision de noms entre les nouveaux gTLD et les espaces de noms privés. Il contient également de nombreux pointeurs vers les commentaires reçus par l'ICANN concernant les propositions antérieures qui se rapportent 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. Préoccupations concernant les nouveaux gTLD : noms sans point et collisions de noms

Les listes de recherche sur des systèmes différents peuvent donner des résultats très différents en fonction de ce qui est dans le nom court non qualifié qui fait l'objet d'une requête. Cet article est ciblé sur les listes de recherche pour les domaines sans point (des TLD ayant des enregistrements d'adresse à leur sommet), mais la description du traitement de la liste de recherche est utile dans d'autres contextes. https://labs.ripe.net/Members/gih/dotless-names

A.5. SAC 045 : requêtes des domaines de premier niveau non-valides au niveau de la racine du DNS

Ce rapport du comité consultatif sur la sécurité et la stabilité de l'ICANN décrit les types de requêtes pour les TLD vérifiées dans les serveurs racines au moment de sa rédaction. http://www.icann.org/en/groups/ssac/documents/sac-045-en.pdf

A.6. SAC 057 : avis du SSAC sur les certificats de noms internes

Ce rapport du comité consultatif sur la sécurité et la stabilité de l'ICANN décrit les implications sur la sécurité et de stabilité pour les certificats qui contiennent des noms privés (internes). Il identifie une pratique des autorités de certification qui peut être exploitée par des attaquants et pourrait poser des

risques importants concernant la confidentialité et l'intégrité des communications Internet sécurisées. http://www.icann.org/en/groups/ssac/documents/sac-057-en.pdf